EU DIGITAL OMNIBUS

Automatic analysis of call for evidence feedback

WWW.SKIMLE.COM Contact: henri@skimle.com

1 Support for deregulation 7
1.1 Harmonized Digital Rulebook Simplification 7
1.1.1 Simplification Governance and Digital Omnibus Consolidation 7
1.1.2 Unified Definitions, Scope and Taxonomy 15
1.1.3 Legal Hierarchy, Lex Specialis and Conflict Resolution 17
1.1.4 Cross-Regulation Alignment and Single Market Coherence 19
1.1.5 Standards, Interoperability and Specifications Governance 24
1.1.6 Digital Identity and Trust Services Streamlining 26
1.1.7 Data, Privacy and AI Governance Alignment 29
1.1.8 Risk-Based Proportionality and SME Relief 34
1.1.9 Uniform Enforcement, Mutual Recognition and One-Stop Supervision 37
1.1.10 Streamlined Compliance, Report-Once and Templates 40
1.1.11 Digital-by-Default Tools and Paperless Administration 42
1.1.12 Miscellaneous 44
1.2 Coordinated Governance, Guidance & Phased Timelines 46
1.2.1 Cross-Regime Alignment, Interoperability & Legal Coherence 46
1.2.2 Centralized Guidance & Aligned Definitions 49
1.2.3 Coordinated Oversight, One-Stop Shop & Unified Reporting 51
1.2.4 Proportional Scope, Simplification & Predictable Enforcement 54
1.2.5 Standards-Aligned Phased Timelines & Grace Periods 58
1.2.6 Capacity Building & Conformity Assessment Infrastructure 63
1.2.7 Stakeholder Consultation, Transparency & Co-Regulation 66
1.2.8 Miscellaneous 70
1.3 Risk-Based, SME-Friendly Proportionality 71
1.3.1 Outcomes-Based, Technology-Neutral Rules 72
1.3.2 Harmonised Frameworks & Cross-Regime Alignment 75
1.3.3 Risk-Tiered Scope, Thresholds & Exemptions 77
1.3.4 Predictable, Phased Timelines & Fair Transitions 79
1.3.5 Proportionate Reporting, Documentation & Transparency 81
1.3.6 Proportionate Oversight & Enforcement 84
1.3.7 Level Playing Field, Fair Costs & Burden Sharing 86
1.3.8 SME Simplification, Guidance & Support Tools 90
1.3.9 Miscellaneous 94
1.4 Competitiveness & Innovation Enablement 95
1.4.1 Industrial Strategy, Sovereignty & Global Competitiveness 96
1.4.2 Open Markets & Fair Competition 98
1.4.3 Proportionate, Predictable Regulation 102
1.4.4 Infrastructure, Standards & Public Procurement 105
1.4.5 Capital, Scale-Up & Investment Climate 107
1.4.6 Talent, Skills & Cross-Border Collaboration 110
1.4.7 Data Access, IP & Legal Certainty 111
1.4.8 Innovation-Friendly AI & Data Governance 113

1.4.9 Experimentation & Sandboxes 116
1.4.10 Miscellaneous 117
1.5 Data Access, Interoperability & Cross-Border Transfers 118
1.5.1 Regulatory Alignment & Streamlining 119
1.5.2 Cross-Border Transfers & Adequacy 123
1.5.3 Interoperability, Standards & Data Spaces 126
1.5.4 Digital Identity & Trust Infrastructure 129
1.5.5 Cloud Portability & Switching 132
1.5.6 Proportionate Access, Privacy & Trade Secrets 134
1.5.7 Competition & Fair Data Access 137
1.5.8 Open Data & B2G Access 139
1.5.9 Sectoral Data Sharing & Compliance 142
1.5.10 AI & Research Data Access 145
1.5.11 Miscellaneous 147
1.6 Unified Reporting & Incident Management 147
1.6.1 Aligned Definitions, Thresholds, Timelines & Triggers 148
1.6.2 Harmonized Templates, Taxonomies & Interoperability 150
1.6.3 Coordinated Authorities, Routing, Group Reporting & Mutual Recognition 152
1.6.4 Streamlined Obligations & Burden Reduction 155
1.6.5 Risk-Based Triage, Proportional Scope & Phased Notifications 157
1.6.6 One-Stop Portals & Once-Only Reporting 160
1.6.7 Digital Automation, APIs & Machine-Readable Data Sharing 164
1.6.8 Safe Harbors, Liability & Role Clarity 166
1.6.9 Miscellaneous 168
1.7 Privacy & Data Protection Modernization 169
1.7.1 Definitions, Scope & De-identification 170
1.7.2 Regulatory Harmonization & Compliance Simplification 174
1.7.3 Enforcement & Governance Modernization 177
1.7.4 International Transfers & Extraterritoriality 180
1.7.5 Risk-Based Processing & Legitimate Interests 181
1.7.6 Consent, Cookies & ePrivacy Modernization 183
1.7.7 Data Subject Rights & User Control 188
1.7.8 Public Interest, Research & Retention Limits 191
1.7.9 Safety, Fraud & Government Access Controls 193
1.7.10 AI Alignment & Privacy-Preserving Technologies 195
1.7.11 Miscellaneous 197
1.8 Cybersecurity & Certification Alignment 198
1.8.1 Regulatory Harmonization & Streamlining 199
1.8.2 International Standards & Mutual Recognition 201
1.8.3 Conformity Assessment, Accreditation & Oversight 205
1.8.4 Risk-Based, Outcome-Focused Assurance 207
1.8.5 Scope, Sectoral Schemes & Guidance 209

1.8.6 Technical Baselines & Cryptography 211
1.8.7 Secure-by-Design & AI Assurance 212
1.8.8 Supply Chain Security & SBOM Assurance 213
1.8.9 Digital Identity & Trust Services (eIDAS/QSCD) 215
1.8.10 Lifecycle Certification & Update Management 217
1.8.11 Vulnerability Disclosure & Management 218
1.8.12 Miscellaneous 219
1.9 Proportionate AI Governance Simplification 220
1.9.1 Roles, Definitions and Proportionate Liability 220
1.9.2 Risk-Tiered Scope and Exemptions 223
1.9.3 Adaptive, Stable and Capability-Based Oversight 225
1.9.4 Safety, Security and Fundamental Rights 227
1.9.5 Cross-Sector, Cross-Border and IP Alignment 229
1.9.6 Standards, Sandboxes and Assurance Pathways 230
1.9.7 Streamlined Compliance and Reporting 233
1.9.8 Proportionate Transparency and Labelling 236
1.9.9 SME-Friendly Implementation and Harmonization 238
1.9.10 Foundation Models and GPAI Simplification 240
1.9.11 Open-Source and Research Flexibility 243
1.9.12 Miscellaneous 245
1.10 Sector-Specific Alignment & Legacy Exemptions 246
1.10.1 Lex Specialis & Cross-Regulatory Harmonization 246
1.10.2 Sector Law Integration & Streamlining 249
1.10.3 Legacy, Grandfathering & Transition Safeguards 252
1.10.4 Intra-Group & Outsourcing Carve-outs 254
1.10.5 Product-Specific Proportionality 255
1.10.6 Cybersecurity, Critical Infrastructure & Digital Services Carve-outs 256
1.10.7 Financial Services & Digital Regulation Alignment 259
1.10.8 Health & Medical AI Alignment 262
1.10.9 Industrial, Energy & Transport Alignment 264
1.10.10 Media, Education & Research Adjustments 267
1.10.11 Miscellaneous 268
1.11 Miscellaneous 269
1.11.1 Trade, Infrastructure & Market Sovereignty 270
1.11.2 Corporate Law, Tax & Business Practices 271
1.11.3 Smart Regulation, Evidence & Compliance 272
1.11.4 Advertising, Marketing & Media Pluralism 276
1.11.5 AI, Public Health & Safety Standards 276
2 Criticism of deregulation 277
2.1 Protect Fundamental Rights and Safeguards 278
2.1.1 Rights-Centered Innovation & Democracy 278
2.1.2 Non-Regression & Regulatory Safeguards 279

2.1.3 Accountability, Oversight & Rights Impact Assessments 282
2.1.4 Fair Automated Decision-Making & Redress 284
2.1.5 Equality and Inclusion 285
2.1.6 Privacy, Data & IP Rights 286
2.2 Harmonized Regulation and Legal Certainty 287
2.2.1 Evidence-Based, Proportionate & Innovation-Friendly Simplification 288
2.2.2 Clear Scope, Definitions, Roles & Liability 291
2.2.3 Cross-Regulatory Coherence & Conflict Resolution 293
2.2.4 Predictable Timelines, Transitions & Regulatory Stability 295
2.2.5 International Alignment & Mutual Recognition 300
2.2.6 Standards, Certification & Technical Interoperability 302
2.2.7 Consistent Guidance, Transparency & Capacity Building 305
2.2.8 Harmonized Implementation, Supervision & Enforcement 308
2.2.9 Streamlined Compliance, Reporting & Contracting 311
2.2.10 Miscellaneous 315
2.3 Enforcement, Oversight and Accountability 316
2.3.1 Governance, Coordination, Jurisdiction & Role Clarity 317
2.3.2 Regulatory Capacity, Powers & Resources 319
2.3.3 Enforcement Strategy, Timeliness & Uniformity 321
2.3.4 Cross-Border & Sectoral Enforcement 323
2.3.5 Transparency, Participation, Audits & Monitoring 324
2.3.6 Independent Oversight, Integrity & Safeguards 327
2.3.7 Accountability, Liability, Sanctions & Redress 328
2.4 Data Governance, Interoperability and Sovereignty 330
2.4.1 Regulatory Coherence & Legal Clarity 330
2.4.2 Digital Sovereignty & Cross-Border Transfers 332
2.4.3 Interoperability, Standards & Portability 335
2.4.4 Access & Reuse Governance 336
2.4.5 Security, Confidentiality & IP 338
2.4.6 Data Intermediaries, Platforms & Market Governance 340
2.4.7 Sectoral Governance & Public Data Infrastructure 341
2.4.8 Open Data, Quality & Metadata 343
2.5 Privacy, Consent and Anti-Tracking Protections 344
2.5.1 Legal Bases, GDPR/ePrivacy & Enforcement 345
2.5.2 Data Minimization, Identifiability & Sharing Controls 347
2.5.3 Consent UX, Transparency & User Choice 348
2.5.4 Consent Signals, Standards & PIMS 351
2.5.5 Privacy-Enhancing Technologies & AI Safeguards 354
2.5.6 Anti-Tracking, Device & Location Protections 356
2.5.7 Adtech, Profiling & Targeted Marketing Limits 358
2.5.8 Economic, Ecosystem & Compliance Trade-offs 359
2.5.9 Miscellaneous 362

2.6 Digital Identity, Trust Services and Wallet Integrity 362
2.6.1 Governance, Business Models & User Protections 362
2.6.2 Security & Interoperability Standards 364
2.6.3 Legal, Regulatory & QTSP Compliance 365
2.6.4 Miscellaneous 367
2.7 Cybersecurity Resilience and Incident Reporting 367
2.7.1 EU Governance, ENISA & Policy Workability 368
2.7.2 Unified Incident Reporting & Definitions 370
2.7.3 Risk-Based Obligations & Timelines 373
2.7.4 Standards & Certification Alignment 374
2.7.5 Supply Chain Security & CRA Alignment 375
2.7.6 Operational Preparedness & Technical Resilience 377
2.7.7 Secure Disclosure, Privacy & Liability 379
2.7.8 Sector Tailoring & SME Support 381
2.7.9 Miscellaneous 382
2.8 AI Governance, Transparency and High-Risk Safeguards 382
2.8.1 Implementation, Standards, Enforcement & Legal Certainty 383
2.8.2 Sectoral Alignment & Regulatory Coherence 385
2.8.3 Risk Classification, Proportionality & Burden Reduction 386
2.8.4 Fundamental Rights, Impact & Accountability 390
2.8.5 Transparency, Disclosure & Registration 392
2.8.6 Data Governance, Testing & Traceability 394
2.8.7 Safety-by-Design, Security & Human Oversight 396
2.8.8 Documentation, Monitoring & Incident Reporting 397
2.8.9 GPAI Governance, Upstream Duties & IP Rights 399
2.8.10 Miscellaneous 401
2.9 Sectoral Safety, Accessibility and Public Interest 402
2.9.1 Critical Infrastructure and Public Interest Governance 402
2.9.2 Environmental Sustainability and Safety 403
2.9.3 Healthcare and Occupational Safety Governance 404
2.9.4 Digital Inclusion, Platforms and Consumer Protection 406
2.10 Fair Competition, Gatekeepers and Media Sustainability 407
2.10.1 Gatekeepers & Market Contestability 408
2.10.2 Open Internet, Device Neutrality & Network Competition 410
2.10.3 Standards, Interoperability & Digital Sovereignty 411
2.10.4 Data Fairness, Access & Privacy 413
2.10.5 Platform Transparency, Regulation & Disinformation 415
2.10.6 Media Sustainability, Advertising & Measurement 416
2.10.7 AI Governance & Competitive Neutrality 417
2.10.8 Miscellaneous 418
2.11 SME Proportionality and Practical Compliance 419
2.11.1 Regulatory Coherence & Harmonization 420

2.11.2 Risk-Based, Proportionate & Sector-Tailored 421
2.11.3 Safeguarded Simplification 424
2.11.4 Compliance Burden & Admin Relief 425
2.11.5 SME Support & Capacity Building 428
2.11.6 Innovation, Competition & Data Access 430
2.12 Miscellaneous 431
2.12.1 Digital Strategy, Leadership & Competitiveness 432
2.12.2 Governance, Evidence & Process Integrity 433
2.12.3 Simplification & Administrative Efficiency 435
2.12.4 Innovation, Trust & Adoption 435
2.12.5 Sustainability & Climate Integration 436

1 Support for deregulation

The strongest insight is EU-wide maximum harmonisation with clear lex specialis and mutual recognition so firms face one set of rules, one audit/report, and one supervisor—scaling duties by risk rather than size. This means coherent cross-regime governance across AI, data, cybersecurity, privacy, and sector laws, with standards-led conformity, single reporting windows, and digital-by-default processes (templates, APIs, reusable evidence, identity and trust services). Sector primacy should embed horizontal duties into established frameworks (health, finance, transport, energy), retire overlaps, and use transparent carve-outs. Proportionality for SMEs requires tiered obligations, phased timelines, practical support (codes, helpdesks, sandboxes), and calibrated fees and assurance. Competitiveness benefits from contestable markets, outcomes-based funding, fast-track licensing, innovation-oriented procurement, and talent mobility. Incident reporting should be once-only, API-first, and severity-tiered, with safe harbors and automated routing. Assurance and certification should align across acts via EU/international standards, MRAs, outcome-focused testing, minimal interoperable SBOMs, and lifecycle-aware credentials. Cross-border data flows need GDPR-grounded certainty, open standards, common data spaces, realistic cloud portability, and an interoperable identity layer (wallets) to automate authorisations. AI oversight should be risk-tiered, context-aware, and role-accurate, preserving research and open-source flexibility with proportionate transparency. Implementation must be sequenced: central guidance, one-stop supervision, capacity building, comitology clarity, and temporary equivalence. Across sub-categories, the dominant trends are harmonisation, risk-proportionate obligations, standards-based interoperability, and digital-first, once-only processes—delivering predictable compliance that sustains rights, security, and EU-wide scale.

1.1 Harmonized Digital Rulebook Simplification

The standout insight is to codify common definitions, scopes, and conflict-resolution (lex specialis, mutual recognition) so providers can rely on one set of rules, one audit, and one supervisor across the EU. Building on this, alignment across AI, data, cybersecurity, privacy, and sectoral regimes should be maximum-harmonisation, reaffirm Single Market principles (country-of-origin, no gold-plating, no data localisation), and deliver predictable cross-border compliance. Practical simplification means report-once mechanisms, a Single Reporting Window, consolidated impact assessments (DPIA/FRIA), and reusable evidence, applied with risk-based, technology-agnostic, outcome-oriented requirements and tailored SME relief. Coherent data/AI/privacy governance must harmonise GDPR, ePrivacy, the AI Act, the Data Act/DGA, DSA/DMA, resolve mixed-data boundaries, and avoid duplicated high-risk AI obligations—leveraging standards and established conformity routes. Identity and trust services should make eIDAS the single reference, align EUDI and Business Wallets, fix PSD2 overlaps, standardise onboarding, and reduce audits, with inclusion by design. A standards-led model (ISO, CEN/CENELEC) enables single disclosures and modular “one-audit” recognition across acts. Uniform enforcement and one-stop supervision need EU-wide risk assessment formats and audit checklists. Digital-by-default (eDeclarations, DPP, digital labelling), administrative silence, responsible declarations, and RegTech portals cut red tape. The Digital Omnibus should drive holistic fitness checks, clear procedures, and future-responsive monitoring, while preserving fundamental rights and security. Across categories, common trends are harmonisation of terminology and enforcement, risk-proportionate obligations, standards-based interoperability, and digital-first processes. Together they enable simpler, cross-border compliance that protects users and supports innovation and competitiveness.

1.1.1 Simplification Governance and Digital Omnibus Consolidation

This category captures broad, cross-sector support for the EU’s Digital Omnibus as a governance vehicle to consolidate and simplify the digital rulebook. Stakeholders from industry, finance, telecoms, energy, cities, and authorities emphasize reducing bureaucracy and administrative costs, harmonising definitions and reporting, and resolving overlaps across the acquis while preserving core objectives: protection, safety, security, fundamental rights, and user safeguards. The aim is greater legal certainty, proportionate and workable compliance, and improved competitiveness and innovation, with an implementation-and-simplification focus following the 2024 elections. The governance guidance embedded in the insights calls for a holistic fitness check across key frameworks (GDPR, ePrivacy, Data Act, Data Governance Act, AI Act, CRA, NIS2), swift negotiations for planning certainty, and fewer, clearer, and more cost-effective procedures. It stresses that guidelines should not replace law or mask ambiguity, that simplification must not lower standards, and that future-responsive monitoring and revision mechanisms are needed. Stakeholders note sector-specific priorities (e.g., streamlining incident reporting, telecom simplification), and flag risks and gaps such as insufficient ambition, slow progress, and controversial ideas like centralised consent management. The overarching aim is coherent, proportionate legislation that eases compliance without weakening protections and that delivers tangible benefits for consumers and businesses alike.

Docusign welcomes the European Commissions ambition to introduce a Digital Omnibus as part of a broader digital package to simplify the EU digital rulebook by reducing administrative costs, harmonising requirements, and increasing legal certainty for businesses without weakening user protections. (Docusign)

To be effective, the simplification package must take a holistic view across all digital legislation at the EU level: aligning legal definitions, harmonizing reporting requirements, and resolving overlaps through targeted and coherent adjustments: (Bitkom e.V.)

While we share the Commissions simplification objectives and welcome the intention to ease the administrative burdens and costs for businesses, we are alarmed by the prospect set out in the Call for Evidence to centralise consent management options. (EMMA-ENPA)

It is essential to recognize that while guidelines serve as valuable tools for illustrating the practical application of legal provisions, they must not be used to substitute areas of legal ambiguity or complexit (Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique)

: Highlights the EU's post-2024 shift toward implementation and simplification, signaling stronger governance focus on practical execution of the digital rulebook.

It was therefore a positive step that the EU Institutions drew the right lessons from the identified shortcomings and - after the 2024 European election - shifted their policy focus to "implementation and simplification".

FERMA - Federation of European Risk Managers Associations: Supports the simplification agenda as a positive signal for businesses, reinforcing confidence in streamlined governance.

FERMA welcomes this package as a positive signal for companies.

Verband kommunaler Unternehmen e.V.: Urges swift negotiations on simplification proposals to deliver planning and legal certainty, emphasizing effective governance and consolidation.

Simplification proposals should be followed by swift conclusions in negotiations in order to ensure planning and legal certainty.

SIEMENS AG: Criticizes the Digital Omnibus for lacking ambition and calls for less bureaucracy, clearer rules, and targeted support to truly simplify governance.

This Call for Evidence on the Digital Omnibus completely lacks the ambition European companies urgently need: less bureaucracy, clear and simple rules, and targeted political support.

City of Stockholm: Welcomes efforts to reduce administrative burdens in EU digital legislation, aligning with consolidation and practical simplification.

The City of Stockholm welcomes the European Commission's proposal to reduce administrative burdens within EU digital legislation.

TIC Council: Advocates efficient, proportionate legislation that simplifies without undermining protection, safety, or security, reflecting balanced governance.

TIC Council, the international trade association representing the independent Testing, Inspection and Certification (TIC) sector, sees the Digital Omnibus as an opportunity to promote efficient and proportionate legislation, without compromising the core policy objectives of protection, safety, and security.

ZVEI e.V.: Backs the Commission's drive to simplify and streamline EU digital regulation, supporting harmonized governance.

ZVEI welcomes this consultation and fully supports the European Commissions efforts to simplify and streamline EU digital regulation.

Kaspersky Labs Limited: Supports reducing compliance costs while preserving core regulatory objectives, aligning simplification with resilient governance.

Kaspersky, a global cybersecurity company committed to supporting secure and resilient digital infrastructure across the EU and globally, welcomes the European Unions efforts to reduce the administrative costs for compliance for businesses, administrations and citizens in the European Union in application of several regulations of the Unions digital acquis without compromising the objectives of the underlying rules.

CNIL (French Data Protection Authority): Welcomes preparatory discussions for an upcoming simplification package, indicating support for structured governance improvements.

We welcome the launch of discussions in preparation for the forthcoming simplification on the digital package expected by the end of this year.

Enel SpA: Endorses simplifying EU digital legislation while safeguarding fundamental rights and resilience, balancing consolidation with protections.

Enel, a leading multinational energy company, supports the European Commissions Digital Omnibus Package initiative aimed at simplifying EU digital legislation while safeguarding fundamental rights and enhancing digital resilience.

Technology Industries of Finland: Supports streamlining the digital policy framework and a comprehensive fitness check to consolidate and harmonize rules.

Technology Industries of Finland welcomes the European Commission's initiative to streamline the EU's digital policy framework through the Digital Package for Simplification, including a comprehensive fitness check of the existing legislative acquis.

PHOENIX group: Welcomes a forward-looking simplification agenda designed to deliver immediate relief for businesses through clearer governance.

PHOENIX group welcomes the Commissions initiative aimed at setting digital simplification agenda for the years to come and bringing immediate relief to businesses across the EU.

Workday: Strongly supports the Digital Omnibus to refine cybersecurity, AI, and data frameworks, boosting coherence and practical implementation.

Workday strongly supports the European Commission's simplification agenda, including the planned Digital Omnibus to enhance cybersecurity, artificial intelligence and data frameworks.

CGI Inc.: Endorses efforts to simplify and harmonize the digital regulatory landscape for clearer, consolidated governance.

We welcome the European Commissions efforts to simplify and harmonise the digital regulatory landscape.

Docusign: Backs a Digital Omnibus to reduce costs, harmonize requirements, and increase legal certainty without weakening user protections.

Docusign welcomes the European Commissions ambition to introduce a Digital Omnibus as part of a broader digital package to simplify the EU digital rulebook by reducing administrative costs, harmonising requirements, and increasing legal certainty for businesses without weakening user protections.

EFPIA: Welcomes simplification and streamlining of Europe’s digital rulebook to enhance coherence and manageability.

The European Federation of Pharmaceutical Industries Associations (EFPIA) welcomes the Commissions efforts to simplify and streamline Europes digital rulebook.

Digital Poland Association: Notes limited progress on simplifying digital rulebooks and calls for acceleration of consolidation efforts.

A year has passed since the publication of the report but little progress has been made in simplifying digital rulebooks.

Volkswagen Group: Supports the Commission's plan to streamline and simplify digital regulation via the Digital Omnibus.

In this context, the Volkswagen Group strongly welcomes the European Commission's announcement of the Digital Om- nibus (Digital Package on Simplification), which aims to streamline and simplify digital regulation.

EMMA-ENPA: Supports simplification but warns against centralising consent management, emphasizing governance that avoids new risks.

While we share the Commissions simplification objectives and welcome the intention to ease the administrative burdens and costs for businesses, we are alarmed by the prospect set out in the Call for Evidence to centralise consent management options.

European Energy Information Sharing and Analysis Centre: Welcomes the Digital Package as a timely step to simplify and harmonize the EU's digital regulatory landscape.

The European Energy Information Sharing and Analysis Centre (EE-ISAC) welcomes the European Commission's Digital Package and Omnibus initiative as a timely and necessary step toward simplifying and harmonising the EU's digital regulatory landscape.

FEBIS: Appreciates the call for evidence and simplification effort to improve the EU digital framework's coherence.

FEBIS members welcome the call for evidence on the Digital Omnibus and appreciate the effort to simplify the EU digital framework.

ALFI - Association of the Luxembourg Fund Industry: Supports simplifying and streamlining the digital regulatory framework for clearer governance.

ALFI welcomes the initiative from the Commission to simplify and streamline the Digital Regulatory framework.

Dun & Bradstreet: Backs the ambition to simplify and harmonize the EU's digital regulatory landscape through the Omnibus.

Dun & Bradstreet (D&B) supports the European Commission's ambition to simplify and harmonise the EUs digital regulatory landscape through the Digital Omnibus initiative.

Unipol Assicurazioni S.p.A.: Welcomes the plan to simplify digital regulations through a Digital Omnibus initiative.

Unipol Group (hereinafter "Unipol") welcomes the European Commission's plan to simplify digital regulations with a "Digital Omnibus" initiative.

Eurofinas: Strongly supports streamlining and simplifying through the Digital Omnibus and a Digital Fitness Check to enhance coherence.

We strongly support the European Commission's ambition to streamline and simplify the EU's digital rulebook through the Digital Omnibus and the forthcoming Digital Fitness Check.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Warns that guidelines should not replace legal clarity, urging governance that resolves ambiguity through law, not guidance.

It is essential to recognize that while guidelines serve as valuable tools for illustrating the practical application of legal provisions, they must not be used to substitute areas of legal ambiguity or complexit

Video Games Europe: Supports reducing regulatory fragmentation and promoting simplification for consistent governance across the EU.

Video Games Europe welcomes measures aimed at reducing regulatory fragmentation and promoting simplification.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Welcomes the Omnibus as overdue to make the digital rulebook workable for innovation through practical simplification.

The German Al Association welcomes the European Commission's Digital Omnibus initiative as a long-overdue opportunity to make the EU's digital rulebook workable for innovation.

Telefonica, S.A.: Supports simplifying the EU's digital regulatory framework to enhance clarity and manageability.

Telefónica welcomes the European Commissions Digital Omnibus initiative to simplify the EUs digital regulatory framework.

Snap Inc.: Highlights that dense legal drafting creates compliance uncertainty, urging clearer, simpler governance and guidance.

Though well-intentioned, these rules are written in dense legal terms, leaving companies uncertain about what compliance requires.

Bitkom e.V.: Calls for a holistic simplification: align definitions, harmonize reporting, and resolve overlaps via targeted adjustments.

To be effective, the simplification package must take a holistic view across all digital legislation at the EU level: aligning legal definitions, harmonizing reporting requirements, and resolving overlaps through targeted and coherent adjustments:

Association française de normalisation (AFNOR): Sees the Omnibus as an opportunity to cut costs, increase coherence, and foster innovation, security, and competitiveness.

The Omnibus offers a chance to reduce administrative costs, bring greater coherence, and ensure that Europes regulatory framework fosters innovation, security, and competitiveness.

German Social Insurance European Representation: Welcomes simplifying and harmonising existing digital legislation via the Digital Omnibus.

The German Social Insurance Agency (DSV) welcomes the European Commission's initiative to simplify and harmonise existing digital legislation with the Digital Omnibus.

Verisure: Supports simplifying and rationalising digital legislation through the Digital Package and Omnibus.

Verisure welcomes the European Commission's initiative to simplify and rationalise the EU's digital legislation through the Digital Package and forthcoming Digital Omnibus.

Seznam.cz, a.s.: Critiques the scope of the review for omitting the DSA, urging inclusion for comprehensive simplification.

Unfortunately, the Digital Services Act (DSA) is not among the digital regulations identified by the Commission for review.

Trellix: Advocates harmonised terms and consolidated processes to reduce the regulatory maze and free resources for security.

In summary, greater harmonisation of terms and consolidation of processes will reduce the regulatory maze that companies navigate, freeing up resources to focus on actual security improvements.

ENGIE: Welcomes the Digital Omnibus initiative and the chance to contribute to simplification efforts.

ENGIE welcomes the European Commissions initiative of a Digital Omnibus and values the opportunity to provide its views on this simplification effort.

BEUC - The European Consumer Organisation: Urges that simplification account for consumer benefits and prior compliance investments, ensuring outcomes for users.

We also need to highlight that many companies have already made investments to comply with the existing regulatory framework, and it is paramount that the Commission factors in its assessment the economic benefits of legislation for consumers and how simplification can deliver for them.

European Express Association (EEA): Supports continued simplification and streamlining to enable innovation, competitiveness, and efficiency.

The EEA welcomes the Commission's continued commitment to simplifying and streamlining the EU's digital regulatory landscape, which plays a central role in enabling innovation, competitiveness, and efficiency across the European economy.

LSEG: Views the Omnibus as a timely opportunity to simplify the EU digital regulatory framework.

LSEG welcomes the European Commissions Digital Omnibus initiative as a timely opportunity to simplify the EUs digital regulatory framework.

Democracy Reporting International (DRI): Supports a digital regulatory framework that balances interests for all stakeholders through sensible governance.

We support a digital regulatory framework for the benefit of all involved.

TEAM-NB: Welcomes simplifying the digital framework and cutting administrative costs for businesses via the Omnibus.

Team NB, as notified bodies association, welcomes the Commission's initiative to drive forward the simplification of the digital regulatory framework and reduce administrative costs for businesses as part of the Digital Omnibus.

Ibec: Urges evidence-based regulation, introducing new rules only where genuine gaps exist to avoid unnecessary burden.

In order to achieve this, any new regulation must be carefully considered and introduced only where regulatory gaps are proven.

Namirial Spa: Calls for radical simplification and coherence that reduce burdens, foster innovation, and sustain new digital services.

Attached the position of Namirial who calls for radical simplification, greater regulatory coherence, and an approach that fosters innovation and European competitiveness by reducing compliance burdens and promoting the sustainability of new digital services.

AIM - European Brands Association: Welcomes plans to simplify rules on data, cybersecurity, and AI in the Digital Omnibus.

We welcome the European Commission's initiative to simplify rules on data, cybersecurity, and artificial intelligence in the upcoming Digital Omnibus.

Emerson Electric Co.: Supports swift burden reduction, focusing on data legislation, cybersecurity reporting, and targeted AI Act adjustments.

Emerson supports the European Commission's objective to introduce measures that swiftly reduce the regulatory burden on businesses, particularly in the areas of "data legislation, cybersecurity incident reporting, and targeted adjustments to the Artificial Intelligence Act".

Schneider Electric: Highlights overlapping laws and standards that complicate implementation, endorsing simplification for a trusted environment.

Schneider Electric welcomes the European Commission's willingness to simplify the European digital regulatory acquis, which has been complexified by overlapping legislations and standards to the detriment of an effective implementation and the development of a trusted environment.

Meta Platforms Ireland Limited: Warns that proliferating regulators and complex laws harm competitiveness, urging consolidation and clearer rules.

As highlighted by former European Central Bank President Mario Draghi, the multiplication of digital regulators, the accumulation of EU-level legislation, its increased complexity, and the challenges companies face in implementing the rules are having a detrimental impact on Europes competitiveness.

The Danish Chamber of Commerce: Supports the Commission's simplification agenda and welcomes the Digital Omnibus effort.

The Danish Chamber of Commerce/Dansk Erhverv support the European Commissions ambitions on the simplification agenda and welcomes the initiative on the Digital Omnibus, as outlined in the Call for Evidence published on September 16, 2025 (Ref. Ares(2025)7724296).

Finnish Food and Drink Industries´ Federation (ETL): Backs streamlining and reducing unnecessary burdens, noting disproportionate complexity in the food sector.

We strongly support the Commission's efforts to streamline digital regulation and reduce unnecessary administrative burdens, particularly in the context of the food sector, where the regulatory framework has become disproportionately complex in relation to technological development.

Adigital (Asociación Española de la Economía Digital): Provides concrete, technical proposals across 13 areas to support the EU's simplification agenda.

In this exercise, the first of its kind in Spain, we set out 13 legislative areas with technical, concrete, and feasible proposals to accompany and support European efforts on simplification.

Vodafone Group: Argues that simplifying telecom rules will spur innovation and investment across the ecosystem.

Simplifying rules in telecoms creates a wider opportunity to boost innovation and investment across the ecosystem.

ING Group: Offers banking-specific recommendations to simplify the digital regulatory framework for practical governance.

This response provides INGs key recommendations to simplify the digital regulatory framework in key areas for the banking sector.

Entrust SAS: Suggests adjustments that lower compliance costs without compromising security or individual rights.

Together, these adjustments would significantly reduce unnecessary compliance costs without compromising security or rights of individuals.

FiCom ry: Points to overlapping and contradictory requirements that need simplification for coherent governance.

There are overlapping and contradictory regulatory requirements needing simplification.

: Welcomes the EU initiative to simplify and modernise its digital acquis from an international perspective.

The African Union, through STRC and ASRIC, welcomes the EU's initiative to simplify and modernise its digital acquis.

Union of Entreprenuers and Employers: Advocates simplification focused on procedural coherence, not lowering substantive standards.

Simplification should aim for procedural coherence rather than lowering standards.

Anitec-Assinform: Supports practical simplification that upholds trust and security while enabling a thriving digital economy.

We support the Commission's simplification agenda and have prepared feedback focused on practical solutions that uphold the EU's trustworthiness and security objectives while fostering a thriving digital economy.

European AI Forum: Proposes measures to align AI, data, privacy, and cybersecurity laws for proportional, clear, and competitive governance.

Our submission outlines concrete simplification measures to improve coherence between the AI Act, GDPR, ePrivacy, Data Act and Data Governance Act, CRA and NIS-2, ensuring proportionality, legal clarity and stronger competitiveness of European AI companies.

: Notes the Commission's programme to simplify, harmonise, and adapt digital frameworks to users' needs.

With the Digital Package – Digital Omnibus, the European Commission has launched a programme to simplify, harmonise and adapt EU digital regulatory frameworks to the needs of citizens and businesses.

2Dyles Services: Insists simplification produce fewer, clearer, more cost-effective procedures rather than new layers of requirements.

It is essential to ensure that simplification results in fewer, clearer, and more cost-effective procedures, rather than adding layers of requirements that complicate the system.

WKÖ - Austrian Federal Economic Chamber: Emphasizes simplification as a core objective of the EU's digital governance agenda.

The second objective is simplification.

ACEA (European Automobile Manufacturers' Association): Welcomes the goal to simplify and streamline the EU's digital legal framework via the Omnibus.

For these reasons, ACEA welcomes the Commission's objective to simplify and streamline the EU digital legal framework through a Digital Omnibus Package.

UNIFE: Supports the announced simplification package to help European companies remain competitive.

UNIFE welcomes the announcement from Executive Vice-President Virkkunen of her simplification package for digital regulation, the so-called Digital Omnibus with initiatives to simplify EU regulation to allow European companies to remain competitive.

: Argues for future-responsive law with monitoring and revision mechanisms, not just fewer rules.

EU digital regulation can be simplified not simply by reducing the number of rules, but also by introducing clear mechanisms for monitoring and revision, moving from future-proof to future-responsive law.

: Stresses that expanding AI, data protection, and cybersecurity frameworks require simplification for clarity and implementation.

As AI, data protection, and cybersecurity frameworks expand rapidly, simplification is essential for both legal clarity and effective implementation.

: Sees the Digital Package and Omnibus as an opportunity to reorganise and simplify digitalisation.

With the Digital Package and the Omnibus initiative, the EU has the opportunity to reorganise and simplify digitalisation.

American Chamber of Commerce to the EU: Highlights regulatory burdens as a top business barrier, underscoring the need for meaningful simplification.

Regulatory burdens are a top concern for businesses in Europe, with 84% of American Chamber of Commerce to the EU (AmCham EU) members citing them as a primary barrier.

CECE - Committee for European Construction Equipment: No substantive excerpt was provided to summarize this document's position on simplification governance.

iProov Ltd: No substantive excerpt was provided to summarize this document's position on simplification governance.

FEDIL, the Voice of the Luxembourg's Industry: No substantive excerpt was provided to summarize this document's position on simplification governance.

Uber B.V.: Supports the EU's simplification agenda, endorsing streamlined digital governance.

Uber supports the EU simplification agenda.

1.1.2 Unified Definitions, Scope and Taxonomy

Stakeholders call for a unified, horizontal set of definitions and a common taxonomy across the EU digital rulebook to eliminate ambiguity, overlaps, and conflicting obligations. Vague or divergent terms (for example, around ICT services, "main establishment," or service typologies) are driving misinterpretations, inconsistent enforcement, and costly compliance debates across frameworks such as DORA, NIS2, the Data Act, the DSA/P2B, the AI Act, and the CRA. They advocate aligning key concepts and scoping criteria across instruments—e.g., a common definition of "significant incident" across NIS2/DORA; harmonized data-acquis terminology (DGA/FFNPDR/Open Data) alongside EU-wide passporting for data intermediaries; and removing overlapping or duplicative requirements (such as international data transfer rules that conflict with GDPR). Clarity should reflect business models (e.g., platform due-diligence duties), user roles (commercial vs private individuals), and sectoral interfaces (e.g., private entities providing public services). Product lifecycle realities also require precise scoping—for instance, defining "placing on the market" consistently across the CRA and sectoral TSIs, and at product-model/type level for long development cycles. Clear service identification and scope boundaries help providers determine the correct regime from the outset and support a genuinely harmonized, predictable compliance environment.

Clearly defining the scope and key terms of a regulation is fundamental. (Schneider Electric)

There remain several ongoing misinterpretations around the adopted definitions across the various legislative acts. (Emerson Electric Co.)

Clarify placing on the market for long development cycles, defining it at product-model or type level rather than each unit, consistent with Union harmonisation law. (Technology Industries of Finland)

Within the data acquis, align key definitions across DGA/FFNPDR/Open Data and introduce EUwide passporting for DGAregistered data intermediation services, while reaffirming tradesecret and security safeguards. (Panasonic Europe B.V.)

FERMA - Federation of European Risk Managers Associations: Advocates narrowing and clarifying the definition of connected product to limit scope and avoid overlap with GDPR, ensuring a consistent regulatory regime.

Narrowing and clarifying the definition of 'connected product' to narrow its scope and remove international transfer requirements that overlap with the GDPR, thereby creating a more consistent regime.

SIEMENS AG: Urges a horizontal, unified CRA approach covering all products to standardize cybersecurity obligations.

It is essential that the CRA horizontally regulates the cybersecurity of all covered products.

Assuralia: Notes that unclear definitions of ICT services cause inconsistent interpretations and disputes, creating uncertainty about whether DORA or Solvency II applies.

unclear definitions of "ICT services" and "ICT services supporting critical or important functions" lead to inconsistent interpretations and disputes with vendors, as well as internal discussion on which a legal regime is applicable (DORA or Solvency II).

Enel SpA: Highlights ambiguity in FRIA scope regarding private entities providing public services and calls for clearer delineation.

Article 27 (1) states that "private entities providing public services" are required by the FRIA.

Technology Industries of Finland: Calls to harmonize and define placing on the market at model or type level to accommodate long development cycles.

Clarify placing on the market for long development cycles, defining it at product-model or type level rather than each unit, consistent with Union harmonisation law.

FEBIS: Seeks clear differentiation between professional or commercial actors and private individuals across EU frameworks.

Regulatory EU frameworks should clearly distinguish between individuals acting in a commercial or professional capacity and those acting as private individuals.

German Insurance Association: Reports that DORA's broad ICT-services definition has caused practical difficulties, indicating need for tighter scoping.

DORA's broad ICT-services definition has already led to numerous time-consuming discussions and difficulties in practice.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Points to vague and conflicting AI Act terminology vis-à-vis other EU digital rules, urging clarity and alignment.

Lastly, the entire AI Act still contains several unclear and vague terminology, which in some cases even conflicts with other EU digital regulations.

GSMA: Welcomes Commission guidance but emphasizes further definitional work for clear, comprehensive Data Act implementation.

While Connect Europe and the GSMA laud the efforts carried out to date by the European Commission, particularly with respect to the Data Act FAQ, there are still several aspects that require further work in order to support a clear and comprehensive implementation of the Data Act.

Government Office of the Czech Republic: Identifies inconsistencies between the P2B Regulation and the DSA that warrant harmonization of definitions and scope.

There are differences between the P2B Regulation and the DSA.

Seznam.cz, a.s.: Stresses the need for clear service taxonomy so providers can correctly identify their service type for compliance.

To prepare for compliance with the regulation, service providers must be able to correctly identify the type of service they are providing.

Trellix: Flags divergent main establishment definitions that complicate cross-border compliance and require alignment.

Definitions of "main establishment" also differ, complicating cross- border compliance.

Emerson Electric Co.: Observes ongoing misinterpretations of adopted definitions across legislative acts, underscoring the need for uniformity.

There remain several ongoing misinterpretations around the adopted definitions across the various legislative acts.

Schneider Electric: Emphasizes that clearly defined scope and key terms are foundational to effective regulation.

Clearly defining the scope and key terms of a regulation is fundamental.

Adigital (Asociación Española de la Economía Digital): Requests clear, business-model-based delineation of platforms' due diligence obligations.

Clarify the scope of the "due diligence" required from platforms based on their business model.

Panasonic Europe B.V.: Advocates aligning key definitions across DGA, FFNPDR, and Open Data and enabling EU-wide passporting with strong safeguards.

Within the data acquis, align key definitions across DGA/FFNPDR/Open Data and introduce EUwide passporting for DGAregistered data intermediation services, while reaffirming tradesecret and security safeguards.

Union of Entreprenuers and Employers: Promotes a common cross-framework definition of significant incident across NIS2, DORA, and sectoral rules.

Common definitions of what qualifies as a "significant incident" across NIS2, DORA, and sectoral frameworks would help reduce ambiguity.

European AI Forum: Highlights unclear AI Act terminology and conflicts with other digital regulations, calling for harmonization.

Lastly, the entire AI Act still contains several unclear and vague terminology, which in some cases even conflicts with other EU digital regulations.

UNIFE: Calls for consistent understanding of placing on the market across CRA and TSI.

It needs to be safeguarded that the CRA and TSI definitions are understood similarly regarding the term "placing on the market".

FEDIL, the Voice of the Luxembourg's Industry: No specific insight on unified definitions, scope and taxonomy was provided in the available text.

1.1.3 Legal Hierarchy, Lex Specialis and Conflict Resolution

Stakeholders across sectors call for a clear legal hierarchy and explicit conflict-resolution principles (e.g., lex specialis, mutual recognition) to reconcile overlaps among horizontal and sector-specific EU digital laws. They highlight inconsistent and duplicative obligations—such as divergent reporting duties across the CRA, NIS2, and GDPR, and tensions between the GDPR and the Data Act—that generate legal uncertainty, inefficiency, and even make some legislative goals unattainable. Proposed fixes include ensuring horizontal rules defer to sectoral regimes where appropriate, recognizing compliance under one framework as sufficient under another (e.g., DORA as a lex specialis baseline), and repealing or amending redundant provisions (e.g., ePrivacy vis-à-vis GDPR; specific Data Act articles duplicating GDPR Chapter V). Stakeholders also urge tighter alignment of definitions and scope (e.g., “related service”), streamlined reporting, and a coherent, innovation-friendly approach under the Digital Omnibus that removes overlaps while safeguarding fundamental rights and security.

The digital regulatory ecosystem in the EU is characterized by increasing complexity due to the lack of a clear hierarchy among different regulatory frameworks such as the Unfair Commercial Practices Directive (UCPD), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the General Data Protection Regulation (GDPR). (Adigital (Asociación Española de la Economía Digital))

Avoiding duplication: Ensure horizontal rules do not unnecessarily overlap with existing sector-specific requirements. (Dun & Bradstreet)

It overlaps with the GDPR and the Data Act, leading to contradictions and inefficiencies and, in the case of the Data Act, impossibility to achieve its legislative goals. (Volkswagen Group)

We propose repealing the ePrivacy Directive, as the GDPR already provides a robust and uniform legal basis for personal data protection, with the principle of confidentiality of communications incorporated directly into the GDPR itself. (Anitec-Assinform)

Verband kommunaler Unternehmen e.V.: Points out inconsistent reporting obligations across CRA, NIS-2, and GDPR, underscoring the need for clear hierarchy and conflict-resolution rules. Calls for harmonisation to avoid contradictory compliance duties.

The requirements are not always consistent: for example, reporting obligations are regulated differently in the Cyber Resilience Act, the NIS-2 Directive, and the GDPR.

City of Stockholm: Supports EU-level harmonisation from a municipal perspective to reduce fragmentation and conflicting requirements. Emphasizes the value of a coherent legal hierarchy.

From a municipal perspective, the Commission's intention of harmonising EU legislation is positive.

Volkswagen Group: Warns that overlaps between new rules and GDPR/Data Act create contradictions and inefficiencies that can undermine legislative objectives. Advocates resolving conflicts through clearer precedence and streamlined scopes.

It overlaps with the GDPR and the Data Act, leading to contradictions and inefficiencies and, in the case of the Data Act, impossibility to achieve its legislative goals.

Dun & Bradstreet: Recommends preventing duplication by aligning horizontal rules with sector-specific regimes. Suggests applying lex specialis so sector rules prevail where appropriate.

Avoiding duplication: Ensure horizontal rules do not unnecessarily overlap with existing sector-specific requirements.

German Insurance Association: Proposes deeming compliance with DORA sufficient to meet overlapping obligations, reducing bureaucracy. This reflects a lex specialis approach to conflict resolution.

It would contribute to simplification and less bureaucracy if compliance with DORA requirements is regularly sufficient in these cases.

GSMA: Welcomes the Digital Omnibus as a vehicle to simplify and align data, cybersecurity, and AI rules. Urges transversal solutions that clarify overlaps and ordering among frameworks.

Connect Europe and the GSMA, representing the European telecommunication sector, welcome the opportunity to comment on the European Commission's 'Digital Omnibus' and to offer our views on how this initiative can help to simplify the regulatory landscape related to data, cybersecurity and artificial intelligence.

Siinda: Supports the Commission’s effort to simplify and modernise EU digital rules while safeguarding rights, competition, and innovation. Endorses coherent conflict-resolution principles across the rulebook.

Siinda members welcome the Commissions Call for Evidence on the Digital Omnibus and the opportunity to help simplify and modernise EU digital rules while preserving fundamental rights, competition and innovation.

Bitkom e.V.: Advocates retaining the regime for data altruism organizations within any simplification effort. Highlights the need to preserve specific constructs while clarifying hierarchy to avoid conflict.

Retain the concept of data altruism organizations.

Ibec: Calls for precise scoping (e.g., defining 'related service') so only necessary software falls under obligations. Clear definitions help prevent overlap and resolve conflicts between regimes.

Clarify a 'related service'xii - only the software that is needed for the functioning of the product should be considered.

Schneider Electric: Sees the simplification package as an opportunity to set transversal principles that eliminate inconsistencies and overlaps. Encourages clarifying precedence across intersecting regulations.

The Digital Simplification Package represents an opportunity to achieve transversal simplification through key principles and to clarify inconsistencies and overlaps between regulations.

Finnish Food and Drink Industries´ Federation (ETL): Argues certain Data Act provisions duplicate GDPR cross-border transfer rules and should be removed. Prefers relying on existing lex specialis to avoid redundant obligations.

Articles 32 and 28(1)(b) of the Data Act should be removed due to their redundancy with Chapter V of the GDPR.

Adigital (Asociación Española de la Economía Digital): Identifies the absence of a clear hierarchy among UCPD, DSA, DMA, and GDPR as a driver of complexity. Calls for explicit ordering and conflict-resolution rules across these frameworks.

The digital regulatory ecosystem in the EU is characterized by increasing complexity due to the lack of a clear hierarchy among different regulatory frameworks such as the Unfair Commercial Practices Directive (UCPD), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the General Data Protection Regulation (GDPR).

ING Group: Notes conflicts from cross-framework data-sharing mandates (e.g., PSD2, AML, IPR), creating compliance friction. Urges alignment and precedence rules to reconcile overlapping requirements.

Problems arise when data sharing is required under other frameworks, including (but not limited to) PSD2, AML, IPR (Verification of Payee).

Anitec-Assinform: Proposes repealing the ePrivacy Directive because GDPR already provides a uniform basis for communications confidentiality. Seeks to remove overlap by consolidating under a single framework.

We propose repealing the ePrivacy Directive, as the GDPR already provides a robust and uniform legal basis for personal data protection, with the principle of confidentiality of communications incorporated directly into the GDPR itself.

ACEA (European Automobile Manufacturers' Association): Requests a coherent data-sharing framework aligned with the Data Act that eliminates overlaps and excessive reporting. Emphasizes streamlined obligations through clear hierarchy.

ACEA urges a coherent, innovation-friendly EU data sharing framework aligned with the Data Act, eliminating overlaps and excessive reporting.

: Advocates sunsetting or repealing overlapping legislation when it becomes redundant. Supports continuous pruning to maintain a coherent, conflict-free rulebook.

Remove any overlapping legislation when it is no longer needed.

: No specific information was provided in the supplied content regarding legal hierarchy, lex specialis, or conflict-resolution.

1.1.4 Cross-Regulation Alignment and Single Market Coherence

Stakeholders across sectors describe a sprawling EU digital rulebook that has evolved in silos, producing inconsistent definitions, overlapping obligations, and fragmented national implementation. They call for cross-regulation alignment across AI, data, cybersecurity, privacy, and sectoral regimes, treating new instruments like the AI Act as maximum-harmonisation measures and integrating obligations through existing frameworks to avoid duplicate assessments. Core Single Market principles—country-of-origin, mutual recognition, and a ban on national gold-plating—should be reaffirmed, with data localisation discouraged in favor of a coherent European approach. To restore competitiveness and innovation while safeguarding consumers, contributors urge codification and clarification of interfaces among the DSA, DMA, GDPR, NIS2, Data Act/Governance, EHDS, and payments rules; alignment of documentation and conformity processes with established certification schemes; and practical guidance for consistent enforcement across Member States. A risk-based, innovation-friendly simplification should remove illogical or duplicative requirements, reduce compliance costs (especially for SMEs and cross-border operators), and enable wider adoption of advanced technologies, all while maintaining high protection standards and supporting resilience and fair competition.

Enhance legal coherence across AI, Data, Cybersecurity, and Privacy legislation. (ZVEI e.V.)

Reaffirm the country-of-origin principle to preserve the integrity of the Single Market and avoid national goldplating. (Bolt)

The current payments industry security practices have proven successful in minimizing fraud rates over the past three decades to as low as 0.031% of the total value of card payments in the EU. (Mastercard Europe SA)

Accelerated harmonisation and reduced compliance barriers for African innovators accessing EU markets. ()

SIEMENS AG: Calls for streamlining EU digital rules, arguing excessive regulatory burden is harming competitiveness and innovation.

The immense regulatory burden stifles competitiveness and pace of innovation of European tech companies: every day, we are losing ground to the USA and China!

ZVEI e.V.: Urges cross-regulatory coherence across AI, data, cybersecurity and privacy laws to reduce fragmentation.

Enhance legal coherence across AI, Data, Cybersecurity, and Privacy legislation.

Kaspersky Labs Limited: Advocates aligning the AI Act's documentation and conformity assessments with existing cybersecurity certifications to avoid duplication.

We also encourage the Commission to align the Al Act's documentation and conformity assessment requirements with existing cybersecurity certification schemes to avoid duplication and ensure consistency across regulatory frameworks.

Enel SpA: Supports maximum harmonisation to prevent regulatory fragmentation across the Single Market.

Advocacy for maximum harmonization to avoid regulatory fragmentation.

Zimmer Biomet: Backs a coherent, innovation-friendly digital rulebook that balances growth with clear, consistent obligations.

We support a bold, coherent, and innovation-friendly approach to digital regulation.

eco - Verband der Internetwirtschaft e.V.: Opposes national data localisation and calls for a unified Single Market approach to data rules.

Provisions for data localisation through national legislation should still be considered critical and abandoned in favour of a European Single Market approach.

European Energy Information Sharing and Analysis Centre: Warns that overlapping and fragmented requirements in the energy sector divert resources from core security and resilience, underscoring the need for alignment.

As digitalisation deepens in the energy sector, the complexity and fragmentation of overlapping regulatory requirements pose operational challenges that risk diverting resources from core security and resilience functions.

FEBIS: Highlights divergent treatment of sole traders across Member States as a source of fragmentation requiring alignment.

The definition and treatment of sole traders vary across EU Member States, influencing their legal status, registration requirements, and inclusion in public registries.

France Digitale: Calls for a consistent, future-proof digital rulebook that fosters innovation, consumer protection, and fair competition across the EU.

The goal should be to establish a well-structured, consistent, and future-proof digital rulebook that fosters innovation, protects consumers, and upholds the principles of fair competition.

Dun & Bradstreet: Notes that key data and digital laws evolved in silos, creating inconsistent definitions, obligations, and enforcement across Member States.

The current data acquis including the Data Governance Act, Free Flow of Non-Personal Data Regulation, and Open Data Directive alongside key legislation such as the EU AI Act, EU GDPR, ESG ratings, credit, and anti-money laundering frameworks, have evolved in silos, resulting in inconsistencies in definitions, obligations, and enforcement across Member States.

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Points to a complex, potentially fragmented EU data legislation landscape that needs streamlining and coherence.

The current EU data legislation landscape (including the EHDS, Data Act, Data Governance Act, Free-Flow of Non-Personal Data Regulation, Open Data Directive and GDPR) is complex and potentially fragmented.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Identifies the need to better align and codify overlapping legal texts that address similar issues.

A review of the current and upcoming legislative corpus reveals a need for better aligning and codifying of certain legal texts that address similar questions.

German Insurance Association: Observes inconsistent regulatory treatment of insurers' third-party providers, indicating a need for cross-context alignment.

Regulatory treatment of insurance companies' use of third-party service providers varies by context.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Recommends using the AI Act as a maximum-harmonisation tool and integrating high-risk obligations via existing sectoral frameworks to avoid duplication.

We recommend treating the Al Act as a maximum-harmonisation instrument and integrate high-risk obligations for Annex I sectors through their existing frameworks, avoiding duplicated assessments and preserving established conformity routes.

Government Office of the Czech Republic: Flags incoherent scoping in the DSA that imposes illogical obligations on internet access providers, pointing to misalignment across rules.

Article 14 of the DSA also imposes an illogical obligation on providers of internet access services (as defined above) to include in their terms and conditions information about all policies, procedures, measures, and tools used for content moderation.

Telefonica, S.A.: Cautions that proliferating, poorly coordinated instruments and their unclear interplays risk undermining EU policy goals, urging simplification and coherence.

An overly complex regulatory landscape, marked by the proliferation of legislative instruments and their unclear and fragmented interplays, risks undermining the very objectives set out by the EU institutions.

Bitkom e.V.: Reports growing overlaps and inconsistencies—especially in definitions and obligations—during implementation of new digital laws.

As these new laws enter the critical phase of implementation, inconsistencies and overlaps, particularly in definitions and obligations, are becoming increasingly apparent.

Amazon: Describes complex, fragmented national rules that create a compliance maze, arguing for greater Single Market coherence.

Complex and fragmented regulations across EU member states create a maze of compliance requirements for businesses.

Association française de normalisation (AFNOR): Notes fragmentation of rules and supervisory practices across Member States as a key business challenge, calling for harmonisation.

One of the key challenges faced by businesses today is the fragmentation of rules and supervisory practices across Member States.

Verisure: Supports simplification and alignment but stresses that coherence must not weaken protection standards.

Simplification, however, must not lead to lower protection standards.

ENGIE: Details implementation hurdles from overlapping acts, unclear definitions, and inconsistent national processes in the energy sector, advocating alignment.

However, its implementation remains challenging and costly due to the proliferation and overlap of legislative acts and obligations, unclear definitions unsuitable for specific energy use-cases, inconsistent processes across Member States, and complex national governance structures.

Mastercard Europe SA: Urges that rulebook changes maintain coherence with proven payment security practices that have delivered very low fraud rates.

The current payments industry security practices have proven successful in minimizing fraud rates over the past three decades to as low as 0.031% of the total value of card payments in the EU.

Bolt: Calls to reaffirm the country-of-origin principle to prevent national gold-plating and preserve Single Market integrity.

Reaffirm the country-of-origin principle to preserve the integrity of the Single Market and avoid national goldplating.

Centre for Information Policy Leadership (CIPL): Welcomes EU efforts to enhance coherence and consistency across the digital rulebook.

CIPL commends the Commission's efforts to identify and address regulatory challenges in support of coherence and consistency across the EU's digital rulebook.

European Express Association (EEA): Argues that clearer, better-aligned rules will improve harmonised implementation by national authorities and strengthen the Single Market.

By enhancing clarity and alignment across the EU, the initiative can help national authorities and Member States achieve greater harmonization in implementation, thereby supporting the integrity of the Single Market.

Infosys Limited: Supports greater coherence across horizontal and sectoral rules to meet objectives at lower cost to businesses.

Infosys is supportive of the European Commissions ambition to achieve greater coherence across its multiple horizontal and sector specific rules, with the aim of reaching regulatory goals at lower cost for businesses.

LSEG: Notes that uncertainty and lack of harmonised rules deter deployment of advanced technologies, underscoring the need for clarity and alignment.

Institutions are hesitant to deploy advanced technologies - such as AI-driven screening, real-time analytics, and cross-border data solutions - without clear, harmonised rules.

Ibec: Advocates harmonisation and mutual recognition across Member States to reduce fragmentation.

Promote harmonisation and mutual recognition across Member States.

AIM - European Brands Association: Calls to prohibit gold-plating and ensure consistent application of digital rules across Member States to strengthen the Single Market.

The prohibition of gold plating and the consistent application of digital rules across all Member States to avoid fragmentation and strengthen the Single Market.

Emerson Electric Co.: Supports an approach that strengthens ICT ecosystem resilience while minimising overlapping regulatory obligations.

We believe this approach will enhance the resilience of the Information Communication Technologies (ICT) ecosystem while minimizing unnecessary regulatory overlap.

Meta Platforms Ireland Limited: Criticises the fragmented EU data regulatory environment for hindering innovation, far from a truly harmonised Digital Single Market.

Today, innovation in the EU is snarled up by a deeply fragmented data regulatory environment far from the harmonised Digital Single Market ("DSM") promised by policymakers.

The Danish Consumer Council: Supports the initiative to address fragmentation in the EU digital rulebook.

The Danish Consumer Council welcomes this consultation and supports the objective of addressing fragmentation in the EU digital rulebook.

Adigital (Asociación Española de la Economía Digital): Highlights duplicative, costly, and fragmented obligations across multiple EU and national regimes, advocating alignment and simplification.

The current regulatory ecosystem-including DAC7, DSA, VIDA, CESOP, and the forthcoming short-term rental regulation (EUSTRR)-has created a complex web of obligations resulting in duplications, high costs, and fragmentation between Member States.

Vodafone Group: States that EU cybersecurity regulation is fragmented and overly complex, calling for consolidation and coherence.

The EU cybersecurity regulatory landscape is fragmented and overly complex.

Almega: Welcomes the digital omnibus initiative aimed at simplifying and aligning existing legislation.

Almega welcomes the digital omnibus and its aim to simplify existing legislation.

FiCom ry: Argues telecom rules have become overly complex relative to technological change, urging simplification and regulatory coherence.

For example, the current regulatory framework for telecommunications has become far too complex compared to the pace of technological development.

: Calls for accelerated harmonisation and lower compliance barriers to ease EU market access for African innovators.

Accelerated harmonisation and reduced compliance barriers for African innovators accessing EU markets.

Union of Entreprenuers and Employers: Points to rising cumulative administrative burdens from recent digital laws, supporting simplification and better alignment to reduce costs.

According to the European Commission's Better Regulation agenda and accompanying impact assessments, the cumulative administrative burden of recent digital legislation, such as the GDPR, the Digital Services Act, the Digital Markets Act, and the NIS2 Directive, has risen markedly since 2018.

European Associations of Co-operative Banks (EACB): Urges simplification and clarification of data rules to sustain competitiveness and unlock the EU data economy.

Simplifying and clarifying the regulatory framework for data is crucial to ensuring that Europe maintains competitiveness and that companies can effectively contribute to, and benefit from, the EU data economy.

ACEA (European Automobile Manufacturers' Association): Warns that overlapping, fragmented rules and inconsistent national implementation sap innovation and competitiveness, calling for harmonisation.

However, manufacturers face a complex, fragmented EU digital framework with overlapping rules and inconsistent national implementation, diverting resources from innovation and weakening competitiveness.

AI & Partners B.V.: Requests clear guidance on how the AI Act interfaces with data protection, product safety, cybersecurity, and sectoral law to avoid duplication.

Concise clarifications on how the AI Act interacts with data protection, product safety, cybersecurity and sectoral law would help avoid duplicative burdens.

Doctrine: Identifies regulatory fragmentation as the main barrier, underscoring the need for coherent, harmonised rules.

Fragmentation is the primary obstacle.

1.1.5 Standards, Interoperability and Specifications Governance

This category urges a coherent, standards-led governance approach to simplify the EU's digital rulebook. Stakeholders call to align definitions, metadata and data standards across horizontal and sectoral laws (AI Act, GDPR/ePrivacy, CRA, DGA/Data Act, NIS2, DORA, eIDAS, etc.), reduce duplicative transparency and reporting duties, and rely on harmonised international and European standards (ISO, CEN/CENELEC) as evidence of compliance across multiple acts. The aim is to curb fragmentation across Member States, lower administrative costs—especially for SMEs—and focus oversight on risk and critical functions. Interoperability and specifications governance should be enabled through common, technology-neutral standards and clear terminology, not proliferating new bespoke specifications. Proposals include unified, risk-based AI labelling and common metadata schemes, a single harmonised disclosure that satisfies overlapping obligations, and modular, one-audit procedures that recognise cross-regime results (e.g., CRA security evaluations counting toward AI Act safety). Maintaining a harmonised approach to ESA RTS/ITS drafting and preserving the European Standardisation System's role are seen as key to consistent implementation, better user understanding, and scalable, future-proof compliance.

Recognise harmonised technical standards (e.g. ISO, CEN/ CENELEC) as evidence of compliance across multiple acts. (European AI Forum)

Unify transparency obligations across the Al Act, GDPR and ePrivacy. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Integrate CRA and Al Act assessments into a single modular procedure with one audit and one certificate. (European AI Forum)

Results of a CRA security evaluation should automatically count towards AI Act safety requirements where applicable. (European AI Forum)

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Calls to unify transparency and labelling obligations across the AI Act, GDPR and ePrivacy, using risk-based output labelling and common metadata standards to reduce duplication and costs.

The Commission should support the creation of common metadata and labelling standards for AI outputs to enable consistent and scalable compliance.

Government Office of the Czech Republic: Proposes harmonised EU definitions and data standards, with interoperable metadata frameworks to enable seamless public-sector data sharing and reuse.

Ensuring alignment, or at least interoperability, between these standards is essential to enable seamless data sharing and reuse across public administrations.

Amazon: Advocates digital simplification by harmonising compliance requirements and preserving the European Standardisation System to cut administrative burdens, especially for SMEs.

Harmonising compliance requirements across frameworks will reduce administrative burdens, allow organisations to focus on security and service delivery rather than regulatory complexity and ensure consistent enforcement across the EU.

National Land Survey of Finland: Urges reliance on existing cybersecurity and data protection standards, simplifying overlapping frameworks to reduce repeated assessments and administrative burden.

The National Land Survey of Finland recommends EU to rely on existing standards in all regulation to promote regulatory consistency and reduce the administrative burden on authorities.

Panasonic Europe B.V.: Highlights the costs of fragmentation and the benefits of coherent, standards-led rules at EU scale.

Operating at EU scale, we see both the cost of regulatory fragmentation and the upside from coherent, standardsled rules.

ING Group: Stresses maintaining a harmonised approach to ESA-level RTS/ITS drafting to ensure consistent technical standards.

We do note the importance of keeping the harmonised approach while drafting RTS/ITS at the ESAs level.

European AI Forum: Recommends unified, standards-based compliance, integrating evaluations across acts and recognizing harmonised standards as evidence across multiple laws.

Recognise harmonised technical standards (e.g. ISO, CEN/ CENELEC) as evidence of compliance across multiple acts.

Danish Standards - National Standardisation Organisation of Denmark: Argues that using standards across domains reduces regulatory fragmentation and compliance costs.

Business & Science Poland: Calls to align EU rules with existing standards to streamline compliance and improve interoperability.

DigitalTrade4.EU: Supports aligning and harmonising EU standards via a technology-neutral, future-proof framework that streamlines green digital regulation and enables cross-sector legal effect.

VDMA - Advancing Europe´s machinery industry: Requests harmonised international standards to ensure interoperability and competitiveness in machinery.

IDRS Platform: Promotes a single standard to improve efficiency, interoperability and compliance.

Japan Business Council in Europe (JBCE): Urges accelerating harmonised standards development to streamline compliance for businesses.

U.S. Chamber of Commerce: Recommends aligning EU rules with global standards, including harmonised digital civil liability norms, to minimize divergence and facilitate trade.

Inter IKEA Group: Supports EU-wide AI content labelling standards to reduce costs and ensure consistent consumer information.

ITI - Information Technology Industry Council: Warns that increasing use of Common Specifications may create fragmentation and complexity, favoring open, consensus-based standards.

Federation of European Securities Exchanges: Calls for standardized contractual terms for operational resilience to ensure consistent implementation across markets.

Comitato Elettrotecnico Italiano - CEI: Advocates convergence between regulations and standards to simplify governance and support implementation.

CECIMO - European Association of Manufacturing Technologies: Requests harmonised standards and guidance to facilitate compliant manufacturing across the EU.

Brunel University of London: Notes that aligned, predictable standards enable ethical innovation and reduce uncertainty for researchers and industry.

CSC - IT Centre for Science: Encourages building legal requirements on established community standards to enhance interoperability and avoid duplication.

Orgalim - Europe's Technology Industries: Asks to align terminology with the New Legislative Framework to maintain coherence across technical rules and conformity processes.

Seznam.cz, a.s.: Calls for harmonised, interoperable digital regulations to reduce fragmentation for online platforms and services.

Bayer AG: Advocates simplified, harmonised standards for EU AI cloud infrastructure to improve interoperability and compliance.

CLOUD INFRASTRUCTURE SERVICES PROVIDERS IN EUROPE: Proposes recognizing and integrating market compliance frameworks into EU law to streamline certifications and reduce overlap.

DECATHLON SE: Supports a unified, maturity-based compliance standard to scale governance consistently across products and services.

SPMS – Shared Services of the Ministry of Health: Endorses a modular compliance model that preserves rigor while harmonizing assessments and reducing duplication.

CEN and CENELEC: Emphasizes that harmonized standards align regulation, support trade and reduce burdens, warning that expanding Common Specifications risks fragmentation and complexity.

European Savings and Retail Banking Group: Urges limiting the proliferation of new RTS to keep technical requirements harmonised and stable.

SAP SE: Seeks to prevent standards fragmentation and ensure interoperability across EU digital legislation.

Zentralverband Deutsches Baugewerbe: Calls for uniform supply chain standards to enable consistent compliance and data interoperability.

Zentralverband der deutschen Werbewirtschaft (ZAW): Warns that inconsistent labelling standards distort competition and advocates EU-wide uniform labelling.

Capgemini Deutschland GmbH: Promotes standardized data flows and harmonised operations to improve interoperability and efficiency.

The European Crypto Initiative (EUCI): Advocates principle-based, technology-neutral standards governance to remain future-proof and interoperable.

Adyen: Encourages enhanced harmonisation and interoperability across digital regulations to ease cross-border compliance.

Logitech: Requests harmonised and aligned technical requirements to avoid duplication and enable consistent product compliance.

1.1.6 Digital Identity and Trust Services Streamlining

This category focuses on streamlining and harmonizing EU digital identity and trust service rules to reduce duplication, complexity, and administrative burden. Stakeholders back the Digital Omnibus as a vehicle to make eIDAS the single, interoperable point of reference, align the European Digital Identity (EUDI) Wallet and the EU Business Wallet, and prioritize legal certainty and practical usability for relying parties and QTSPs. The goal is to integrate with existing standards, minimize overlap across frameworks, and deliver cost-effective, cross-border solutions that work at scale, especially for SMEs. Contributors call for clear scope boundaries (e.g., EUDIW primarily for natural persons, business features in the Business Wallet) and, in some cases, for avoiding a new Business Wallet regulation by upgrading eIDAS instead. They advocate an EU-wide Business Wallet to standardize digital onboarding and e-signature requirements, resolve PSD2/eIDAS authentication overlaps, and fix country-by-country inconsistencies. Addressing redundant audits, fragmented standards, and high compliance costs under eIDAS is essential; alignment of assurance levels across AMLR and eIDAS and reuse of existing trust services (e.g., for DPP) can prevent parallel infrastructures. To accelerate adoption, stakeholders suggest pilots, incentives, and integrations with public registers, while ensuring the wallet experience remains straightforward, interoperable, and consistent. A human-centric approach that emphasizes inclusion, accessibility, and capacity building is also highlighted, extending the value of simplification beyond the EU context.

We look forward to contributing practical insights and solutions that help the Digital Omnibus reduce regulatory duplication, harmonise expectations, and strengthen legal certainty for all actors in the digital and identity ecosystem. (Docusign)

With implementation of the European Digital Identity (EUDI) Wallet currently underway, and efforts to create an EU Business Wallet in the pipeline, the Commission's Digital Omnibus is a timely opportunity to streamline rules that directly affect how identity is issued, verified, and relied upon in practice. (Docusign)

AMLR Article 22 allows elDs with Level of Assurance (LoA) Substantial to open bank accounts, which is fully aligned with anti-money laundering (AML) requirements and risk controls where potential damages or misuse could be significantly greater than those resulting from signing a contract, whereas Article 24 eIDAS 2 demands LoA High. (Namirial Spa)

In our view, this Regulation should concentrate on enabling EUDIW for natural persons, while matters relating to wallets for legal persons ought to be addressed within the upcoming European Business Wallet initiative. (Government Office of the Czech Republic)

DATEV eG: Supports simplification of digital policy via the Digital Omnibus and sees the European Business Wallet as a way to ease SMEs daily processes.

The European Business Wallet has enormous potential to significantly simplify everyday life for SMEs.

TIC Council: Welcomes the EU Business Wallet as a means to reduce administrative burdens for cross border interactions, improving efficiency for TIC sector companies.

TIC Council welcomes this initiative, as it would reduce administrative burdens for cross-border companies interacting with different public authorities, including TIC Council members themselves.

Docusign: Urges aligning EUDI and Business Wallet frameworks to reduce duplication, harmonize expectations, and strengthen legal certainty, with a focus on relying parties and QTSPs.

With implementation of the European Digital Identity (EUDI) Wallet currently underway, and efforts to create an EU Business Wallet in the pipeline, the Commission's Digital Omnibus is a timely opportunity to streamline rules that directly affect how identity is issued, verified, and relied upon in practice.

Intesi Group: Calls to streamline eIDAS by removing overlapping compliance, redundant audits, and unclear standards that drive up costs and fragment the market. Supports simplification that preserves trust and interoperability.

The current and future eIDAS framework imposes avoidable administrative and financial burdens, mainly due to overlapping compliance with other EU rules, redundant audits, and technical standards.

Government Office of the Czech Republic: Seeks clarity by focusing EUDIW on natural persons and addressing legal person wallets within the separate EU Business Wallet initiative.

In our view, this Regulation should concentrate on enabling EUDIW for natural persons, while matters relating to wallets for legal persons ought to be addressed within the upcoming European Business Wallet initiative.

ING Romania: Advocates an EU wide Business Wallet to standardize onboarding and e signature rules, eliminate paper requirements, and clarify PSD2 and eIDAS overlaps.

Create a EU-wide Business Wallet to standardise digital onboarding and e-signature rules, eliminate paper-based requirements, and clarify authentication overlaps between PSD2 and eIDAS 2.0.

Bitkom e.V.: Emphasizes keeping eIDAS as the central, coherent reference for identification and credential validation to ensure interoperability through simplification.

Simplification should ensure that existing eIDAS provisions remain the single point of reference to ensure European interoperability.

LSEG: Recommends a straightforward, interoperable, cost effective Wallet framework that integrates with existing standards and minimizes overlap, supported by incentives and pilots to drive adoption.

The regulatory framework for the Wallet should aim to be straightforward, interoperable, and cost-effective, while minimising overlap with existing digital identity and trust service frameworks.

Evotrust: Opposes creating a new Business Wallet regulation and proposes incorporating business wallet features into the existing eIDAS framework.

Rather than creating a new Business Wallet Regulation, the eIDAS regulation should be updated to support business wallets based on current needs.

Namirial Spa: Highlights inconsistencies across assurance levels and urges leveraging eIDAS trust services to avoid redundant infrastructures, improving adoption and simplicity.

This omission creates redundant infrastructures where trusted digital identities and signatures already exist.

ING Group: Supports a harmonized EU Business Wallet built on eIDAS to standardize e ID, remote verification, and e signature rules, remove paper, and resolve PSD2 and eIDAS overlaps for cross border onboarding.

ING supports the initiative to develop a European Business Wallet, consistent with and building on eIDAS, as a way to standardise e-ID and remote verification rules for businesses across the EU, allowing seamless cross-border digital onboarding.

: Calls for human centric simplification that emphasizes user control, accessibility, and inclusion, enabling equitable participation while safeguarding digital sovereignty.

Africa's Digital ID systems must learn from the EU's experience with complexity: simplification should focus on user control, accessibility, and inclusion, particularly for rural and underserved populations.

European Associations of Co-operative Banks (EACB): Welcomes efforts to simplify and clarify digital identity rules, including the EU Business Wallet, to uphold high standards while reducing compliance costs and reinforcing sovereignty.

We welcome the Commission's initiative to simplify and clarify the regulatory landscape for digital identity, including the forthcoming EU Business Wallet, while upholding high standards and reducing compliance costs.

DigitalTrade4.EU: Advocates clear legal validity and recognition for electronic documents to streamline cross border digital trade and trust services.

Inter IKEA Group: Stresses the need for a consistent, user friendly wallet experience across the EU to encourage business adoption and reduce friction.

ASNEF: Supports harmonized, risk based remote onboarding to streamline identity verification while maintaining appropriate safeguards.

SGI Europe: Warns against administrative complexity in eIDAS implementation and suggests limiting obligations primarily to cross border contexts to reduce burdens.

ACT | The App Association: Calls for simplification and harmonization of EUDI implementation to reduce fragmentation and facilitate SME participation.

Cigref: Views the EU Business Wallet as a lever to simplify compliance and streamline identity related processes for large organizations.

D-Trust: Urges prioritizing eIDAS as the backbone and harmonizing compliance and business wallet requirements to reduce redundancy and complexity.

InfoCert: Recommends prioritizing eIDAS based approaches and harmonizing rules to strengthen the Single Market and streamline trust services.

Computer & Communications Industry Association (CCIA Europe): Encourages using eIDAS to reduce overlapping compliance obligations and deliver clearer, more interoperable digital identity rules.

1.1.7 Data, Privacy and AI Governance Alignment

This category highlights the call to align Europe's core data, privacy, and AI governance regimes into a coherent, interoperable, and risk-based framework. Stakeholders urge full harmonisation across the GDPR, ePrivacy, AI Act, Data Act, Data Governance Act, Digital Services Act, and Digital Markets Act; consolidation of the fragmented EU data acquis; and clearer delineation of responsibilities where data regimes intersect, notably for mixed personal/non-personal datasets and sectoral contexts like health and finance. They advocate consistency between the AI Act's obligations and GDPR principles, alignment of cross-cutting requirements (e.g., age verification under AVMSD/GDPR/DSA), reliance on technical standards and established conformity routes, and avoiding duplicated assessments (e.g., DPIA/FRIA) to reduce compliance burdens and provide legal certainty. Beyond simplification, contributors emphasize proportionate, evidence-based rules that preserve fundamental rights while enabling innovation (e.g., via text and data mining exceptions and open data policies). Addressing overlaps in high-risk AI obligations (documentation, data governance, human oversight, monitoring) and resolving foundational issues such as the personal vs non-personal data boundary are seen as prerequisites to unlock AI's potential. The vision extends to globally interoperable governance models—supporting the EU's Data Union Strategy and fostering international trust and competitiveness.

Align with other EU Digital Laws: Fully harmonise theGDPR and ePD with the AIA, Data Act, Data Governance Act ("DGA"), Digital Services Act ("DSA"), and Digital Markets Act ("DMA"), clarifying relationships and ensuring proportionality, transparency, and legal certainty across the digital regulatory landscape. (Meta Platforms Ireland Limited)

Data processing for AI should follow harmonised rules under both the GDPR and the AI Act to prevent companies from facing overlapping regulatory requirements. (Technology Industries of Finland)

However, the central question, whether data is personal or non-personal has yet to be resolved. (eco - Verband der Internetwirtschaft e.V.)

Strengthened text and data mining (TDM) exceptions and open data policies are essential to accelerate innovation in Europe. (European Alliance for Research Excellence)

FERMA - Federation of European Risk Managers Associations: Advocates aligning the Data Act, GDPR, and Data Governance Act into a coherent, predictable, interoperable Data Union framework.

A Comprehensive Data Union Strategy will require to align all data legislation (Data Act, GDPR, Data Governance Act) into a coherent, predictable, and interoperable regulatory regime.

TIC Council: Urges consolidation of the fragmented EU data acquis to improve coherence and certainty.

Call for consolidating the EU data acquis, which is currently fragmented across various legislations.

CNIL (French Data Protection Authority): Supports EU-level harmonisation via regulation to provide legal certainty for stakeholders.

Nevertheless, a legislative reform through an EU Regulation would allow for harmonisation at the EU level and provide legal certainty for stakeholders.

European Alliance for Research Excellence: Calls for stronger text and data mining exceptions and open data policies to accelerate innovation.

Strengthened text and data mining (TDM) exceptions and open data policies are essential to accelerate innovation in Europe.

Zimmer Biomet: Highlights legal uncertainty from unclear boundaries between the Data Act and GDPR when handling mixed health data.

Unclear boundaries between the Data Act and the GDPR create legal uncertainty in handling mixed personal and non-personal health data.

Technology Industries of Finland: Seeks harmonised AI data processing rules under the GDPR and AI Act to avoid overlapping requirements.

Data processing for AI should follow harmonised rules under both the GDPR and the AI Act to prevent companies from facing overlapping regulatory requirements.

Workday: Emphasises the role of technical standards and consistency between the AI Act and GDPR for demonstrating compliance.

For this reason, our recommendations focus on the importance of available technical standards for high-risk AI providers to demonstrate their compliance, and for the need for consistency between the AI Act and other EU laws like the GDPR.

eco - Verband der Internetwirtschaft e.V.: Notes that the unresolved distinction between personal and non-personal data undermines clarity in governance.

However, the central question, whether data is personal or non-personal has yet to be resolved.

France Digitale: Calls for clarifying how the AI Act interacts with the GDPR to enable AI while protecting fundamental rights.

To unlock the full potential of AI while preserving fundamental rights, the interaction between the AI Act and the GDPR must be clarified.

Eurofinas: Requests alignment between the AI Act, GDPR, and financial sector rules to avoid duplication and ensure consistency.

Alignment between the Al Act, the GDPR, and financial sector legislation, avoiding duplication and ensuring consistency.

German Insurance Association: Warns that overlapping GDPR, AI Act, and national requirements drive significant compliance costs.

Overlapping requirements under GDPR, AI Act and national regulations lead to significant compliance costs.

Video Games Europe: Advocates a holistic rethink of the instrument to improve coherence rather than incremental updates.

Video Games Europe recommends rethinking this instrument holistically rather than just updating the existing provisions.

Government Office of the Czech Republic: Recommends aligning age verification requirements across AVMSD, GDPR, and the DSA.

It would be appropriate to align the requirements for age verification of users under the AVMSD and GDPR with those set out in the DSA.

Snap Inc.: Flags broad, overlapping obligations on high-risk AI systems that cause administrative burden.

The current framework places broad, overlapping obligations on high-risk AI systemscovering documentation, data governance, human oversight, and monitoring.

Mastercard Europe SA: Supports simplification to reduce duplicative obligations, enhance legal certainty, and foster a balanced Digital Single Market.

We fully support the EU's objectives of simplification and fostering the Digital Single Market by reducing duplicative obligations, creating legal certainty, and promoting a balanced regulatory approach.

Bolt: Warns that overlapping instruments with similar goals cause legal uncertainty, duplication, and fragmented national implementation.

Yet the interaction of overlapping instruments pursuing similar objectivessafety, fairness, and transparencybut through different processes and reporting requirements can result is legal uncertainty, administrative duplication, and fragmented national implementation.

Leading Baltic tech and other businesses and professional associations listed in the submission: Stresses that ePrivacy simplification must be part of a broader, coordinated reform for coherence.

However, ePrivacy cannot be simplified in isolation.

LSEG: Proposes a harmonised, interoperable framework across existing data laws to advance the Data Union Strategy and Digital Omnibus.

To support the EUs Data Union Strategy and the upcoming Digital Omnibus, the EU should set up a harmonised and interoperable framework across existing data laws.

European Tech Alliance: Observes misalignment between the AI Act's risk classification and the GDPR's risk-based approach.

The risk classification of the AI Act does not necessarily align with the risk based approach of the GDPR and its interpretation by the data protection authorities.

The International Center for Law & Economics: Advocates a clear, predictable, proportionate digital rulebook grounded in evidence and sound economics to support consumer welfare and innovation.

Our interest is to ensure that the EU's digital rulebook advances consumer welfare and innovation through clear, predictable, and proportionate rules grounded in evidence and sound economics.

Meta Platforms Ireland Limited: Calls for full harmonisation among GDPR, ePrivacy, AI Act, Data Act, DGA, DSA, and DMA with clarified relationships and proportionality.

Align with other EU Digital Laws: Fully harmonise theGDPR and ePD with the AIA, Data Act, Data Governance Act ("DGA"), Digital Services Act ("DSA"), and Digital Markets Act ("DMA"), clarifying relationships and ensuring proportionality, transparency, and legal certainty across the digital regulatory landscape.

Adigital (Asociación Española de la Economía Digital): Illustrates overlapping obligations for platforms under multiple EU and national regimes, underscoring the need for coherence.

For instance, second-hand product platforms are simultaneously subject to the DSA, the GPSR, and national consumer and sustainability regulations.

Almega: Notes that complex EU standards create operational and documentation burdens for businesses.

EU standards are complex and pose operational and documentation burdens.

: Envisions an EU–Africa partnership to pioneer simpler, ethical, globally interoperable digital governance.

Together, the EU and Africa can pioneer a new model of digital governancesimpler, ethical, and globally interoperableanchored in mutual trust and the shared goal of inclusive prosperity in the digital age.

Anitec-Assinform: Seeks to avoid duplication between DPIA under GDPR and FRIA under the AI Act.

Avoid DPIA and FRIA duplications between Al Act and GDPR

European AI Forum: Recommends maximum harmonisation of the AI Act and integrating high-risk obligations via existing sector frameworks to avoid duplicate assessments.

We recommend treating the Al Act as a maximum-harmonisation instrument and integrate high-risk obligations for Annex I sectors through their existing frameworks, avoiding duplicated assessments and preserving established conformity routes.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Insists on consistency between AI Act transparency and data protection requirements and the GDPR.

The AI Act should ensure that its transparency and data protection require- ments are consistent with the General Data Protection Regulation (GDPR).

Didomi: Welcomes efforts to simplify the digital framework and reduce consent fatigue while maintaining strong data protection.

Didomi welcomes the Commissions objective to simplify the EUs digital framework and reduce cookie consent fatigue while maintaining strong data protection standards.

American Chamber of Commerce to the EU: Insufficient information provided to summarise this document's position on alignment.

FEDIL, the Voice of the Luxembourg's Industry: Insufficient information provided to summarise this document's position on alignment.

Insurance and Pension - Denmark: Insufficient information provided to summarise this document's position on alignment.

Business & Science Poland: Insufficient information provided to summarise this document's position on alignment.

carVertical: Insufficient information provided to summarise this document's position on alignment.

EuroGeographics: Insufficient information provided to summarise this document's position on alignment.

Ingka Group IKEA: Insufficient information provided to summarise this document's position on alignment.

Digital Business Ireland: Insufficient information provided to summarise this document's position on alignment.

Japan Business Council in Europe (JBCE): Insufficient information provided to summarise this document's position on alignment.

BusinessEurope: Insufficient information provided to summarise this document's position on alignment.

European Banking Federation: Insufficient information provided to summarise this document's position on alignment.

Federation of Austrian Industries: Insufficient information provided to summarise this document's position on alignment.

IBM: Insufficient information provided to summarise this document's position on alignment.

Criteo: Insufficient information provided to summarise this document's position on alignment.

Intesa Sanpaolo: Insufficient information provided to summarise this document's position on alignment.

Inter IKEA Group: Insufficient information provided to summarise this document's position on alignment.

Ireland - Department of Enterprise, Tourism and Employment: Insufficient information provided to summarise this document's position on alignment.

ING: Insufficient information provided to summarise this document's position on alignment.

ASNEF: Insufficient information provided to summarise this document's position on alignment.

ENTSO-E: Insufficient information provided to summarise this document's position on alignment.

Association des Constructeurs Européens de Motocycles: Insufficient information provided to summarise this document's position on alignment.

European Broadcasting Union: Insufficient information provided to summarise this document's position on alignment.

Google: Insufficient information provided to summarise this document's position on alignment.

Agilitation: Insufficient information provided to summarise this document's position on alignment.

AFME: Insufficient information provided to summarise this document's position on alignment.

SGI Europe: Insufficient information provided to summarise this document's position on alignment.

European Fund and Asset Management Association (EFAMA): Insufficient information provided to summarise this document's position on alignment.

Orgalim - Europe's Technology Industries: Insufficient information provided to summarise this document's position on alignment.

ACT | The App Association: Insufficient information provided to summarise this document's position on alignment.

Digital Currencies Governance Group (DCGG): Insufficient information provided to summarise this document's position on alignment.

European Federation for Market Research Organisation (EFAMRO): Insufficient information provided to summarise this document's position on alignment.

Global Data Alliance: Insufficient information provided to summarise this document's position on alignment.

Insurance Europe: Insufficient information provided to summarise this document's position on alignment.

INVERCO: Insufficient information provided to summarise this document's position on alignment.

Audience Measurement Coalition (AMC): Insufficient information provided to summarise this document's position on alignment.

Computer & Communications Industry Association (CCIA Europe): Insufficient information provided to summarise this document's position on alignment.

European Savings and Retail Banking Group: Insufficient information provided to summarise this document's position on alignment.

SAP SE: Insufficient information provided to summarise this document's position on alignment.

Danish Industry: Insufficient information provided to summarise this document's position on alignment.

Alliance Digitale: Insufficient information provided to summarise this document's position on alignment.

Dedalus S.p.A.: Insufficient information provided to summarise this document's position on alignment.

DIGITALEUROPE: Insufficient information provided to summarise this document's position on alignment.

Wolt: Insufficient information provided to summarise this document's position on alignment.

AMETIC: Insufficient information provided to summarise this document's position on alignment.

The European Crypto Initiative (EUCI): Insufficient information provided to summarise this document's position on alignment.

Chamber of Commerce and Industry for Munich and Upper Bavaria: Insufficient information provided to summarise this document's position on alignment.

AI Accountability Lab (AIAL), Trinity College Dublin: Insufficient information provided to summarise this document's position on alignment.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Insufficient information provided to summarise this document's position on alignment.

Association Française des Entreprises Privées: Insufficient information provided to summarise this document's position on alignment.

Lenovo: Insufficient information provided to summarise this document's position on alignment.

Estonian Ministry of Justice and Digital Affairs: Insufficient information provided to summarise this document's position on alignment.

WindEurope: Insufficient information provided to summarise this document's position on alignment.

Confederation of Swedish Enterprise: Insufficient information provided to summarise this document's position on alignment.

1.1.8 Risk-Based Proportionality and SME Relief

This category advances a harmonised, risk-based and proportionate digital rulebook that curbs cumulative and overlapping obligations across EU acts. It emphasises principle-based, technology-agnostic and outcome-oriented requirements; coherent definitions, thresholds and roles; and systematic cost–benefit analysis, relying on existing frameworks to avoid duplication and scope creep. Where appropriate, obligations should be clarified, streamlined or shifted to voluntary best practices, with targeted tailoring such as reducing unnecessary granularity (e.g., in illegal-content taxonomies) or limiting burdens to higher-risk services and larger actors. SME relief is central: micro and small firms face disproportionate administrative and reporting costs. The preferred toolkit includes exemptions or simplified self-assessments for smaller entities, harmonised guidance (e.g., joint security and AI risk-management guidance), and accessible support channels—while preserving high levels of user protection and trust. Stakeholders caution against expanding scopes or adding new layers of rules; instead, they urge withdrawing redundant obligations and delivering concrete, coherent simplification that boosts innovation, competitiveness and collaboration across startups, SMEs, mid-caps and incumbents.

Telefónica supports reinforcing the risk-based approach to reduce unnecessary burdens and improve legal certainty. (Telefonica, S.A.)

Exempt micro and small enterprises from extensive NIS-2 documentation; allow simplified self-assessments. (European AI Forum)

Work on new legislation in this field should be suspended. (Digital Poland Association)

Exclude stand-alone software Al applications from CRA obligations unless they control hardware or network-critical functions. (European AI Forum)

Zimmer Biomet: Argues that aligning digital frameworks and proportionate burden reduction will unlock innovation and reduce administrative obstacles, improving patient access.

A more coordinated and proportionate approach will allow manufacturers to focus resources on advancing safe, effective technologies rather than navigating regulatory uncertainty.

Digital Poland Association: Warns that excessive, complex digital rules impede growth and disproportionately burden SMEs, urging simplification by enforcing existing laws and pausing new ones.

The European Union's excessive and complex regulations in the digital space impede its growth and disproportionately burden small and medium-sized European enterprises.

France Digitale: Supports streamlined, coherent and proportionate simplification to empower startups, including clarifying and where appropriate easing procedural obligations.

A simplified yet robust regulatory framework, built on consistency, and proportionality, would empower startups to innovate confidently, compete fairly, and contribute to a dynamic and resilient European digital economy.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Advocates maximizing existing frameworks and principle-based, proportionate regulation to keep the rulebook innovation-friendly and competitive.

In response to the EU Commissions recent call for evidence, this paper outlines concrete proposals to ensure the digital rulebook remains proportionate, innovation-friendly, and globally competitive.

Government Office of the Czech Republic: Proposes harmonizing key definitions and converting certain obligations into voluntary best practices to lower compliance burdens without compromising goals.

Such evaluation reports might, for example, explore the potential to unify the notion of "main establishment" throughout the DGA, DSA and other files, or the potential to transform some requirements for data intermediation service providers to voluntary best practices.

Telefonica, S.A.: Calls for fact- and risk-based, harmonised obligations backed by cost-benefit analyses and funding, alongside coherent deregulation to reduce unnecessary burdens.

Ensure that all regulatory obligations are fact- based, risk-based, and that they are consistently accompanied by thorough cost-benefit analyses and clear funding strategies.

World Federation of Advertisers: Endorses a principles- and risk-based approach that aligns with GDPR, provides legal certainty, and encourages innovation while upholding strong user protection.

Adopting such a principles- and risk-based approach, rather than granting flexibility only for specific marketing models or technical configurations, would ensure a future-proof framework that encourages innovation, including the development and use of privacy-enhancing technologies.

Accountancy Europe: Urges clearly scoped, practical simplification with a specific focus on SME needs and cautions against expanding legislation such as DORA's scope.

These 10 principles remain highly relevant today, and in pursuing its digital simplification initiative, we urge the Commission to clearly define the scope and objectives of the simplification measures; focus on practical measures that achieve concrete simplification for businesses, and avoid political solutions that risk adding further complexity and uncertainty; address specific challenges faced by SMEs; and engage with stakeholders including Accountancy Europe and the accountancy profession early, meaningfully and effectively

Seznam.cz, a.s.: Recommends reducing granularity in illegal content categories by making subcategories voluntary or limited to VLOPs, easing burdens proportionately.

Therefore, we suggest reducing the granularity by making the subcategories (categories 1a-1c, 2a-2f, 3a-3g, etc.) voluntary (or mandatory only for VLOPs).

Mastercard Europe SA: Supports technology-neutral, outcome-based rules grounded in proportionality to avoid duplication and administrative burden while enabling innovation and security.

A regulatory framework built on proportionality, flexibility, and cooperation will protect consumers and businesses while enabling innovation and global competitiveness.

Meta Platforms Ireland Limited: Notes reforms are vague and limited, focusing mainly on record-keeping relief and extending SME derogations to mid-caps rather than broader harmonisation.

Yet the only change on the table so far is an easing of record keeping and extending SME derogations to mid-caps.

Adigital (Asociación Española de la Economía Digital): Advocates horizontal, principles-based simplification that maintains robust consumer protection while reducing disproportionate burdens and fostering collaboration across company sizes.

Rather, it calls for adapting the existing framework to make regulation more coherent, efficient, and proportionate-while ensuring consistent consumer protection across the digital value chain.

European AI Forum: Highlights overlapping security regimes that duplicate reporting and impose disproportionate costs on startups and SMEs, proposing harmonised guidance and SME exemptions.

Exempt micro and small enterprises from extensive NIS-2 documentation; allow simplified self-assessments.

: From a micro-business perspective, calls for simplified, harmonised rules and accessible support to reduce disproportionate compliance burdens and refocus on innovation.

Simplified and harmonised rules across the EU would help us focus more on service quality and innovation instead of paperwork.

Ingka Group IKEA: Supports harmonisation and proportionality in digital rules to ensure workable, innovation-friendly compliance without unnecessary burdens.

Telekom Austria AG: Calls to streamline redundant risk management approaches across regimes to improve coherence and proportionality for operators.

BusinessEurope: Urges aligning risk concepts and actor roles across acts to deliver proportionate, consistent obligations and reduce fragmentation.

MedTech Europe: Supports balanced, proportionate simplification that maintains high safety and performance standards in medtech.

ASNEF: Endorses digital simplification to ease SME compliance and strengthen participation in the digital economy.

Association of Finnish Cities and Municipalities: Requests that municipalities be included in simplification measures and reliefs, reflecting capacity constraints and proportional risk.

TikTok Technology Ltd.: Calls for proportionate exemptions, sandbox presumptions, and a ban on national gold-plating to ensure consistent, innovation-friendly obligations.

Sdružení pro internetový rozvoj (SPIR): Opposes burdensome categorisation of orders, advocating lighter, risk-based requirements that reflect platform size and impact.

EFCA - European Federation of Engineering Consultancy Associations: Seeks a harmonised, proportionate framework with reliance mechanisms to reduce duplicative compliance for engineering consultancies, including SMEs.

Eurochambres: Requests clear, risk-based thresholds for roles and obligations to provide certainty and proportional relief, especially for SMEs.

Insurance Europe: Proposes exempting intra-group IT services to avoid duplication and reduce compliance burdens in a proportionate manner.

Danish Industry: Advocates unified risk assessment criteria across overlapping regimes to lower duplication and enhance proportionality for businesses.

Free ICT Europe Foundation: Emphasizes that harmonised, proportionate rules will ease heavy compliance burdens on ICT SMEs and improve competitiveness.

OpenAI: Warns that regulatory overlap and fragmentation create disproportionate burdens for SMEs, urging coherent, risk-based simplification.

Council of European Municipalities and Regions (CEMR): Calls for simplification and tailored municipal data obligations relief to match capacity and risk while maintaining trust.

1.1.9 Uniform Enforcement, Mutual Recognition and One-Stop Supervision

The insights consistently call for a simplified, harmonized digital rulebook built on uniform enforcement, mutual recognition, and one-stop supervision. Fragmentation stems from directives and divergent national interpretations (e.g., NIS2, GDPR, ePrivacy), creating uncertainty about applicable rules and competent authorities, and raising costs for cross-border activity. Stakeholders urge consistent application across the EEA (including digital identity and wallets), prioritization of common EU trust and identity standards (eIDAS), and stable, harmonized implementation to avoid burdens on SMEs and QTSPs. Sectoral examples (AMLD onboarding, DAC7 definitions) illustrate how inconsistent supervision and guidance multiply duplicative procedures. Overlapping risk-management regimes (NIS2, CRA, DORA and others) impose similar yet distinct obligations without clear mapping or presumptions of conformity, leading to redundant controls. The proposed fixes include EU-wide standardized risk assessments, monitoring formats and audit checklists; mutual recognition of equivalent compliance; a one-stop shop for conformity assessment and supervision; and clearer, harmonized risk evaluation and enforcement criteria. Initiatives like the Digital Omnibus are seen as levers to curb fragmentation; ultimately, a coherent framework with uniform enforcement and one-stop mechanisms would streamline compliance, support cross-border scaling, and strengthen resilience and competitiveness.

Connect Europe and the GSMA call on the European Commission to consider further clarification and harmonisation of risk evaluation and enforcement criteria across EU Member States. (GSMA)

For the Cyber Resilience Act, a one-stop shop provision should be established for the conformity assessment process. (Emerson Electric Co.)

Key legislation such as the NIS2 Directive, the Cyber Resilience Act ("CRA"), the Digital Operational Resilience Act ("DORA"), and sectoral rules impose similar yet distinct risk-management requirements without providing a clear mapping or a presumption of conformity between them, leading to redundant controls. (Meta Platforms Ireland Limited)

On top of the much-delayed transposition process, in its current form, the NIS2 directive does not effectively create the conditions for enhanced cyber resilience in the EU and undermines the EU's competitiveness. (Schneider Electric)

Volkswagen Group: Notes that using a Directive for NIS2 led to divergent national implementations, undermining uniform enforcement and mutual recognition.

Since the co-legislators opted for a Directive as the regulatory instrument when drafting NIS 2, the implementation of its requirements varies significantly across the EU's 27 Member States.

eco - Verband der Internetwirtschaft e.V.: Welcomes a digital business wallet and urges its swift, uniform rollout across the EEA to ensure mutual recognition and consistent supervision.

eco welcomes the application of a digital business wallet and hopes for a swift and uniform application throughout the European Economic Area (EEA).

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Supports simplification-by-design and streamlined legislative instruments to enable a harmonized digital rulebook and more uniform enforcement.

Luxembourg aligns with member states that called for a simplification of legislative instruments in the digital policy space and a simplification by design approach for new EU legislative initiatives, as was recommended by D9+ member states at the beginning of the EU Commissions mandate.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Highlights uncertainty over applicable rules and competent authorities when meeting AI-related transparency duties, calling for clearer allocation and one-stop supervision.

Companies often face uncertainty about which rule applies or which authority is competent, for instance when processing personal data to fulfil AI transparency.

GSMA: Calls for EU-wide clarification and harmonisation of risk evaluation and enforcement criteria to achieve uniform enforcement.

Connect Europe and the GSMA call on the European Commission to consider further clarification and harmonisation of risk evaluation and enforcement criteria across EU Member States.

World Federation of Advertisers: Urges the Commission to remedy fragmented interpretations of consent under ePrivacy to deliver uniform enforcement and reduce compliance complexity.

In particular, we encourage the Commission to address fragmentation in the interpretation of consent requirements under the ePrivacy Directive, which creates complexity for businesses and for consumers.

Bitkom e.V.: Observes that while data rules have curbed early fragmentation, the framework remains incoherent, underscoring the need for a harmonised, mutually recognized rulebook.

While the recent acquis of rules on access, localisation, intermediation, and transfer of (non-)personal data has avoided the fragmentation of the single market for data during its very onset, it has not been possible to create a fully coherent framework yet.

European Tech Alliance: Warns that divergent GDPR implementation blocks harmonisation and inflates cross-border costs, arguing for consistent, one-stop supervision.

National conflicting or divergent interpretation and implementation of the GDPR prevent any harmonisation and generate significant complexities and costs for cross-border activities.

Evotrust: Advocates prioritising eIDAS standards to drive mutual recognition and consistent enforcement across Member States.

To avoid these burdens, laws should prioritize eIDAS standards where applicable.

ISP Alliance a.s.: Stresses stable, harmonised implementation of digital identity rules to avoid burdens on smaller providers and enable predictable, uniform supervision.

We merely note the importance of ensuring a stable and harmonised implementation across Member States, as frequent technical or procedural changes could be disproportionately burdensome for smaller service providers integrating digital identity solutions into their platforms.

Namirial Spa: Notes that QTSPs face acute challenges, implying the need for harmonised supervision and mutual recognition to ensure consistent trust services across the EU.

Qualified Trust Service Providers (QTSPs), as the cornerstone of digital trust, face particularly acute challenges.

Emerson Electric Co.: Proposes a one-stop-shop conformity assessment under the CRA to streamline oversight and foster uniform enforcement.

For the Cyber Resilience Act, a one-stop shop provision should be established for the conformity assessment process.

Schneider Electric: Flags that delayed transposition and NIS2's current design hinder effective resilience and competitiveness, reinforcing the case for harmonised implementation and enforcement.

On top of the much-delayed transposition process, in its current form, the NIS2 directive does not effectively create the conditions for enhanced cyber resilience in the EU and undermines the EU's competitiveness.

Meta Platforms Ireland Limited: Points to overlapping, inconsistent risk-management obligations across NIS2, CRA, DORA and sectoral rules, and calls for mapping and mutual recognition to avoid duplicative controls.

Key legislation such as the NIS2 Directive, the Cyber Resilience Act ("CRA"), the Digital Operational Resilience Act ("DORA"), and sectoral rules impose similar yet distinct risk-management requirements without providing a clear mapping or a presumption of conformity between them, leading to redundant controls.

Adigital (Asociación Española de la Economía Digital): Highlights uncertainty in DAC7 definitions and thresholds, indicating a need for clearer, harmonised guidance and uniform enforcement.

Regarding DAC7 (Directive on Administrative Cooperation in tax matters), the lack of clarity on the definition of "reportable sellers" and the low thresholds set generate operational uncertainty.

ING Group: Reports varying AMLD interpretations that cause duplicative onboarding, urging harmonised standards and one-stop recognition across the EU.

Varying interpretations of AMLD across Member States create inconsistent and duplicative onboarding processes.

Union of Entreprenuers and Employers: Identifies overlapping risk assessment and documentation duties, advocating streamlined, standardised approaches and mutual recognition.

A first area of concern is the overlap in risk assessment and documentation requirements.

European AI Forum: Describes a patchwork of digital laws with inconsistent enforcement that burdens startups and SMEs, calling for uniform, simplified supervision and mutual recognition.

For European AI startups and SMEs, the current patchwork of digital laws creates disproportionate challenges: overlapping transparency obligations, restrictive data-use provisions, duplicate documentation and assessments, inconsistent enforcement across Member States, and many more.

2Dyles Services: Recommends EU-wide standardised risk assessments, monitoring and audit formats to enable mutual recognition and consistent enforcement.

Introduce standardized risk assessments, monitoring formats, and audit checklists that are universally recognized within the EU.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Notes that adopting a Directive for NIS2 led to divergent national implementations, underscoring the need for harmonised enforcement and supervision.

Since the co-legislators agreed on the regulatory measure of a "Directive" when develop- ing the NIS 2, the regulatory requirements are implemented differently across the EU's 27 Member States.

: Supports the Digital Omnibus initiative as a means to reduce regulatory fragmentation and promote uniform enforcement across the digital rulebook.

The Digital Omnibus initiative is a timely step to reduce regulatory fragmentation in the EUs digital rulebook.

Swisscom IT Services Finance S.E.: No specific input on uniform enforcement, mutual recognition or one-stop supervision was provided in this document.

FEDIL, the Voice of the Luxembourg's Industry: No specific input on uniform enforcement, mutual recognition or one-stop supervision was provided in this document.

1.1.10 Streamlined Compliance, Report-Once and Templates

The insights call for a harmonized, predictable, and proportionate digital rulebook that streamlines compliance by aligning overlapping obligations across EU, national, and sectoral regimes. Stakeholders highlight the need to reduce bureaucracy without lowering protections, so SMEs and pan-European firms face less duplicative paperwork and can focus on innovation, resilience, and competitiveness. Simplification should prioritize coherence, stability, and consistent enforcement while avoiding conflicting national rules. Practically, the category emphasizes "report-once" mechanisms and standardized templates: a Single Reporting Window for supervisory reporting; consolidation of assessments (e.g., one AI and data protection impact assessment covering FRIA and DPIA); and cross-recognition and reuse of evidence so that controls proven under one law (e.g., Data Act) count under related frameworks (e.g., AI Act). Removing duplication in documentation and reporting, combined with risk-proportionate obligations, enables targeted, surgical fixes that lower administrative burden without sacrificing security or individual rights.

> *The regulations should be simplified ONLY if this means alignment in terms of bureaucratic load and less burden for SMEs (e.g. allowing companies to generate one report that covers multiple regulations).* ()
>
> *Allow a single, comprehensive Al and Data Protection Impact Assessment that satisfies both FRIA and DPIA requirements.* (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))
>
> *Secondly, applying horizontal AI rules in sectors with already existing legal frameworks (e.g., automotive, medical, machinery, aviation) risks duplicative documentation, strained notified bodies, and divergent technical pathways.* (European AI Forum)
>
> *Once an organisation demonstrates robust governance for data access, provenance, or security under the Data Act, this evidence should be recognized across related frameworks, including the AI Act.* (Association française de normalisation (AFNOR))
>
> **:** Advocates simplification only when it aligns bureaucratic requirements across laws and reduces SME burden, including letting firms file one report covering multiple regulations.
>
> *The regulations should be simplified ONLY if this means alignment in terms of bureaucratic load and less burden for SMEs (e.g. allowing companies to generate one report that covers multiple regulations).*
>
> **Assuralia:** Urges DORA simplification that is coherent and proportionate to avoid unnecessary burdens, so insurers can focus on resilience, innovation, and competitiveness.
>
> *By prioritizing stability for insurers, coherence, and proportionality, the DORA simplification can achieve its objectives without imposing unnecessary burdens, enabling insurers to focus on resilience, innovation, and competition (e.g. enhancing their ability to serve policyholders and remain competitive globally).*
>
> **Technology Industries of Finland:** Calls for a coherent, predictable and proportionate EU digital framework to streamline compliance across initiatives.
>
> *The Digital Package should ensure Europes digital regulatory framework is coherent, predictable and proportionate.*
>
> **eco - Verband der Internetwirtschaft e.V.:** Supports the Digital Omnibus to cut bureaucracy and improve coherence and applicability of EU rules, easing compliance.
>
> *With the Digital Omnibus, the European Commission aspires to contribute to the agenda of reducing bureaucracy and increasing coherence and applicability of European regulation through the Commission Framework "A simpler and faster Europe".*
>
> **European Energy Information Sharing and Analysis Centre:** Seeks simplification that preserves security while enabling innovation, information sharing, and effective risk management in the energy sector.
>
> *By bringing the perspective of a community that bridges policy and operations, EE-ISAC aims to ensure that the Digital Omnibus delivers simplification without sacrificing security, enabling*

innovation, facilitating information sharing, and supporting effective risk management in the energy sector.

France Digitale: Highlights overlapping digital requirements creating complexity and argues for harmonization to streamline obligations.

In recent years, the proliferation of digital regulations, each pursuing legitimate policy goals, has resulted in overlapping requirements and growing complexity.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Proposes a single combined AI and data protection impact assessment to eliminate duplicative documentation across FRIA and DPIA.

Allow a single, comprehensive Al and Data Protection Impact Assessment that satisfies both FRIA and DPIA requirements.

Airbus: Warns that complex, fragmented, and overlapping EU, national, and sectoral rules burden pan-European firms, underscoring the need for alignment and simplification.

However, the current framework presents challenges due to its complexity and fragmentation, in particular for pan-European players, for which European, national & sectorial regulations overlap.

ING Romania: Recommends relying on EU-level frameworks to avoid conflicting national rules and harmonizing supervisory reporting via a Single Reporting Window.

Rely on EU-level frameworks like GDPR to avoid conflicting national rules, clarify how data minimisation interacts with other regulations, and harmonise supervisory reporting through a Single Reporting Window.

Association française de normalisation (AFNOR): Advocates mutual recognition of demonstrated governance across laws so evidence under one act can satisfy others, avoiding rework.

Once an organisation demonstrates robust governance for data access, provenance, or security under the Data Act, this evidence should be recognized across related frameworks, including the AI Act.

Centre for Information Policy Leadership (CIPL): Endorses targeted, accountability-based simplification with risk-proportionate obligations and consistent enforcement to reduce burden without weakening rights.

CIPL strongly believes that targeted simplification, anchored in accountability, risk-proportionate obligations, and consistent enforcement, can strengthen both individual rights and support innovation.

Infosys Limited: Aims to reduce administrative burden across AI, data, and cybersecurity compliance to speed responsible AI adoption while maintaining safeguards.

The scope of this submission is to reduce the administrative burden triggered by AI, Data and Cybersecurity compliance requirements and speed up responsible AI adoption while preserving necessary safeguards.

Meta Platforms Ireland Limited: Supports efforts to lower unnecessary administrative costs amid a complex web of digital legislation and regulators.

As companies continue to grapple with a complex web of digital legislation and regulators, the goal of lowering unnecessary administrative costs for businesses is a laudable task, and one that we strongly support.

Adigital (Asociación Española de la Economía Digital): Argues administrative burdens can be reduced without compromising the objectives of EU rules.

It is clear that administrative burdens could be reduced without compromising the objectives of EU regulations and, particularly, directives.

Panasonic Europe B.V.: Backs a surgical Digital Omnibus delivering near-term, high-impact simplifications without reducing protection.

We support the Digital Omnibus as a surgical simplification package that delivers nearterm, highimpact fixes without lowering protection.

European AI Forum: Warns that layering horizontal AI rules onto sectors with existing regimes creates duplicative documentation and divergent pathways, calling for streamlining.

Secondly, applying horizontal AI rules in sectors with already existing legal frameworks (e.g., automotive, medical, machinery, aviation) risks duplicative documentation, strained notified bodies, and divergent technical pathways.

Alcon Laboratories Inc: Calls to simplify clinical and post-market documentation by removing duplicative adverse event reporting.

Simplify documentation requirements for clinical investigations and post-market surveillance (PMS), e.g., removing duplication in adverse event reporting,

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Notes the current regulatory framework hampers internal company processes and digital business model development, indicating a need for simplification.

This regulatory framework has negative implications for companies internal processes and the development of digital business models.

Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg: Requests clearer AI Act authorization procedures to streamline compliance and reduce uncertainty.

On the one hand, the AI Act should, among other things, include clarifying rules on authorisation procedures:

American Chamber of Commerce to the EU: No specific insight on streamlined compliance, report-once or templates was provided in the excerpt.

CECE - Committee for European Construction Equipment: No specific insight on streamlined compliance, report-once or templates was provided in the excerpt.

: Suggests processes can be made more business-friendly but cautions that simplification must not enable illiberal interference or undermine democratic safeguards.

You can still make processes more business-friendly, but ultimately, allowing globalised illiberal nations to operate in the EU cannot lead to anything but the adaptation of their autocratic rulebooks and their continued interference with liberal democracy.

: No specific insight on streamlined compliance, report-once or templates was provided in the excerpt.

iProov Ltd: No specific insight on streamlined compliance, report-once or templates was provided in the excerpt.

1.1.11 Digital-by-Default Tools and Paperless Administration

Digital-by-default tools and paperless administration aim to mandate electronic processes across the EU rulebook: replacing wet signatures, physical archives, and paper declarations with electronic declarations of conformity, digital product passports, online documentation, and digital labelling (including functional equivalence for digital communications and QR-based approaches). A harmonized backbone like an EU Business Wallet would standardize digital onboarding and e-signatures while clarifying overlaps between PSD2 and eIDAS, enabling consistent, cross-border compliance and cutting delays and costs. The Commission's "paperless omnibus" under Omnibus IV modernizes product legislation to make digital documentation the norm. Administrative simplification complements digitization: generalizing positive administrative silence and replacing licenses with responsible declarations, enabling faster deployments; accepting one-time, verifiable notarized documents across portals to avoid repeated uploads; and promoting EU-backed RegTech and portals that automate filings (e.g., auto-filled procurement forms from public databases). The broader Digital Omnibus agenda seeks a clearer, more coherent rulebook (including sectoral updates like networks, toy safety, and aviation) to reduce burden, improve supervision and traceability, speed infrastructure rollout, and boost SME

competitiveness—delivering trust through quick, visible pilots and consistent privacy- and security-respecting data reuse.

Adopt a digital-first approach replace paper-based documentation and declarations with digital ones. (ZVEI e.V.)

The Commission is currently modernising several product legislations via a so-called "paperless omnibus initiative" to allow more digital documentation. (ZVEI e.V.)

For branch establishment, it could transport notarised documents and official extracts once, in verifiable format, rather than requiring repeated manual uploads across different portals. (Entrust SAS)

Generalize the use of positive administrative silence to streamline deployments. (Adigital (Asociación Española de la Economía Digital))

ZVEI e.V.: Urges a digital-first, paperless approach to product compliance by replacing paper-based documentation and declarations with digital versions, aligning with the Commission's paperless modernisation.

Adopt a digital-first approach replace paper-based documentation and declarations with digital ones.

ING Romania: Proposes an EU-wide Business Wallet to standardise digital onboarding and e-signature rules, remove paper requirements, and clarify overlaps between PSD2 and eIDAS.

Create a EU-wide Business Wallet to standardise digital onboarding and e-signature rules, eliminate paper-based requirements, and clarify authentication overlaps between PSD2 and eIDAS 2.0.

Adigital (Asociación Española de la Economía Digital): Advocates administrative streamlining by using responsible declarations and positive administrative silence to speed deployments and reduce paperwork.

Replace licenses with responsible declarations as the preferred mechanism.

ING Group: Calls to mandate digital processes and eliminate remaining paper requirements across EU and national law, enabled by an EU Business Wallet for onboarding and signatures.

eIDAS/Business Wallet: Create a EU-wide Business Wallet to standardise digital onboarding and e-signature rules, eliminate paper-based requirements, and clarify authentication overlaps between PSD2 and eIDAS 2.0.

Entrust SAS: Recommends one-time submission of notarised and official documents in verifiable digital format for branch establishment to avoid repeated uploads across portals.

For branch establishment, it could transport notarised documents and official extracts once, in verifiable format, rather than requiring repeated manual uploads across different portals.

Union of Entreprenuers and Employers: Supports the Commission's digital-by-default approach with electronic declarations, digital product passports, and online documentation to cut admin effort and improve traceability.

Electronic declarations of conformity, digital product passports, and online documentation can reduce administrative effort, facilitate supervision, and improve traceability.

: Posits the Digital Omnibus as the vehicle to simplify and clarify the EU digital rulebook, creating predictable conditions for lawful data reuse while upholding privacy and security.

By simplifying and clarifying the EUs digital rulebook, the initiative can create predictable conditions for lawful data reuse while maintaining high standards of privacy and security.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Calls for ambitious regulatory reform to speed permits and simplify the framework for digital networks, enabling faster infrastructure deployment.

An ambitious reform of the current regulatory framework is essential with the upcoming Digital Networks Act (DNA) - including a shift towards horizontal consumer protection law, extended spectrum licences, and an overall more coherent and simpler regu- latory framework.

: Suggests quick-win pilots like auto-filled EU procurement forms and centralised cookie management to prove impact and build trust in the Digital Omnibus.

Quick wins within 12 months: tangible pilots e.g., standardised EU procurement forms auto-filled via public databases, or a centralised cookie management dashboard to prove impact fast.

European Travel Retail Confederation (ETRC): Urges permission for digital labelling, noting multilingual packaging needs are better served via digital solutions.

DigitalTrade4.EU: Recommends full digitisation of sectoral compliance, including toy safety frameworks and EASA procedures, to streamline oversight and reduce burden.

PII Guard: Promotes technology-based approaches to simplify compliance obligations and reduce administrative overhead.

Japan Business Council in Europe (JBCE): Advocates replacing physical labels with QR codes to provide dynamic, multilingual product information digitally.

Confederation of Norwegian Enterprise (NHO): Supports using Digital Product Passports to replace Declarations of Conformity and removing paper backup requirements.

Ireland - Department of Enterprise, Tourism and Employment: Encourages adoption of digital tools and a single portal to harmonise and simplify administrative interactions with government.

REIF: Calls for EU-harmonised, rights-respecting digital tools that ease compliance while safeguarding privacy and data protection.

: Urges clearer rules and automated processes to cut administrative burden and improve compliance efficiency.

Brunel University of London: Highlights how recognising electronic trade documents can simplify cross-border processes and reduce paperwork.

RECHARGE - The Advanced Rechargeable & Lithium Batteries Association: Requests clear, digital-first documentation rules to ensure consistency and reduce compliance friction across the battery value chain.

Computer & Communications Industry Association (CCIA Europe): Recommends functional equivalence for digital communications and prioritising digital labelling to modernise obligations without paper.

Enedis: Welcomes simplification of digital documentation and filing processes to reduce administrative effort.

AI Accountability Lab (AIAL), Trinity College Dublin: Proposes EU-backed RegTech tools to automate compliance and reporting, lowering costs and errors.

Too Good To Go: Asks to reduce burdensome paper-based compliance and enable digital alternatives for efficient reporting.

1.1.12 Miscellaneous

Stakeholders converge on simplifying and harmonizing the digital rulebook to remove overlapping and bureaucratic burdens that slow innovation and investment. Priorities include streamlining national frameworks, cutting permit delays that hamper electrification of digital sectors, and shrinking resource-heavy contractual and compliance artefacts that absorb commercial, technical, and legal capacity. Properly executed, simplification is expected to strengthen transparency, market trust, and competitiveness while remaining user-friendly for

innovators. Equally emphasized are guardrails: simplification must not dilute fundamental rights or consumer protections, and it should be inclusively designed to avoid new digital barriers for people with disabilities and residents from diverse backgrounds. Suggestions include making rules more accessible and understandable, exploring open-source-driven transparency with calibrated access, respecting national competences where appropriate, and avoiding burdensome obligations like proactive illegality searches. Several note that today's complexity often stems from well-intended protective laws—hence the goal is smarter, clearer rules that preserve protections and subsidiarity while eliminating duplication and red tape.

> *The Polish Chamber of Insurance (PIU) appreciates the European Commissions efforts to streamline and simplify the regulatory framework in the digital sphere, which is an important step towards enhancing innovation and competitiveness across the European Union.* (Polish Chamber of Insurance (PIU))
>
> *Regulatory simplification would also strengthen market trust, boosting transparency levels and investment in the sector.* (Adigital (Asociación Española de la Economía Digital))
>
> *Of course, there is a need for simplification of laws, including all of them, making the use of open source mandatory, for reasons of transparency and reliability, but this access, paradoxically for businesses, by accredited persons, not the average person.* ()
>
> *Introducing strong regulatory over- sight, streamlining national frameworks and eliminating bureaucratic bottlenecks, such as permit delays, is es- sential for the electrification of key digital sectors.* ()
>
> **:** Proposes stronger oversight and streamlined national frameworks to eliminate bureaucratic permit delays that slow electrification of digital sectors.
>
> *Introducing strong regulatory over- sight, streamlining national frameworks and eliminating bureaucratic bottlenecks, such as permit delays, is es- sential for the electrification of key digital sectors.*
>
> **SIEMENS AG:** Highlights that standardized agreements are excessively long and demand substantial commercial, technical and legal resources to finalize and implement.
>
> *The existing MCT8 and its annexes already exceed 100 pages, possibly making these agreements longer than the original customer contracts.*
>
> **Enel SpA:** Supports simplification only if it preserves individuals' fundamental rights and freedoms, warning against any erosion of protections.
>
> *However, we would like to emphasize that any simplification of the regulatory landscape must not impact the individuals' fundamental rights and freedoms.*
>
> **CERMI:** Welcomes digital simplification while calling for an inclusive, rights-based approach that safeguards persons with disabilities and prevents new barriers or exclusion.
>
> *We urge the Commission to adopt an "inclusive simplification" approach, ensuring that technology and legislation serve as tools for empowerment, not exclusion.*
>
> **Polish Chamber of Insurance (PIU):** Backs EU efforts to streamline digital rules to foster innovation and competitiveness across the Union.
>
> *The Polish Chamber of Insurance (PIU) appreciates the European Commissions efforts to streamline and simplify the regulatory framework in the digital sphere, which is an important step towards enhancing innovation and competitiveness across the European Union.*
>
> **Adigital (Asociación Española de la Economía Digital):** Argues that regulatory simplification will enhance market trust, improve transparency and catalyze investment in the digital sector.
>
> *Regulatory simplification would also strengthen market trust, boosting transparency levels and investment in the sector.*
>
> **Akava:** Open to user-friendly simplification that encourages innovation while maintaining effective regulation.

we do not oppose simplification, making regulation user-friendly and encouraging innovation,

: Calls for legal simplification and mandatory open-source use to improve transparency and reliability, with access mediated by accredited persons rather than the general public.

Of course, there is a need for simplification of laws, including all of them, making the use of open source mandatory, for reasons of transparency and reliability, but this access, paradoxically for businesses, by accredited persons, not the average person.

: Emphasizes that EU-level digital regulations must be accessible and understandable to residents from diverse backgrounds, reflecting practical user experience with national digital services.

As someone who has successfully integrated into Czech society including learning the Czech language and actively using national digital services (such as BankID and the data mailbox system) I see how vital it is that EU-level digital regulations are accessible and understandable for residents from different backgrounds.

The European Lotteries Association: Urges respect for Member State competence and warns against EU-level harmonization in the lotteries domain.

Federation of Austrian Industries: Notes that overlapping and fragmented rules hinder innovation and investment, advocating for streamlined, coherent regulation.

U.Di.Con. APS UNIONE PER LA DIFESA DEI CONSUMATORI: Supports simplification that preserves strong consumer protection, ensuring clearer rules without weakening safeguards.

The Center for Countering Digital Hate: States that platforms should not be required to proactively search for illegal content and should be protected from general monitoring obligations.

OpenAI: Observes that layers of protective laws have generated complexity, underscoring the need to simplify while maintaining essential safeguards.

1.2 Coordinated Governance, Guidance & Phased Timelines

Legal obligations and oversight should go live only when standards, guidance, and capacity are ready—sequenced with clear buffers and phased timelines to prevent fragmentation and rework. Centralized, practical guidance with aligned definitions, FAQs, roadmaps, and local-language tools enables consistent scoping and early planning across the EU. A coordinated one-stop-shop supervisory model, with mutual recognition and harmonized reporting formats and timelines, reduces duplicative filings and jurisdictional confusion. Capacity must be built in parallel: rapid designation and accreditation of conformity bodies, standardized procedures, helpdesks, trainings, RegTech toolkits, pilots and sandboxes, and temporary acceptance of equivalent testing. Early, inclusive consultation and co-regulatory instruments (codes, standards, sandboxes) improve usability, while transparent risk-assessment sharing and modernized supervisory mandates support rights and innovation. Cross-regime alignment is vital: clarify hierarchies among NIS2, DORA, GDPR, AI Act, and the Data Act; promote interoperability (e.g., organizational identity wallets), cross-border testbeds, swift Omnibus fixes, GPAI grace periods, and clear IP/copyright guidance. Proportionality mechanisms—one-in-one-out, ex-post evaluations, stop-the-clock/soft-landing, machine-readable obligations—sustain predictability and uniform application. Governance should be principle-based, with clarified EU-national roles, transparent comitology, selective pauses to monitor outcomes, and spectrum policy as a phased, investment-oriented testbed. Across sub-categories, the dominant pattern is coordinated, phased implementation anchored in shared standards, interoperable processes, and clear accountability. The common goal is predictable, harmonized compliance that builds capacity while safeguarding safety, resilience, and innovation.

1.2.1 Cross-Regime Alignment, Interoperability & Legal Coherence

This category centers on cross-regime alignment, interoperability, and legal coherence across the EU's dense digital rulebook. Stakeholders call for a clarified hierarchy among interlinked instruments (e.g., NIS2, DORA, GDPR, AI Act, Data Act), consistent terminology and risk methodologies across supervisory domains, and clear scoping of cybersecurity obligations, so that complex AI value chains spanning model providers, developers, and deployers can operate with legal certainty. Attention is also drawn to interactions between acts (e.g., AI Act with CRA on robustness and incident reporting), and to the uncertainty created by divergent governance regimes and compensation rules. Interoperability mechanisms and mutual recognition are seen as enablers of coherence:

a European Business Wallet as a single, reliable organizational identity (while keeping business and citizen wallets legally distinct), improved cross-border recognition of security clearances, and administrative streamlining. There are also proposals for cross-continental testbeds (e.g., data sandboxes, cyber resilience facilities, AI readiness ladders) to pilot simplified, interoperable compliance models, alongside strengthened enforcement of Single Market rules to reduce de facto fragmentation with tariff-like effects. Coordinated governance, guidance, and phased timelines emerge as practical levers: using Omnibus procedures to swiftly correct inconsistencies and reflect agency mandates (e.g., ENISA) while avoiding mandate overlap; integrating AI duties into sectoral frameworks; sequencing enforcement until harmonised standards exist; granting grace periods for general-purpose AI; and issuing clear guidance (e.g., copyright for open-source) that also mitigates IP conflicts created by disclosure obligations. An agile governance posture is recommended to keep regulation coherent as the ecosystem evolves.

> *We also emphasise the urgent need for the EU to clarify the hierarchy and order of prevalence among the various interlinked digital regulations (e.g. NIS2, DORA, GDPR, AI Act, Data Act) and with local/national laws.* (CGI Inc.)
>
> *The scope of different cybersecurity rules must be clear and coherent.* (FIGIEFA aisbl)
>
> *The unfinished single market has the same effect as if the member states were to impose tariffs of 44% on goods and 110% on services (IMF, 2024).* (WKÖ - Austrian Federal Economic Chamber)
>
> *ASRIC proposes concrete initiatives such as a Continental Data Sandbox, a Mutual Cyber Resilience Facility, an AI Readiness Ladder, and an African Digital Fitness Observatoryall designed to test and align simplified compliance models between the continents.* ()
>
> **:** Stresses that coordinated governance and collective action are the missing ingredients to achieve cross-regime alignment.
>
> *What is missing is not potential, but coordinated action.*
>
> **FERMA - Federation of European Risk Managers Associations:** Notes the AI ecosystem's multi-actor complexity, calling for interoperable roles and coherent responsibilities across the value chain.
>
> *The Al ecosystem is complex, with multiple actors involved in the value chain (model providers, system developers, deployers, etc.).*
>
> **Enel SpA:** Urges aligning the AI Act with ENISA's existing mandates to avoid duplication and ensure legal coherence across regimes.
>
> *Inclusion of targeted changes to reflect tasks already assigned to ENISA under other legislative acts.*
>
> **FIGIEFA aisbl:** Calls for clear, coherent scoping across overlapping cybersecurity rules to deliver consistent obligations.
>
> *The scope of different cybersecurity rules must be clear and coherent.*
>
> **CGI Inc.:** Requests a clarified hierarchy and precedence among EU digital laws and national rules to resolve conflicts and guide implementation.
>
> *We also emphasise the urgent need for the EU to clarify the hierarchy and order of prevalence among the various interlinked digital regulations (e.g. NIS2, DORA, GDPR, AI Act, Data Act) and with local/national laws.*
>
> **EUROMOT - The European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers:** Recommends coordinating corrections through the Commission's Omnibus Procedure to harmonize cross-regime inconsistencies.
>
> *EUROMOT recommends that the proposed corrections be addressed within the framework of the Omnibus Procedure announced by the European Commission.*
>
> **Docusign:** Advocates a single, interoperable European Business Wallet to streamline representation and administrative processes across jurisdictions.
>
> *The European Business Wallet should serve as a single, reliable means of identification for organisations, reflecting powers of representation and streamlining administrative processes.*

Volkswagen Group: Warns that fragmented governance and divergent compensation rules create significant uncertainty, underscoring the need for alignment.

The uncertainty that is cur- rently being created by different governance regimes and different compensation rules provided by the plentiful regulations is considerable.

Dun & Bradstreet: Promotes harmonized terminology, risk methodologies, and supervisory expectations across major frameworks to support legal coherence.

To support legal clarity and operational consistency, D&B encourages the Commission to promote alignment of terminology, risk assessment methodologies, and supervisory expectations across the AI Act, GDPR, ESG ratings, credit, and anti-money laundering frameworks.

Government Office of the Czech Republic: Supports swift endorsement of the Digital Omnibus to synchronize and harmonize EU digital regulations.

CZ recognises the need to endorse the Digital Omnibus swiftly.

Snap Inc.: Suggests integrating AI obligations into sectoral frameworks, phasing enforcement, and providing grace periods to enable coherent rollout.

The Commission should integrate AI obligations into existing sectoral frameworks, delay enforcement until harmonised standards are in place, and provide grace periods for general-purpose AI requirements.

Verisure: Encourages focusing ENISA's coordination within CRA and NIS2 to avoid overlaps and strengthen cross-regime coherence.

Focus ENISA's efforts on existing responsibilities and coordination tasks under the CRA and NIS2.

Ibec: Calls for stronger Commission processes to enforce Member State compliance and ensure consistent Single Market governance.

Lastly, we call for the strengthening of European Commission processes to assess/enforce Member State compliance with Single Market rules.

Namirial Spa: Proposes separating business and citizen wallet frameworks to reflect distinct representation models while enabling interoperability.

Separate the EUBW legal framework from the EUDI Wallet to reflect the distinct nature of business identities and representation models.

Schneider Electric: Highlights the need to align AI Act requirements with CRA provisions, especially on robustness and incident reporting.

Attention should be paid to the Al Act's interaction with other regulations, such as the CRA, notably regarding robustness and incident reporting (see section I. iii.).

Meta Platforms Ireland Limited: Warns that disclosure obligations risk intellectual property conflicts, urging balanced, coherent requirements across regimes.

Additionally, these requirements create unavoidable intellectual property conflicts, as disclosures may expose proprietary architectures and optimisation techniques.

Adigital (Asociación Española de la Economía Digital): Advocates agile governance and organizational adaptability to maintain coherence across evolving digital regulations.

Finally, agility in digital regulation governance is recommended, both in the design process and organizational dimension.

FiCom ry: Urges improved interoperability and mutual recognition of national security clearances to streamline cross-border compliance.

The EU should work to improve the interoperability and mutual recognition of national security clearance processes.

: Proposes EU-Africa coordination initiatives to pilot simplified compliance and enhance cross-regime interoperability.

ASRIC proposes concrete initiatives such as a Continental Data Sandbox, a Mutual Cyber Resilience Facility, an AI Readiness Ladder, and an African Digital Fitness Observatoryall designed to test and align simplified compliance models between the continents.

WKÖ - Austrian Federal Economic Chamber: Emphasizes the economic costs of fragmentation and urges completing the Single Market with coherent governance.

The unfinished single market has the same effect as if the member states were to impose tariffs of 44% on goods and 110% on services (IMF, 2024).

ACEA (European Automobile Manufacturers' Association): Seeks clear, harmonized guidance on copyright duties for open-source AI to avoid disproportionate liability for developers.

Clear guidance is needed on copyright obligations under the AI Act, especially for open-source models, to avoid disproportionate liability for developers.

1.2.2 Centralized Guidance & Aligned Definitions

Stakeholders call for centralized, practical guidance and aligned definitions to deliver predictable, consistent compliance across the EU. They seek consolidated guidance, templates, FAQs, and sector-specific advice issued early by central bodies, as well as clear scoping, monitoring, and terminology harmonized across adjacent frameworks to avoid conflicts. Harmonized Member State interpretation is seen as essential for multinational operations and investment. To operationalize this, respondents propose formal, binding pre-consultation pathways, mandated publication of interpretive guidance upon adoption, and roadmaps with phased timelines and cost-benefit justifications. They emphasize aligning thresholds and reporting timelines, clarifying edge cases (e.g., scope and support periods), reducing reliance on informal interpretations, providing guidance in local languages with easy-to-use compliance tools, and enabling future-proofing via delegated acts. Clear, early, and unified guidance lets operators focus on resilience and innovation instead of navigating ambiguity.

LightingEurope calls for clear and practical guidance for expected outcomes when carrying out product risk assessments under the CRA, and advises the Commission to strive for consistent harmonisation of terminology between the CRA and other EU product legislation to prevent inconsistencies. (LightingEurope)

The EU should provide formal guidance, request a cost-benefit analysis for any provisions proposed to be retained, and publish a roadmap with key timelines to achieve simplification. (GSMA)

Empower the Commission to adopt delegated acts for future-proofing. (Meta Platforms Ireland Limited)

Structured dialogue with Notified Bodies helps, but a formalized pre-consultation pathway providing binding guidance would improve predictability. (Epic Systems)

Epic Systems: Calls for a formal, binding pre-consultation pathway with Notified Bodies to centralize guidance and increase predictability for compliance.

Structured dialogue with Notified Bodies helps, but a formalized pre-consultation pathway providing binding guidance would improve predictability.

LightingEurope: Requests clear, practical CRA guidance on product risk assessments and harmonized terminology across EU product laws to avoid inconsistencies.

LightingEurope calls for clear and practical guidance for expected outcomes when carrying out product risk assessments under the CRA, and advises the Commission to strive for consistent harmonisation of terminology between the CRA and other EU product legislation to prevent inconsistencies.

European Energy Information Sharing and Analysis Centre: Advocates clear, consolidated guidance to streamline compliance so operators can focus resources on building resilience.

Clear, consolidated guidance will improve compliance while allowing operators to focus resources on building resilience capabilities.

Intesi Group: Highlights that legal ambiguity and uneven eIDAS application across Member States require harmonized, centralized interpretations to reduce risk and enable investment.

Legal ambiguity and inconsistent application of the eIDAS framework across Member States create risks and hinder investment, making it hard to develop new products.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Urges coordinated, joint guidance for startups from the EU AI Office and the EDPB to ensure consistent expectations.

Develop joint guidance for startups through cooperation between the EU Al Office and the European Data Protection Board.

GSMA: Calls for formal EU guidance paired with a simplification roadmap and evidence-based review to provide clear timelines and reduce burdens.

The EU should provide formal guidance, request a cost-benefit analysis for any provisions proposed to be retained, and publish a roadmap with key timelines to achieve simplification.

Telefonica, S.A.: Seeks centrally defined jurisdiction and scope of NIS2 obligations, developed through close dialogue with industry to ease supervision.

The jurisdiction and scope of obligations should be clearly defined to simplify the supervision of operators providing NIS2-regulated services (e.g., connectivity, but also managed services, DNS, or cloud), ideally through close dialogue with industry.

National Land Survey of Finland: Asks for clearer, centralized guidance on how compliance monitoring should be conducted and assessed.

Mon- itoring of compliance needs to be clarified.

LSEG: Encourages the AI Office to publish practical guidance, templates, and FAQs well before application to clarify obligations.

The AI Office should issue practical guidance, templates, and FAQs well ahead of the Act's application date in order for businesses to understand their obligations.

Ibec: Identifies unclear definitions in the AI Act and calls for aligned terminology to clarify market-scope determinations for multinational models.

There is a lack of clarity on the definition of "putting into use on the market" in the Al Act, which is causing confusion for multinational entities on whether their Al models are in scope.

Emerson Electric Co.: Requests specific Commission guidance on determining support periods across licensing models and serially manufactured hardware under Article 26.

In anticipation of the guidance coming from the Commission regarding support periods under Article 26, we would appreciate specific clarification on how to determine support periods for different licensing arrangements (e.g., perpetual vs subscription licensing), as well as hardware products that are manufactured serially in the industrial space.

Meta Platforms Ireland Limited: Supports empowering the Commission to issue delegated acts to keep guidance future-proof and coherent.

Empower the Commission to adopt delegated acts for future-proofing.

Finnish Food and Drink Industries´ Federation (ETL): Calls for harmonized interpretations and guidance across Member States so multinational companies face consistent practices.

Member States guidance and interpretation should also be harmonised to ensure that internationally operating companies can operate under similar practices regardless of the Member State to which they report.

Adigital (Asociación Española de la Economía Digital): Recommends mandatory issuance of interpretive guidance aligned with adjacent frameworks when new regulations are adopted.

Recommendation: When a regulation is adopted, it should be mandatory to publish guidance on its interpretation in conjunction with adjacent frameworks.

ING Group: Seeks clearer EU-level, sector-specific guidance to resolve conflicting obligations and ensure consistent compliance.

It would help to have clearer EU-level sector-specific guidance on handling conflicting obligations.

Union of Entreprenuers and Employers: Advocates aligning thresholds and reporting timelines to avoid premature or repetitive notifications and enable thorough investigations.

Alignment of thresholds and timelines would help avoid premature or repetitive notifications and allow organisations sufficient time to complete internal investigations before submitting final reports.

Alcon Laboratories Inc: Urges more consistent, formal MDCG guidance to reduce reliance on informal interpretations and improve predictability.

Improve MDCG guidance consistency and reduce reliance on informal interpretations.

: Emphasizes transparent rules, localized guidance in national languages, and accessible compliance tools to balance efficiency and accountability.

Transparency in rules, clear guidance documents in local languages (such as Czech), and easy-to-use compliance tools would be key to balance efficiency with accountability.

: No substantive input on centralized guidance, aligned definitions, or phased timelines is available in this document.

1.2.3 Coordinated Oversight, One-Stop Shop & Unified Reporting

Stakeholders call for coordinated oversight built on a main-establishment, one-stop-shop model to curb fragmentation across AI, cybersecurity, data protection and sectoral rules. Divergent national interpretations, overlapping competent authorities and local add-ons create legal uncertainty and duplicative obligations, making unified security and compliance strategies hard to execute. Consistent enforcement should be driven by stronger EU-level coordination, alignment between the Commission and EDPB, and mutual recognition among market surveillance authorities, so that firms face single registration/supervision and clear jurisdiction, avoiding multiple reporting for a single incident. To operationalize this, respondents propose EU guidance to rationalize and minimize the number of authorities, and to harmonize reporting formats, information requirements, processes and timelines. They urge cross-regulatory integration via the EU AI Office, joint guidance (e.g., AI Office with EDPB), and coordination among ENISA, the ECB and national bodies; sectoral coordination within EMA for high-risk or combination products; and dedicated coordinating units to oversee data-sharing initiatives. Given the anticipated proliferation of authorities and complex oversight landscape, they also advocate transparency and monitoring of implementation and early-warning mechanisms to detect fragmentation and other systemic risks early.

The EC should enforce the intent behind the One Stop Shop and ensure that organisations are registered and supervised by only a single Member State, determined by the NIS jurisdictional criteria. (Amazon)

For highly interconnected, cross-border sectors such as transport and logistics, a "main establishment" concept should allow single registration and coordination for groups operating in multiple Member States, avoiding duplicative registrations and divergent local add-ons. (European Express Association (EEA))

The enforcement landscape under the AI Act is also quite complex, as over 200 competent authorities are expected to be designated. (Mastercard Europe SA)

For example, in the consumer protection domain, Spain has 17 regional consumer authorities in addition to the competent national ministry. (Adigital (Asociación Española de la Economía Digital))

: Proposes revising competition policy to enable ex-post merger enforcement, flexible state aid, and agile procedures with tight deadlines, strengthening streamlined and transparent oversight.

In this regard, the whole "EU Competition Policy Toolbox" should be revi- sed, in particular by adjusting merger rules and introdu- cing greater possibilities to enforce merger conditions ex-post, by

allowing more flexible state-aid policies in strategic sectors, and by establishing agile procedures, tighter deadlines, and transparent decision-making pro- cesses.

FERMA - Federation of European Risk Managers Associations: Advocates extending the main establishment principle across cybersecurity regimes to reduce duplicative supervision and promote one-stop coordination.

Another possibility is to expand the application of the 'main establishment' principle across all cybersecurity legislation.

Technology Industries of Finland: Calls for stronger EU-level coordination to achieve consistent enforcement and reduce fragmentation.

Consistent enforcement requires stronger EU coordination.

Volkswagen Group: Warns that national add-on rules under the ePrivacy Directive create divergent interpretations among authorities, underscoring the need for harmonized oversight.

Implemented into national law, the ePD allows Member States to establish addi- tional rules, with the result that interpretation and enforcement vary among Data Protection Authori- ties (DPAs) and with Telecommunications Regulators.

EMMA-ENPA: Urges alignment between the European Commission and the EDPB to prevent legal uncertainty and ensure consistent governance.

Against this background, we would like to highlight that a consistent approach between the Commission and the EDPB is a precondition to avoid legal uncertainty.

FEBIS: Highlights that creditworthiness AI is classified as high-risk, implying coordinated sector-specific oversight and clear supervisory roles.

FEBIS draws attention to the inclusion of creditworthiness assessment systems under Annex III of the Al Act as "high-risk Al".

Dun & Bradstreet: Supports stronger transparency and monitoring of implementation to improve coordinated enforcement.

Finally, we strongly support the Commission's efforts to improve transparency and monitoring of implementation.

Eurofinas: Seeks coherent, consistent rules across Member States to prevent Single Market fragmentation and contradictory obligations.

Regulatory coherence and consistency across Member States, preventing fragmentation of the Single Market and contradictory obligations.

German Insurance Association: Welcomes designation of financial supervisors as market surveillance authorities for financial services, clarifying competent oversight within the sector.

We welcome the fact that Article 74 (6) of the AI Act provides for the financial su- pervisory authority to be the competent market surveillance authority for the finan- cial services sector.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Notes the AI Act network of national authorities lacks integration with data and cyber regulators, calling for cross-regulatory coordination.

The AI Act introduces a new network of national competent authorities but lacks a clear cross-regulatory integration mechanism with data and cyber regulators.

Telefonica, S.A.: Recommends mutual recognition and cooperation among national authorities to streamline compliance and oversight.

Facilitate mutual recognition and cooperation between national authorities.

Bitkom e.V.: Points to divergent interpretations and enforcement across Member States that hinder unified security strategies, calling for harmonized oversight.

In particular, for companies operating across multiple Member States, divergent interpretations and enforcement practices create uncertainty and risk of inconsistent compliance, making it difficult to implement a unified security strategy.

Amazon: Urges enforcing a true one-stop shop under NIS so organizations have a single supervising Member State.

The EC should enforce the intent behind the One Stop Shop and ensure that organisations are registered and supervised by only a single Member State, determined by the NIS jurisdictional criteria.

ENGIE: Encourages EU guidance to minimize the number of competent authorities and harmonize reporting formats and processes for generic obligations.

Firstly, we encourage the Commission to consider providing Member States with guidance to rationalise the appointment of the national competent authorities by minimising their number and harmonise to the extent possible the type of information, format and process for reporting, especially for generic obligations.

Mastercard Europe SA: Warns of enforcement complexity under the AI Act due to hundreds of competent authorities and calls for streamlined coordination.

The enforcement landscape under the AI Act is also quite complex, as over 200 competent authorities are expected to be designated.

European Express Association (EEA): Proposes a main establishment concept enabling single registration and coordination for cross-border groups to avoid duplicative local requirements.

For highly interconnected, cross-border sectors such as transport and logistics, a "main establishment" concept should allow single registration and coordination for groups operating in multiple Member States, avoiding duplicative registrations and divergent local add-ons.

Emerson Electric Co.: Requests clear determination of main establishment to avoid multiple reporting of a single incident across countries.

Organizations need clear legal certainty regarding their country of main establishment not only for each separate legislation, but also to prevent multiple reporting to multiple countries for one single incident.

Meta Platforms Ireland Limited: Warns that fragmented governance fosters divergence and legal uncertainty, risking failure to harmonize AI rules across the EU.

Coupled with a fragmented governance structure that fosters regulatory divergence and legal uncertainty, the AIA risks failing its core objective of harmonising AI rules across the EU.

Finnish Food and Drink Industries´ Federation (ETL): Advocates a GDPR-like harmonisation mechanism to prevent simultaneous multi-authority actions against the same IoT product.

A harmonisation procedure similar to the GDPR should be implemented to avoid situations where an IoT product is simultaneously subject to decisions and penalties from multiple national authorities.

Adigital (Asociación Española de la Economía Digital): Illustrates fragmentation with numerous regional consumer authorities, emphasizing the need for streamlined and coordinated oversight.

For example, in the consumer protection domain, Spain has 17 regional consumer authorities in addition to the competent national ministry.

ING Group: Observes AI Act supervision is nationally based and suggests coordination to ensure consistency across borders.

Supervision on the AI Act that is currently in implementation, is also on a national basis.

Union of Entreprenuers and Employers: Calls for greater coordination among ENISA, the ECB, and national authorities to enhance consistent enforcement.

Increased coordination between ENISA, the European Central Bank, and national authorities would also strengthen consistency.

Anitec-Assinform: Proposes AI Office coordination and mutual recognition among market surveillance authorities to harmonize enforcement.

Streamline and harmonize enforcement through Al Office coordination and MSA mutual recognition

European AI Forum: Recommends joint guidance for startups from the EU AI Office and the EDPB to align interpretations and reduce fragmentation.

Develop joint guidance for startups through cooperation between the EU Al Office and the European Data Protection Board.

Alcon Laboratories Inc: Calls for centralized EMA coordination for high-risk and combination products to streamline oversight.

Establish centralized coordination within EMA for high-risk and combination products.

ACEA (European Automobile Manufacturers' Association): Suggests a dedicated central coordinating unit for data sharing initiatives to avoid duplication and resolve regulatory conflicts.

Designate a dedicated coordinating unit to serve a central point of reference for all legislative initiatives on data sharing, to help avoid duplication, resolve conflicts and promote regulatory coherence across the board.

AI & Partners B.V.: Argues non-legislative support can reduce red tape and promote uniform enforcement, aiding smaller firms and a more dynamic single market.

Non-legislative support can cut red tape, foster uniform enforcement, and enable smaller firms to adopt AI responsiblywhile Europe simultaneously pursues sovereignty through targeted investment in emerging technologies, stronger innovation ecosystems, and a more dynamic single market.

: Suggests early-warning mechanisms to detect power concentration, abuse, or fragmentation to inform coordinated oversight.

They could also serve as an early warning system to detect power concentration, abuse or fragmentation in a timely manner.

1.2.4 Proportional Scope, Simplification & Predictable Enforcement

This category stresses keeping regulatory scope proportional, simplifying obligations, and making enforcement predictable through coordinated EU guidance and phased timelines. It prioritizes one-in-one-out discipline, systematic ex-post evaluations and fitness checks to ensure coherence and fitness-for-purpose across the policy cycle. When standards or downstream measures are delayed, alternative compliance mechanisms and stop-the-clock or soft-landing approaches help avoid rushed, high-burden implementations. Predictability depends on clear, consistent guidance that stays within primary legislative mandates and clarifies what is in or out of scope. Stakeholders call for uniform application of the AI Act across Member States, targeted adjustments over new layers of rules, and adaptive, machine-readable obligations. These guardrails limit over-interpretation in secondary acts, ensure proportional accountability, and align compliance with realistic innovation cycles, reducing fragmentation and unintended consequences.

With the AI Act entering into force, simplification should provide predictability in its application across Member States. ()

As a long-term supporter of the 'one-in, one-out approach', CZ welcomes the Commission's recognition of its importance. (Government Office of the Czech Republic)

Google, Meta, and Microsoft have turned off political advertising in the EU rather than risk falling afoul of unclear rules around political ads. (The International Center for Law & Economics)

Introduce mechanisms for ex-post impact assessment at the final stage of the legislative process (i.e. after trilogue negotiations but before formal adoption) to help identify and mitigate unintended consequences and administrative burdens. (Snap Inc.)

: Proposes independent oversight and systematic ex-post evaluations to ensure laws stay fit for purpose and enforcement remains consistent across the policy cycle.

Alongside a more empowered European Court of Auditors, the new Board would be sufficiently resourced to conduct ex- post evaluations more systematically and to monitor the entire EU policy cycle, ensuring that all adopted EU laws are fit for purpose, that the Better Regulation agenda is implemented, and the 2023 Better Regulation Toolbox is assiduously followed for any new legislative initiative.

TIC Council: Calls for activating alternative compliance mechanisms when standards are delayed to keep obligations proportionate and predictable.

ctivate the use of alternative compliance mechanisms4 envisioned in the Al Act (Art. 41) when standards are delayed.

ZVEI e.V.: Urges the Commission to avoid adding new obligations and to evaluate impacts before changing core rights and duties, ensuring stable scope and burdens.

The European Commission should not introduce new obligations, modify the core rights and duties, or impose requirements that goes beyond the current regulatory framework.

Docusign: Supports targeted, limited adjustments and simplification in data, AI, and digital identity to reduce complexity while improving legal clarity.

We strongly support these objectives, particularly in the areas of data, AI, and digital identity, where simplification can deliver real benefits for businesses and users alike.

eco - Verband der Internetwirtschaft e.V.: Warns that rapid, frequent regulatory cycles strain both companies and regulators, arguing for more predictable timelines.

At the same time, it is necessary to understand, that the short cycles of regulation pose a challenge to companies and regulators alike.

German Insurance Association: Requests simplifications like a stop-the-clock mechanism for IRRD to prevent disproportionate administrative burdens during implementation.

We therefore believe simplifications such as the Stop the clock for the Insurance Recovery and Resolution Directive, for example, which will cause significant additional administrative effort for insurers, are needed.

Government Office of the Czech Republic: Backs cumulative evaluations like a Digital Fitness Check and supports one-in-one-out to control regulatory scope and complexity.

CZ preliminarily supports the proposed "Digital Fitness Check" initiative, which aims to assess the coherence and cumulative effect of rules on the digital economy.

Snap Inc.: Advocates an ex-post impact check before formal adoption to catch unintended burdens and improve proportionality.

Introduce mechanisms for ex-post impact assessment at the final stage of the legislative process (i.e. after trilogue negotiations but before formal adoption) to help identify and mitigate unintended consequences and administrative burdens.

Bitkom e.V.: Highlights uncertainty and heavy administrative burdens under the CRA and urges timely downstream measures so firms have adequate preparation time.

The downstream measures required to operationalise the CRA remain delayed, leaving manufacturers with insufficient time for preparation.

Seznam.cz, a.s.: Argues that certain guidance exceeds the DSA's legal scope, calling for alignment strictly with Article 15 to maintain proportionality.

The Annex II, part II, section 2 contains several areas that provide instructions beyond the scope of Art. 15. of the DSA, especially in indicators Meaningful and comprehensible information regarding content moderation engaged in at the providers' own initiative and Qualitative description of indicators of accuracy and possible rate of error of automated means .

European Express Association (EEA): Calls for management accountability rules that are proportionate to actual risk to sustain trustful, balanced supervision.

It is overall necessary to guarantee that provisions involving personal accountability for non-compliance are proportionate to the specific risks entailed.

Infosys Limited: Supports simplification while ensuring supervisory authorities retain full investigative powers for predictable, effective enforcement.

Under this simplification, supervising authorities retain full investigative powers.

The International Center for Law & Economics: Notes that unclear political advertising rules have driven platforms to disable ads, underscoring the need for clear, predictable obligations.

Google, Meta, and Microsoft have turned off political advertising in the EU rather than risk falling afoul of unclear rules around political ads.

Schneider Electric: Urges secondary acts and guidance to stay within primary law mandates to prevent scope creep and maintain proportionality.

Secondary acts and guidance should remain strictly within the mandate and scope defined in their primary legislation.

Meta Platforms Ireland Limited: Flags the AI Act's indefinite post-market monitoring and updating duties as unpredictable and potentially disproportionate, seeking clearer temporal limits.

Furthermore, the AIA imposes post-market monitoring obligations that extend indefinitely, without a clearly defined temporal scope.

Finnish Food and Drink Industries´ Federation (ETL): Requests clarification of mandatory contractual obligations across complex supply chains to ensure proportionate, predictable responsibilities.

The mandatory contract obligation in extensive supply chains should be examined and clarified.

Vodafone Group: Seeks clear guidance on scope and compliant use cases (e.g., whitelists) to deliver predictable application of current rules ahead of broader reforms.

Issue guidance on how the current framework would apply to new and innovative use cases including a non-exhaustive 'whitelist' of use cases assumed to be compliant under the current rules.

FiCom ry: Insists every new rule be preceded by impact assessment and warns that regulatory complexity harms market functioning and product availability.

The core principle is simple: every new regulation must be preceded by an impact assessment.

2Dyles Services: Proposes extending responsibility to users with logging and monitoring duties so accountability is proportionate to where risks arise.

Users should have clear responsibilities, with obligations for logging, monitoring, and usage declarations to expand accountability beyond developers.

WKÖ - Austrian Federal Economic Chamber: Calls for a tightly scoped, evidence-based ENISA role with transparent recommendations, reflecting its non-policymaking mandate.

It is therefore all the more important that ENISA not only supports the Member States and their institutions in line with the questions raised in the first section, but above all is transparent with regard

to its purely evidence-based recommendations, precisely because, as mentioned at the beginning, it is not a political decision-maker.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Asks for faster, more flexible funding procedures aligned with rapid innovation cycles to reduce bureaucracy and improve timely implementation.

The Commission should implement significantly faster and more flexible funding procedures for microelectronics projects, aligned with the sector's rapid innovation cy- cles.

: Promotes adaptive regulation built on continuous monitoring, clear triggers, and machine-readable obligations to combine certainty with responsiveness.

It rests on operational principles (continuous data monitoring, clear triggers, distributed learning institutions, and machine-readable obligations) that make regulation both legally certain and technologically responsive.

: Urges coordinated EU-level guidance for the AI Act to deliver predictable, harmonized application and avoid fragmentation.

A coordinated EU-level approach, with consistent guidance, is essential to avoid fragmentation and to build trust in the emerging AI ecosystem.

Fédération des Industries Ferroviaires: Advocates aligning obligations, support, and cost recovery with industry lifecycles to keep compliance proportionate and manageable.

FINANSFORBUNDET (CVR 15320613): Calls for predictable, harmonized application of the AI Act to support planning and compliance.

Elia Group: Requests uniform AI Act implementation across Member States to ensure clarity and avoid fragmentation.

VDMA - Advancing Europe´s machinery industry: Opposes retroactive CRA compliance and urges phased, forward-looking obligations to preserve legal certainty.

U.S. Chamber of Commerce: Calls for transparent guidance and predictable timelines so businesses can adapt compliance processes quickly without constant rule changes.

Polish Confederation Lewiatan: Urges limiting reliance on soft law and clarifying delegated powers to keep rules within a clear, proportionate scope.

Association of Consumer Credit Information Suppliers: Stresses legal predictability and effective implementation support rather than expanding obligations.

European Justice Forum: Calls for assessing cumulative impacts and administrative burden to prevent overregulation and ensure proportional scope.

Ecommerce Europe: Opposes expanding EDPB’s remit beyond its mandate, seeking a proportionate and clearly delimited scope.

ITI - Information Technology Industry Council: Highlights complex, multi-layered enforcement as a burden for businesses and calls for streamlined, coordinated oversight.

Federation of European Securities Exchanges: Notes enforcement challenges on decentralized networks and seeks proportionate, workable approaches.

Verband der Automobilindustrie e.V.: Proposes request-based oversight to cut bureaucracy and urges a clearer, phased CRA scope and timing for predictable compliance.

The Guild of European Research-Instensive Universities: Supports timely framework revisions but warns against omissions in scope that undermine clarity and predictability.

TikTok Technology Ltd.: Requests clear, consistent enforcement mechanisms for the Transparency Code to avoid uncertainty.

Brunel University of London: Calls for public simplification roadmaps with phased timelines to provide predictability during transitions.

Google: Warns that early DMA enforcement has created friction and urges clear, prioritized enforcement guidance and a focus on implementation over new rules.

Business Software Alliance: Advocates stability and full implementation of existing frameworks before introducing changes, to maintain predictability.

Eurochambres: Supports regular reviews and consistent, coordinated enforcement to keep obligations proportionate and clear.

Broadcom: Asks for clarifications and guidance rather than new burdens to simplify compliance.

Orgalim - Europe's Technology Industries: Recommends limiting regulatory obligations to the digital support period to ensure proportional lifecycle requirements.

Cigref: Seeks precise thresholds for what constitutes a substantial modification to avoid overbroad obligations and unpredictable enforcement.

NDM: Proposes an observatory model to inform policy as an alternative to detailed prescriptive legislation, reducing complexity.

CIO Platform Nederland: Recommends guidance-first approaches and restraint on fines during initial rollout to enable predictable, proportionate compliance.

Usercentrics: Advocates reducing compliance friction for businesses and users without centralizing data or control.

Clever Cloud: Supports soft-landing periods and flexible simplification to accommodate varied readiness while maintaining compliance goals.

Computer & Communications Industry Association (CCIA Europe): Calls for procedural fairness and hearing rights for gatekeepers and warns that subjective B2G needs create unpredictable burdens.

SAP SE: Warns that retroactive application of rules harms businesses and undermines predictability.

Danish Industry: Flags risks from retroactivity and premature enforcement before guidance is in place, urging phased application.

Middle Tech Europe: Suggests tackling consultation fatigue and enabling permit bundling to streamline processes and timelines.

DIGITALEUROPE: Urges postponing Data Act obligations to reduce overlap and preserve predictability while maintaining agreed political balances.

European Society of Radiology: Supports coherent, safety-focused implementation with consistent guidance to avoid fragmentation.

VAUNET - German Association of Private Media: Encourages prioritizing enforcement of existing laws before adding new regulations to ensure stable, predictable frameworks.

1.2.5 Standards-Aligned Phased Timelines & Grace Periods

This category captures a broad consensus to sequence regulatory obligations with the maturity of harmonised European standards, guidance, and secondary acts. Stakeholders ask for clear, predictable transition periods so requirements apply only after the necessary technical benchmarks and interpretative materials are available—

commonly proposing a buffer (e.g., at least 12 months) after standards are published, alongside timely guidance to ensure legal and technical certainty. They also caution against overlapping or uncoordinated rulemaking and premature national implementation until the core EU frameworks are fully operational. Implementation should be phased and sector-aware, with milestone-based runways and targeted grace periods that reflect real product development cycles and build capacity in conformity assessment bodies and competent authorities. Many highlight misalignments between current timelines and standards work, calling for cross-regime coordination (AI Act, CRA, Data Act, MDR/IVDR). Concrete proposals range from focused six-month technical extensions for CAB readiness to broader 24–36 month extensions for complex regimes—aimed at improving compliance quality, safety, and innovation outcomes by aligning timing with workable standards and guidance.

> *Link transition periods to the availability of harmonised European standards to ensure legal and technical certainty.* (ZVEI e.V.)
>
> *Delay the entry into application of high-risk requirements until 12 months after relevant harmonised standards are available, based on past examples (e.g., Medical Device Regulation).* (Technology Industries of Finland)
>
> *Push back the current deadlines by: CRA = 36 months, AI Act = 24 months.* (SIEMENS AG)
>
> *Further, the TIC industry could support a limited and clearly defined technical extension of up to six months, solely to ensure that CABs are notified in due time and, hence, are eligible to carry out conformity assessments for high-risk AI systems in line with the AI Act.* (TIC Council)

DATEV eG: Reports delays in CRA downstream initiatives, underscoring the need for adjusted and coordinated implementation timelines.

The downstream initiatives required to implement the Cyber Resilience Act (CRA) are still pending and continue to be delayed.

FERMA - Federation of European Risk Managers Associations: Advocates sequencing sector-specific rules after the AI Act framework is fully operational to ensure smooth, coordinated implementation.

To ensure smooth implementation, FERMA advises delaying sector-specific rules until the AI Act framework becomes fully operational.

Verband kommunaler Unternehmen e.V.: Notes and supports discussions to postpone the AI Act's entry into force, favoring a phased timeline.

The VKU is following the discussions around postponing the entry into force of the AI Act.

SIEMENS AG: Requests substantial deadline extensions—36 months for the CRA and 24 months for the AI Act—to enable realistic compliance.

Push back the current deadlines by: CRA = 36 months, AI Act = 24 months.

TIC Council: Supports a limited technical extension to align the notification and capacity of conformity assessment bodies with AI Act timelines.

Further, the TIC industry could support a limited and clearly defined technical extension of up to six months, solely to ensure that CABs are notified in due time and, hence, are eligible to carry out conformity assessments for high-risk AI systems in line with the AI Act.

ZVEI e.V.: Urges linking transition periods to the availability of harmonised standards to provide legal and technical certainty.

Link transition periods to the availability of harmonised European standards to ensure legal and technical certainty.

Enel SpA: Calls for delayed enforcement until guidance, certification schemes, and competent authorities are operational.

Enel supports simplification and calls for delayed enforcement until (i) guidance, (ii) certification schemes, and (iii) competent authorities are operational.

Zimmer Biomet: Stresses that successful implementation requires more time and predictability across the EU digital agenda.

The European Union's digital agenda is ambitious and forward-looking, yet its successful implementation demands greater time and predictability.

Technology Industries of Finland: Proposes applying high-risk AI requirements only 12 months after relevant harmonised standards are available.

Delay the entry into application of high-risk requirements until 12 months after relevant harmonised standards are available, based on past examples (e.g., Medical Device Regulation).

Workday: Calls for correct, consistent implementation and avoiding additional overlapping AI rules during the current mandate.

For the Al Act to succeed, it requires correct, consistent implementation, and the EU should avoid additional AI regulation during this mandate (such as proposals on AI in the workplace, currently being discussed by the European Parliament).

Volkswagen Group: Highlights misalignment between implementation timelines and the availability of harmonised standards, urging synchronization.

However, their im- plementation timelines and the availability of harmonized standards are not aligned.

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Supports extending AI Act application deadlines for MDR/IVDR-governed AI systems beyond August 2027, providing sectoral grace periods.

COCIR supports extending the AI Act application deadline for MDR/IVDR-governed AI systems beyond 2 August 2027.

Unipol Assicurazioni S.p.A.: Calls for realistic, phased implementation timelines to enable orderly compliance.

iii) The adoption of realistic and phased implementation timelines.

Video Games Europe: Requests a grace period for the Data Act rollout to safeguard user experience and implementation quality.

For the roll-out of the Data Act, a grace period is needed to ensure a better and safer user experience

GSMA: Asks for clear minimum transition periods in new regulations to allow companies to prepare.

New regulations should also provide minimum and clear transition periods to allow companies to prepare and implement necessary measures.

Telefonica, S.A.: Links effective AI Act implementation to the timely development and adoption of guidelines and harmonised standards.

The effective implementation of the AI Act likewise depends on the timely development and adoption of guidelines and harmonised standards, particularly for high-risk AI systems.

ANIE Federazione - ANIE ASSIFER: Warns that typical railway product development cycles exceed CRA timelines, necessitating longer transitions.

The development time of railway products, which in most cases exceeds 5 years, is not compatible with the 36-month implementation period of the CRA.

ING Romania: Urges postponing high-risk AI obligations until 12 months after harmonised standards are published.

Postpone high-risk AI obligations until 12 months after harmonised standards are published to ensure realistic compliance timelines.

Bitkom e.V.: Suggests a later fixed deadline for public-authority high-risk AI, providing an extended transition window.

In any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps to comply with the requirements and obligations of this Regulation by 2 August 2030.»

Amazon: Calls for coordination between sectoral legislation and cybersecurity frameworks to avoid conflicting timelines.

Ensure coordination between sectoral legislation (DSA, CSAM) and cybersecurity frameworks.

Verisure: Seeks to align reporting obligations with the CRA's overall applicability date for coherent phasing.

In particular, the reporting obligations should become applicable on 11 December 2027, in line with the overall CRA applicability date.

Trellix: Advocates adjusting CRA timelines to align with the development of necessary technical standards.

Ensuring a Pragmatic Implementation of New Rules: Adjusting the timeline for the Cyber Resilience Act to align with the development of necessary technical standards.

Bolt: Requests predictable transition periods and coordinated guidance to support implementation.

Provide predictable transition periods and coordinated guidance to support implementation.

Leading Baltic tech and other businesses and professional associations listed in the submission: Urges a pause and recalibration of the EU's AI regulatory approach to ensure manageable timelines.

In light of recent developments, we urge the EU to pause and recalibrate its approach to AI regulation.

Ibec: Supports applying high-risk requirements only after relevant harmonised standards are published, with time to adapt.

Apply high risk requirements after relevant harmonised standards are published, allowing sufficient time for adaptation.

Namirial Spa: Notes inconsistent implementation calendars across digital acts and calls for harmonization.

The regulatory implementation calendars across digital acts are inconsistent.

Schneider Electric: Recommends publishing secondary acts and key guidance at least 12 months before requirements apply.

Secondary acts and important guidance should be published at least 12 months before the applicability of the related requirements.

Meta Platforms Ireland Limited: Highlights the absence of established standards and consensus metrics for advanced models, arguing for timeline adjustments.

However, such standards have not yet been established, and there is currently no consensus within the field regarding appropriate metrics or thresholds for evaluating advanced AI models.

Finnish Food and Drink Industries´ Federation (ETL): Advocates deferring technical obligations until standardized frameworks are in place and companies have time to integrate them.

The implementation of the more technical obligations of the AI Act should be deferred until standardised frameworks are established for companies, allowing them adequate time to incorporate these standards into their operations.

Adigital (Asociación Española de la Economía Digital): Warns against premature or uncoordinated national implementation, urging coordinated phasing.

Premature or uncoordinated national implementation of EU rules.

Panasonic Europe B.V.: Proposes a 36-month staged runway for digitised compliance and prioritising harmonised standards over temporary specifications.

Digitisation of product compliance needs realistic timelines: adopt a 36month runway (with staged milestones) for Digital Product Passports and digital technical files, include the CRA in scope, unify digital contact around the GPSR electronic address and drop mandatory printed postal addresses, limit use of temporary common specifications in favour of harmonised standards, and permit digitalonly instruction manuals except where a specific standard mandates paper.

ING Group: Calls to postpone high-risk AI obligations until 12 months after harmonised standards are published to ensure realistic timelines.

AI Act: Postpone high-risk AI obligations until 12 months after harmonised standards are published to ensure realistic compliance timelines.

Entrust SAS: Urges realistic timelines, expanded accredited capacity, and precise definitions in eIDAS implementing acts for consistent enforcement.

The eIDAS implementing acts must adopt realistic timelines, expand accredited capacity, and deliver precise definitions to ensure consistency in enforcement.

Almega: Points to misalignment between guideline publication and high-risk applicability, suggesting coordination or delay.

The Commission's guidelines for high-risk Al are expected to be published in February 2026, while the sections of the AI Act concerning high-risk systems will start to apply from August 2026.

FiCom ry: Recommends extending AI Act and Data Act transition periods to enable evaluation and simplification.

The EU should extend the transition periods for the Al Act and Data Act to conduct a detailed evaluation and simplification of their provisions.

Union of Entreprenuers and Employers: Supports a phased, adaptive implementation model so guidance can evolve with technology.

Finally, a phased and adaptive implementation model would allow guidance to evolve with technology.

Anitec-Assinform: Calls for realistic implementation timelines aligned with the availability of harmonised standards.

realistic implementation timelines aligned with standards availability,

European AI Forum: Observes that the AI Act timeline is overly ambitious and often unachievable, warranting adjustments.

Since the Al Act's entry into force in 2024 and with the first provisions becoming applicable, it has become clear that the timeline as well as the implementation in general prove to be quite ambitious and, in several cases, could not be met.

ACEA (European Automobile Manufacturers' Association): Recommends a 24-month delay for high-risk AI rules with clarifications and scoped exemptions, enabling phased compliance.

We recommend delaying high-risk AI rules by 24 months, aligning the Act's biometric definitions with the GDPR's, limiting high-risk emotion recognition, granting intra-group and open-source AI exemptions, and clarifying copyright obligations.

UNIFE: Proposes pausing the application of the Data Act and AI Act by 24 months to allow preparation.

Propose to pause the application of the Data Act and the Artificial Intelligence Act by 24 months.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Urges extending key implementation deadlines by at least 24 months to ensure realistic compliance.

The Implementation Deadlines for Annex I and Annex III should be ex- tended by at least 24 months.

American Chamber of Commerce to the EU: No specific position on standards-aligned phased timelines or grace periods was provided.

1.2.6 Capacity Building & Conformity Assessment Infrastructure

This category centers on building the people, processes, and institutions needed to make coordinated governance workable, with a particular focus on conformity assessment capacity and practical guidance. It calls for streamlined compliance structures and clearer technical standards, rapid designation of notifying authorities, accelerated accreditation and expansion of Conformity Assessment Bodies, and standardized procedures and timelines across Member States to reduce fragmentation. Clear, measurable definitions and independent measurement frameworks are emphasized to support consistent enforcement and trust. To translate rules into action, stakeholders urge the Commission and Member States to provide practical implementation support: actionable guidance, toolkits, templates, trainings, checklists, and easily reachable helpdesks or dedicated support centers, complemented by EU-wide awareness campaigns (especially for SMEs). They advocate regulatory education that clarifies how laws interact and the real implications of non-compliance, broader sharing of lessons learned (e.g., from generative AI use cases), and wider use of RegTech/SupTech and centrally provided tools to reduce burden and improve coherence. Existing guidance that is overly abstract should be complemented with concrete examples, best practices, and hands-on materials. Given capacity constraints, the category stresses realistic, phased timelines and transitional measures to avoid bottlenecks—using pilots and sandboxes before EU-wide rollout, aligning rollout with accredited supply, and temporarily accepting equivalent testing (e.g., ISO/IEC 17025) while capacity scales. These steps are framed as essential to avoid delays seen in prior digital health and AI standardization efforts and to ensure harmonized, effective implementation across the EU.

Accelerate the accreditation of Conformity Assessment Bodies (CABs). (TIC Council)

Prioritise the designation of notifying authorities. (TIC Council)

The Netherlands medicatieoverdracht medicatieproces 9 projectnarrower in scope than EHDS, covering only ePrescriptions and eDispensationsremains incomplete after three years. (Epic Systems)

One pragmatic solution would be to introduce a transition period during which testing performed by laboratories accredited under ISO/IEC 17025, entitled General requirements for the competence of testing and calibration laboratories, would be accepted as sufficient. (Entrust SAS)

FERMA - Federation of European Risk Managers Associations: Calls for streamlined compliance structures and enhanced technical standards at EU level to strengthen cybersecurity governance and reduce fragmentation.

Develop a better governance through more streamlined compliance structure and en- hanced technical standards.

Epic Systems: Warns that the proposed EHDS implementation timeline is unrealistic and urges phased rollouts with testing to ensure systems and stakeholders can comply.

A two-year rollout from implementing acts to live systems is unrealistic.

TIC Council: Urges rapid accreditation of Conformity Assessment Bodies and swift designation of notifying authorities to operationalize the AI Act's conformity assessment infrastructure.

Accelerate the accreditation of Conformity Assessment Bodies (CABs).

CGI Inc.: Recommends complementing rules with practical implementation tools—guidance, templates, toolkits, trainings, and checklists—to build compliance capacity across organizations.

To make this simplification truly effective in practice, we recommend the Commission complement the regulatory framework with practical implementation tools, including detailed actionable and understandable guidance, toolkits, model templates, trainings and checklists to help organisations translate legal requirements into concrete actions.

Government Office of the Czech Republic: Supports a dedicated Data Act legal helpdesk to offer businesses hands-on implementation support and clarity on obligations.

However, CZ fully supports the establishment of a dedicated Data Act Legal Helpdesk to provide businesses with information and support regarding the implementation of the rules.

National Land Survey of Finland: Advocates EU-wide sharing of generative AI use cases and lessons learned to accelerate collective capacity building.

Use cases and lessons learned from leveraging generative AI should be shared more broadly within the EU.

Adigital (Asociación Española de la Economía Digital): Promotes RegTech and SupTech to automate compliance and calls for regulatory education to help organizations understand and adapt to requirements.

Promote systematic use of automated compliance technologies across all digital legislation.

Entrust SAS: Proposes realistic timelines, expanded accredited capacity, transitional measures for testing, and EU-wide awareness and training to avoid compliance bottlenecks and ensure uptake, especially for SMEs.

Adjusting the eIDAS implementing acts to provide realistic compliance timelines, expand accredited capacity, and deliver clear, measurable definitions.

Alcon Laboratories Inc: Requests standardized forms, procedures, and timelines across Member States and notified bodies to harmonize CE marking and reduce administrative variability.

Standardize timelines and procedures across Member States to reduce variability in CE marking

WKÖ - Austrian Federal Economic Chamber: Calls for concrete guidance—templates, best practices, and a dedicated AI support centre—to translate abstract standards into practical compliance.

Companies should receive comprehensive support, e.g. through a dedicated AI support centre within the national authorities that can be easily contacted in case of uncertainties or when advice is needed.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Highlights slow progress on standards and establishing competent authorities, urging clearer mandates and faster implementation support across the AI Act ecosystem.

In addition, we see slow progress in establishing com- petent authorities at national level, in clarifying various points in the AI Act that require interpretation (high-risk definition, AI literacy, transparency requirements, materiality threshold for changes to AI sys- tems, etc.) and in clarifying the interaction with other horizontal and sectoral legislation.

Actuarial Association of Europe: Calls for training programs and ready-to-use compliance toolkits to help practitioners operationalize new requirements efficiently.

DigitalTrade4.EU: Recommends integrating EUTIR into the EU budget and policy framework to secure sustained funding for implementation capacity and infrastructure.

Telekom Austria AG: Emphasizes supportive regulators and clear, practical guidelines to ease implementation and reduce compliance burdens.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Encourages collaboration and upskilling, including industry–academic partnerships, to build the expertise needed for robust compliance.

Healthtech Finland: Seeks pre-enforcement assistance and harmonization to help health tech firms prepare for compliance consistently across the EU.

Federation of Austrian Industries: Supports phased CRA transitions, digital support channels, and monitoring mechanisms to strengthen compliance capacity without disrupting innovation.

Ministry of Industry and Trade of the Czech Republic - this entry represents the official position of the Czech Republic for the section "Targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules: Asks for clear, consistent guidance for notified bodies to ensure reliable and harmonized conformity assessments.

Inter IKEA Group: Calls for standardized AI literacy materials to build organizational competence and consistent practices.

ITI - Information Technology Industry Council: Advocates industry-supported training for regulators to strengthen supervisory expertise and consistent enforcement.

Association of Netherlands Municipalities: Requests coherent, predictable funding for municipalities to build implementation capacity and deliver compliant digital services.

Brunel University of London: Proposes regulatory sandboxes before EU-wide rollout to de-risk implementation and refine compliance requirements.

EFCA - European Federation of Engineering Consultancy Associations: Recommends mapping workflows and obligations in multi-party consortia to clarify responsibilities and streamline compliance.

SGI Europe: Urges centrally provided tools and guidance for public authorities and support for timely AI Act implementation across services.

Orgalim - Europe's Technology Industries: Asks authorities to publish sandbox timelines to help SMEs plan resources and build compliance capacity.

Seznam.cz, a.s.: Calls for advisory support and timely guidance to help companies interpret and meet new rules.

Chair in Cyber Policy, University of Luxembourg: Argues for investing in compliance support and capacity building rather than weakening safeguards to ease implementation.

Clever Cloud: Supports coordinated sandboxes for harmonized application and helpdesks plus training to simplify compliance for developers and SMEs.

Siemens Healthineers AG: Notes that current compliance support is delayed and insufficient, calling for earlier, more substantial guidance and resources.

INVERCO: Proposes creating AI compliance training hubs to centralize expertise and accelerate organizational readiness.

Audience Measurement Coalition (AMC): Promotes independent measurement governance and common benchmarks to enable enforceable, consistent oversight.

Hugging Face: Advocates centralized, shared compliance resources to reduce duplication and lower barriers for open and small actors.

Pharma Deutschland e.V.: Requests extended transition periods and simplified processes to alleviate pressure on notified bodies and ensure continuity.

SAP SE: Calls to strengthen regulators' technical expertise to enable proportionate, consistent supervision and guidance.

Free ICT Europe Foundation: Proposes an EU digital business support desk to provide practical, accessible implementation assistance to SMEs.

AMETIC: Encourages public–private collaboration to co-develop standards and guidance that are implementable and interoperable.

Capgemini Deutschland GmbH: Urges leveraging existing monitoring and reporting mechanisms to reduce duplication and support efficient compliance.

1.2.7 Stakeholder Consultation, Transparency & Co-Regulation

Stakeholder Consultation, Transparency & Co-Regulation under Coordinated Governance, Guidance & Phased Timelines emphasizes early, inclusive, and iterative engagement across the digital ecosystem. Stakeholders should be consulted at formative stages and throughout implementation, with guidance published well in advance (e.g., 18–24 months) and developed through meaningful dialogue with affected professionals (clinicians, SMEs, manufacturers, notified bodies, disability organizations). Clear communication strategies and ongoing feedback mechanisms (surveys, review panels, public reporting) help make rules understandable and workable while enabling phased compliance. Transparency and collaborative oversight are central enablers: publishing elements of risk assessments (DPIAs/FRIAs) to reduce duplication along value chains; modernizing supervisory mandates and explicitly recognizing DPAs' dual role of rights protection and innovation; and using co-regulatory instruments—codes of conduct, standards, and well-measured regulatory sandboxes with public overviews—to coordinate cross-border adoption. Bridging public and private sectors, fostering trust, and opening dialogue before opinions (e.g., EDPB) strengthen coherence, legal certainty, and the free flow of data with appropriate safeguards.

> *Publish guidances early, but at least 18-24 months before they come into effect and ensure meaningful consultation with stakeholders, such as manufacturers, notified bodies, and healthcare professionals during the drafting process.* (Zimmer Biomet)

> *When guidance on EU legislation is being drafted, the process must allow for meaningful stakeholder consultation to ensure the result is actionable and workable.* (Ibec)

> *For instance, a proposed multi-factor authentication design would have required clinicians to remove medical gloves up to 14 times more per day, harming both efficiency and sustainability.* (Epic Systems)

> *An alternative way to ease any confusion as to what elements may have been covered by which risk assessment would be to make elements of both DPIAs and FRIAs publicly available, so that providers and deployers along the value chain may benefit from work that has already been done.* (Centre for Democracy and Technology Europe)

Epic Systems: Calls for including clinicians and technical experts in EHDS consultations to avoid impractical designs and ensure user-centered, sustainable implementation.

> *For instance, a proposed multi-factor authentication design would have required clinicians to remove medical gloves up to 14 times more per day, harming both efficiency and sustainability.*

Zimmer Biomet: Advocates publishing guidance 18-24 months in advance with meaningful consultation of manufacturers, notified bodies, and healthcare professionals to ensure workable implementation.

> *Publish guidances early, but at least 18-24 months before they come into effect and ensure meaningful consultation with stakeholders, such as manufacturers, notified bodies, and healthcare professionals during the drafting process.*

Encode Europe: Notes entrepreneurs struggle with rule complexity and urges a coordinated communication strategy with national authorities to simplify compliance.

> *Therefore, we believe a solid communication strategy (possibly in collaboration with national compliance authorities) is a vital part of simplification.*

Volkswagen Group: Proposes modernising supervisory authorities to support data flows and innovation alongside privacy, aligning enforcement with coordinated, pro-innovation governance.

> *In addition to safeguarding personal data, their responsibilities should also include sup- porting the free flow of data-both within the EU and, with appropriate safeguards, beyond-as well as promoting innovation and the competitiveness of data-driven businesses.*

Centre for Democracy and Technology Europe: Recommends publishing parts of DPIAs and FRIAs to increase transparency and enable coordination across providers and deployers.

An alternative way to ease any confusion as to what elements may have been covered by which risk assessment would be to make elements of both DPIAs and FRIAs publicly available, so that providers and deployers along the value chain may benefit from work that has already been done.

Mastercard Europe SA: Stresses that effective public–private cooperation is critical to interoperability, data portability, and trusted EU market access.

Effective cooperation between European authorities and the private sector is critical.

Centre for Information Policy Leadership (CIPL): Calls for agile, collaborative oversight that provides legal certainty, recognizing the dual role of DPAs in protecting rights and enabling innovation.

CIPL's work on smart regulation and innovation further highlights the importance of a more agile and collaborative regulatory culture across the EU's digital ecosystem, to ensure the coherent oversight and legal certainty organisations need.

Ibec: Insists guidance drafting must feature meaningful stakeholder consultation to produce actionable, workable outcomes.

When guidance on EU legislation is being drafted, the process must allow for meaningful stakeholder consultation to ensure the result is actionable and workable.

AIM - European Brands Association: Urges robust ongoing stakeholder engagement and transparent, continuous assessment of digital rules to keep simplification effective.

Continuous assessment of the coherence and cumulative impact of digital rules-together with regular monitoring and transparent reporting-will be essential to guarantee that simplification measures remain effective over time.

CERMI: Proposes a systematic disability inclusion test of the digital regulatory framework, led by representative organisations of persons with disabilities.

This assessment must be carried out with the direct participation and leadership of representative organisations of pWd

Meta Platforms Ireland Limited: Advocates open, timely consultations at the formative stage with sufficient information for meaningful public input.

Consultations must occur while proposals are still at a formative stage.

Adigital (Asociación Española de la Economía Digital): Acts as a bridge for public–private dialogue and calls for transparent engagement with affected companies prior to EDPB opinions.

First, it is suggested that before any opinion from the EDPB, a transparent and dialogical engagement with the affected company take place, rather than the company merely receiving a closed opinion used to support any subsequent judicial decision.

Vodafone Group: Recommends mechanisms like annual surveys, review panels, and transparent reporting to maintain responsive regulatory simplification.

This could include annual stakeholder surveys, regular review panels with industry and SME representatives, and transparent public reporting on the effectiveness of simplification measures.

Entrust SAS: Expresses readiness to collaborate with the Commission to translate governance objectives into practical, trust-building outcomes.

We stand ready to support the Commission in translating these objectives into practical outcomes that strengthen Europes competitiveness and trust in its digital economy.

: Emphasizes making public funding structures visible to ensure transparency before deploying digital control tools.

It creates transparency by first making the public funding structure itself visible before the introduction of digital control tools.

WKÖ - Austrian Federal Economic Chamber: Calls for clear sandbox success metrics and publication of a comprehensive overview of national sandboxes to foster cross-border cooperation.

o further promote cross-border cooperation, we call for the publication of a comprehensive overview of all national sandboxes, including their specific focus areas.

European Cyber Security Organisation: Signals ECSO's readiness to engage institutions and actively contribute to advancing coordinated, transparent processes.

ECSO is ready to engage relevant institutions and actively contribute to advancing this process.

American Chamber of Commerce to the EU: Urges openness and stakeholder consultations that include transatlantic business perspectives.

Danish Standards - National Standardisation Organisation of Denmark: Highlights the value of broad stakeholder consensus through standards to support coordinated governance.

German Property Federation: Promotes constructive collaboration between regulators and industry to achieve balanced, transparent governance.

DigitalTrade4.EU: Supports industry-led collaborative policy development and co-regulatory approaches for practical, transparent implementation.

European Signature Dialog: Advocates coordinated stakeholder engagement to align regulation and oversight in electronic signatures.

Cisco: Encourages early consultations and guidance to ease compliance and reduce regulatory friction.

IBM: Calls for improved stakeholder consultation and transparent processes throughout the regulatory lifecycle.

Outpacr / VAICE: Proposes public self-assessment mechanisms to enhance transparency and accountability in governance.

ITI - Information Technology Industry Council: Urges formal consultation duties with industry and inclusive safeguards in coordination structures to avoid overreach.

ENCIRCLE Research Consortium: Supports structured consultations to clarify AI Act application and ensure coherent cross-sector implementation.

DOT Europe: Calls for harmonised, consultative pre-enforcement guidance to enable consistent compliance across the EU.

Verband der Automobilindustrie e.V.: Advocates a pro-innovation stance by the EDPB and strong stakeholder input to balance data protection and competitiveness.

kaiko.ai: Suggests collaborative public–private platforms for regulatory dialogue to streamline guidance and co-regulation.

Comitato Elettrotecnico Italiano - CEI: Endorses ESO roles and multi-stakeholder consultations to guide AI governance and standards.

Google: Recommends publishing a public list of empowered authorities to increase transparency and accountability.

Fastweb S.p.A.: Supports adjusting annual regulatory plans based on stakeholder feedback and evolving operational needs.

secunet Security Networks AG: Emphasizes ongoing collaboration between regulators and industry as essential for effective, secure digital governance.

Business Software Alliance: Promotes regulator–stakeholder consultation and recognition of co-regulatory codes and standards for workable outcomes.

SGI Europe: Calls for transparent, coordinated processes in drafting delegated acts to avoid fragmentation.

European Fund and Asset Management Association (EFAMA): Urges early industry involvement in policy and technical design to ensure practicable, phased implementation.

Bocconi University: Argues for procedural transparency and independent monitoring to uphold accountability in digital governance.

Charter of Trust: Encourages strong industry involvement in standards development as a co-regulatory tool.

European Federation for Market Research Organisation (EFAMRO): Supports international self-regulatory codes and co-regulation to ensure ethical, consistent practices.

Global Data Alliance: Recommends voluntary co-regulatory mechanisms and inclusive guideline consultations, especially for SMEs.

Computer & Communications Industry Association (CCIA Europe): Calls for evidence-based regulation with impact assessments and greater transparency in trilogues and legislative processes.

CEN and CENELEC: Highlights open consultation channels and multi-stakeholder standards development as key tools for coordinated governance.

European Savings and Retail Banking Group: Advocates market-driven, phased rollout and transparent reporting on eID Large-Scale Pilot deliverables.

Danish Industry: Urges user-oriented joint guidance, early industry involvement, and facilitation of codes of conduct to support coordinated compliance.

Eurosmart: Proposes mandated consultations to secure consistent, harmonised implementation across Member States.

Alliance Digitale: Calls for mandatory public consultations to develop joint guidance and avoid divergent enforcement.

Middle Tech Europe: Recommends open stakeholder dialogue, robust impact assessments, and an annual transparency strategy to strengthen trust.

BioMed Alliance: Advocates involving professionals in the digital transition to ensure safe, workable governance.

Zentralverband der deutschen Werbewirtschaft (ZAW): Promotes industry collaboration with regulators to achieve balanced governance that supports innovation and consumer protection.

OpenMined: Highlights benefits of cross-sector collaboration and recommends a dedicated expert working group to coordinate governance.

DIGITALEUROPE: Urges recognition of voluntary industry codes and warns against implementing acts that restrict stakeholder input.

OpenAI: Proposes a democratic AI governance forum to institutionalise inclusive, transparent stakeholder dialogue.

Enedis: Requests company feedback be included in regulatory revaluations to ensure practical, transparent outcomes.

Dutch Startup Association: Calls to institutionalise startup representation in policy processes to improve transparency and proportionality.

Deutscher Bauernverband e.V.: Emphasizes trust-based governance and collaboration to ensure workable digital regulation in agriculture.

Esomar: Supports formal recognition of self-regulatory frameworks as part of co-regulation in data and research.

Adyen: Advocates close collaboration between regulators and the payments industry for clear, consistent guidance and compliance.

1.2.8 Miscellaneous

This category gathers calls to move from reactive, piecemeal rulemaking toward a coherent, principle-based EU digital governance model with clear roles, accountability, and phased implementation. Proposals emphasize strengthening the European Parliament's role in comitology to combine transparency with agility, shifting routine enforcement to Member States or independent agencies while the Commission focuses on implementation, and treating the Digital Omnibus as a lever for strategic governance rather than a narrow technical fix. Stakeholders also urge beginning framework development now, even if lengthy, to align priorities and provide guidance over time. Operational realism features prominently: industry experience points to cross-border implementation frictions, even where policies are sound on paper. Several contributions argue that existing dispute-resolution channels should suffice, that enforcement alone will not achieve reform without better coordination and guidance, and that in some areas it may be prudent to pause new rulemaking, rely on monitoring, and reassess based on actual disputes. Additional themes include reinforcing legal accountability and auditability, limiting the Commission's direct role in technical standards/specifications, and fostering structured collaboration with the Commission and DG CONNECT. Spectrum policy is a concrete testbed for coordinated governance with phased timelines: advocates call for much longer license durations with default prolongations, pro-investment auction designs, and fair "use it or lose it" rules that also safeguard device usability and network resilience. The consensus is to keep spectrum management and authorization—along with concrete timelines—at Member State level, while strengthening EU-level coordination on factors like sufficient license duration, early and harmonized spectrum availability, and investment-oriented design to achieve scale and predictability.

It argues that the EU must move beyond reactive regulation and piecemeal initiatives, instead embracing a unified, principle-based approach that leverages its collective strengths. ()

The European Parliament's role in shaping secondary legislation ought to be streng- thened (i.e. including MEPs in comitology committees), bringing greater accountability and transparency to this part of the EU policy cycle, while keeping the agility of those processes. ()

The Commission must cede its politicised role as enforcer, and focus again solely on the implementation of law ()

German Industries supports indefinite spectrum licenses or at least a longer duration of frequency usage rights of with a minimum of 40 years. (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)

: Advocates a unified, principle-based EU digital governance approach with better alignment across initiatives and strengthened comitology accountability, while shifting enforcement to Member States or independent agencies to depoliticize implementation.

It argues that the EU must move beyond reactive regulation and piecemeal initiatives, instead embracing a unified, principle-based approach that leverages its collective strengths.

Technology Industries of Finland: Urges beginning the development of a coordinated framework immediately to enable a realistic, phased timeline for adoption.

It is important to start developing such a framework now, even if the preparation takes a longer time.

Association française de normalisation (AFNOR): Positions the Digital Omnibus as a lever for strategic, coordinated European digital governance rather than a mere technical simplification exercise.

The Digital Omnibus should not be seen as a purely technical adjustment (« simplify, just to simplify >>), but as a step towards a strategic European digital governance model.

Adigital (Asociación Española de la Economía Digital): Highlights that coordinated measures can speed implementation of digital-transition policies and align corporate governance with EU economic security principles.

Moreover, there are highly relevant indirect effects, such as greater agility in implementing public policies linked to the digital transition, including circular economy initiatives and the adoption of corporate governance frameworks aligned with the EU's principles of economic security.

Vodafone Group: Reports cross-border implementation challenges that underscore the need for more coordinated governance, clearer guidance, and predictable timelines across Member States.

The examples provided reflect real-world challenges faced by cross- border service providers.

ACEA (European Automobile Manufacturers' Association): Maintains that existing Data Act redress and oversight mechanisms already provide adequate governance for disputes, reducing the need for additional structures.

Should any decision of a data holder give rise to a dispute, the data recipient can apply for redress before the dispute settlement body (Art. 10(1)) or lodge a complaint with the competent authority (Art. 38(1)), which is empowered to request all necessary information from the data holder to assess whether its decision complies with the Data Act (Art. 37(14)).

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Calls for EU-level coordination on spectrum policy to ensure long-duration, investment-friendly licenses and harmonized availability while keeping authorization procedures and concrete timelines with Member States.

German industry believes that spectrum management and authori- zation procedures, including concrete timelines, have to remain the responsibility of Member States, while a certain level of coordination at EU level - e. g. on license duration being long enough, pro- investment auction design, early and coordinated availability of spectrum resources to create scale - must be ensured and further strengthened.

European Signature Dialog: Stresses the importance of clear legal accountability and auditability within coordinated governance frameworks to ensure trustworthy implementation.

Outpacr / VAICE: Seeks formal recognition by DG CONNECT to anchor roles and guidance within a coordinated governance setup.

ENTSO-E: Commits to supporting Commission-led coordination to deliver coherent implementation and phased rollouts across the sector.

Association des Constructeurs Européens de Motocycles: Recommends pausing new rulemaking and reassessing after observing real-world disputes, favoring a phased and measured governance approach.

Google: Prefers maintaining coordinated oversight via BEREC monitoring instead of new regulation, emphasizing proportionate governance and gradual adjustments.

Euroconsumers: Argues that enforcement alone will not drive necessary reforms, calling for coordinated policy guidance and structural changes to achieve outcomes.

DIGITALEUROPE: Advocates curbing the Commission's powers over standards and specifications to rebalance and coordinate governance through broader stakeholder-led standardization.

1.3 Risk-Based, SME-Friendly Proportionality

The unifying insight is to "scale obligations with risk, not size," pairing outcomes-based flexibility with concrete simplification so SMEs can comply without cliff-edges. Risk tiering uses objective triggers, exempts

benign or low-criticality uses, tailors by context (e.g., B2B/B2C), and confines supply-chain duties to direct suppliers. Outcomes-based, technology-neutral rules recognize compensating controls and lifecycle realities (including a product's digital lifetime), focusing on material impacts over process formalism. Practical supports—codes of conduct, helpdesks, templates, sandbox access, and streamlined onboarding—bridge capability gaps; technical-feasibility clauses and best-effort compliance apply until interoperable standards arrive, with verifiable SME status to ensure trust. Reporting and transparency scale to risk, reduce duplication (e.g., AI Act quality management, DORA registers), omit low-value entries, limit prescriptive translations, and leverage automation/RegTech. Harmonized, cross-regime guidance and consistent Member State application cut conflicts and duplicative filings, with standards used judiciously to maintain interoperability. Phased, predictable timelines, longer adaptation, time-boxed enforcement and first-time correction, vouchers and open tools, reduced audit fees, and targeted exemptions prevent cascading burdens. Oversight is targeted and proportionate: alternative assurance, regulatory equivalence, self-certification for low risk, conditional/lifetime certification, risk-based testing, and urgent tell-and-do changes. Fair cost sharing uses tiered/capped fees, upstream duties, SME data-access preferences, and calibrated sanctions. Across categories, clarity, coherence, and proportionality anchored in risk—plus practical support and sequencing—create a predictable, efficient path that preserves high protections while enabling SMEs to innovate and compete.

1.3.1 Outcomes-Based, Technology-Neutral Rules

Outcomes-based, technology-neutral rules set clear objectives and measure effectiveness against real-world risks and harms, rather than prescribing specific processes or technical designs. Obligations scale with risk profiles and allow flexible, alternative means of compliance, enabling organizations—including SMEs—to choose proportionate controls that achieve the same protective outcomes. This approach avoids one-size-fits-all requirements, remains future-proof across evolving technologies, and focuses enforcement on material impacts rather than minor procedural deviations. In practice, regulators define what must be achieved (e.g., effective detection, reporting, mitigation; transparency and accountability; contestability) while remaining neutral about how it is delivered. They encourage functionally targeted remedies and recognize compensating controls, provide transition periods and guidance, and replace rigid structural mandates with operational safeguards and transparency. Sectoral tailoring and concepts like distinguishing a product's digital lifetime from its physical lifetime align obligations with actual risk and lifecycle realities, maintaining innovation, interoperability, and legal certainty without diluting core protections.

> *Streamlined obligations should focus on outcomes, effective detection, reporting, and mitigation, rather than rigid procedural requirements.* (European Energy Information Sharing and Analysis Centre)
>
> *To ensure regulation remains relevant, adaptable, and supportive of innovation, it is essential to adopt a technology-neutral approach that focuses on the responsible use and real-world impacts of AI systems.* (Meta Platforms Ireland Limited)
>
> *Regulating the underlying technology, rather than its use or outcomes, is not only ineffective but ultimately counterproductive.* (Meta Platforms Ireland Limited)
>
> *Shift to outcomes-based international data flow assessments instead of strict equivalence requirements.* (Centre for Information Policy Leadership (CIPL))
>
> **ZVEI e.V.:** Advocates a risk-based, outcomes-focused CRA by distinguishing physical and digital lifetimes and allowing manufacturer-defined digital support periods, particularly in B2B markets. This aims to avoid disproportionate burdens while maintaining cybersecurity objectives.
>
> *We recommend introducing a "digital lifetime" concept, defined and transparently declared by the manufacturer, to allow for risk-based and economically viable support obligations.*
>
> **European Energy Information Sharing and Analysis Centre:** Calls for proportional, risk-based obligations that center on outcomes like detection and mitigation rather than rigid procedures. Simplification should reflect operator risk profiles to reduce unnecessary burdens.
>
> *Streamlined obligations should focus on outcomes, effective detection, reporting, and mitigation, rather than rigid procedural requirements.*
>
> **Dun & Bradstreet:** Urges regulators to align requirements with effectiveness and desired outcomes instead of prescriptive processes. This approach supports technology-neutral compliance and proportionality.

Focusing on effectiveness: Align regulatory obligations with desired outcomes rather than prescriptive processes.

Snap Inc.: Supports defining clear regulatory objectives while granting flexibility in how firms meet them. This outcomes-based, tech-neutral approach enables innovation and proportionate compliance.

Define clear regulatory objectives while allowing flexibility in how companies meet them.

Siinda: Promotes risk-based, technology-neutral rules with tailored, contestability-preserving remedies and SME-friendly scaling of obligations. Emphasizes transparency, interoperability, and avoiding one-size-fits-all mandates.

EU Al strategy must be risk-based, technology-neutral, and interoperable with DMA and GDPR.

Centre for Information Policy Leadership (CIPL): Recommends codifying risk-based, outcomes-focused regulatory behavior and shifting assessments from formal equivalence to results. Focus enforcement on real harms and embed innovation-enabling tools without major overhauls.

Codifying expectations for risk- based, outcomes-focused regulatory behaviour can deliver significant impact without major legal overhauls.

Meta Platforms Ireland Limited: Advocates technology-neutral, impact-focused regulation that tailors obligations to actual risks and avoids regulating underlying tech. This future-proof approach supports innovation and proportional compliance.

To ensure regulation remains relevant, adaptable, and supportive of innovation, it is essential to adopt a technology-neutral approach that focuses on the responsible use and real-world impacts of AI systems.

Vodafone Group: Seeks proportionate, future-proof rules with flexibility to deem requirements irrelevant when risk assessments justify it. Penalties should incentivize proactive security rather than box-ticking.

Allow flexibility for companies to demonstrate when specific requirements are not relevant based on risk assessment.

Anitec-Assinform: Urges replacing rigid structural separation with operational controls, transparency, and safeguards to achieve neutrality. This outcomes-based shift reduces burdens while maintaining trust.

We propose replacing the structural separation requirement with clear operational controls and transparency mechanisms: organizational measures and internal controls to ensure service neutrality, transparent pricing mechanisms demonstrating independence, and technical/operational safeguards to prevent conflicts of interest.

ALSTOM: Endorses targeted, risk-based CRA adjustments aligned with operational and safety constraints to cut administrative costs. The goal is to preserve interoperability and investments while meeting objectives.

A risk-based compliance strategy, aligned with operational and safety constraints, is essential to maintain interoperability, availability, cost-efficiency, and preserve ongoing investments.

European Associations of Co-operative Banks (EACB): Calls for proportionate, harmonised, innovation-friendly regulation that respects market-driven schemes. Avoid imposing prescriptive data-sharing mandates when industry solutions can deliver outcomes.

The EACB urges the Commission to ensure a proportionate, harmonised, and innovation-friendly approach that supports Europe's financial and data ecosystems.

European Travel Retail Confederation (ETRC): Encourages adapting and tailoring DFTR rules with flexible, proportionate measures rather than blanket exemptions. Emphasis is on outcomes and risk-based adjustments to fit sector realities.

Business & Science Poland: Proposes replacing sweeping gatekeeper bans with targeted anti-solicitation rules that address the problem functionally. This focuses on outcomes and proportionality rather than technology-specific constraints.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Prefers internal governance mechanisms over broad restrictions to achieve responsible AI outcomes. This supports technology-neutral rules emphasizing risk management and accountability.

Polish Confederation Lewiatan: Advocates outcome-based, risk-proportionate regulation to avoid excessive burdens. Rules should scale with impact and remain technology-neutral to foster innovation.

ITI - Information Technology Industry Council: Supports Better Regulation practices with risk-based design and robust consultations to ensure proportionate, outcome-focused rules. This helps avoid unnecessary burdens, especially for SMEs.

ING: Calls for pragmatic, risk-based requirements tailored to use cases rather than prescriptive tech mandates. A proportionate approach improves effectiveness and reduces compliance drag.

Salesforce, Inc.: Urges allowing alternative, equivalent compliance measures to meet clear objectives. This outcome-focused flexibility keeps rules technology-neutral and proportionate.

Federation of European Securities Exchanges: Seeks removal of prescriptive third-party training mandates in favor of outcome-based safeguards. Rules should be technology-neutral and proportionate to actual risks.

Advertising Information Group: Warns against compliance burdens that lack consumer benefit and backs outcomes-focused, risk-based regulation. Enforcement should prioritize material consumer harm over minor procedural issues.

CECIMO - European Association of Manufacturing Technologies: Argues that proportional, outcome-based rules enable innovation in manufacturing technologies. Avoid prescriptive designs that constrain SME competitiveness.

Independent Retail Europe: Calls for proportionate, clear laws that provide legal certainty while focusing on outcomes. Technology-neutral, risk-based obligations help smaller retailers comply effectively.

Fastweb S.p.A.: Advocates proportionate, technology-neutral regulation aligned with objective-based compliance. This ensures flexibility and effectiveness across diverse network and service contexts.

European Entrepreneurs CEA-PME: Supports a shift from risk avoidance to risk management with proportionate, outcome-oriented rules. This SME-friendly approach reduces overregulation while maintaining safeguards.

PensionsEurope: Promotes principle-based proportionality for IORPs, focusing on outcomes rather than prescriptive processes. Tailored, risk-based obligations fit sector specifics and ensure efficiency.

European Publishers Council: Endorses a risk-based approach that reduces consent fatigue, builds trust, and preserves rights while enabling flexibility. Functionally targeted, outcome-focused rules support editorial media.

Data & Technology for Compliance Alliance: Supports outcome-based, proportionate regulation that recognizes practical compliance pathways. Emphasizes clear objectives with flexible, risk-based implementation.

DIGITALEUROPE: Proposes deregulatory changes that retain core protections and recognize compensating security measures as equivalent. This outcome-focused, tech-neutral approach avoids one-size-fits-all compliance.

Too Good To Go: Calls for shifting compliance toward outcome-based objectives with proportionate obligations. Flexibility helps innovate while meeting risk-based safeguards.

Confederation of Swedish Enterprise: Critiques expanding, absolutist requirements and urges proportionate, outcome-focused, technology-neutral rules. Emphasis on practicality and avoiding burdens that outpace benefits.

1.3.2 Harmonised Frameworks & Cross-Regime Alignment

This category emphasises risk-based proportionality as the backbone of harmonised, cross-regime regulation. Stakeholders call for a streamlined, coherent interplay between overlapping EU digital, data, and security laws, coupled with consistent application across Member States and clear, common technical guidance. They favour leveraging horizontal frameworks and recognised standards to minimise fragmentation, using binding Common Specifications only in exceptional cases with transparent governance. The objective is to simplify without diluting safeguards—supporting safe innovation and competitiveness while maintaining high levels of privacy, security, and trust. A strong SME and startup lens runs throughout: align and rationalise requirements to cut duplicative filings, documentation, and conflicting obligations; enforce proportionately and based on risk; and ensure new measures are evidence-based and targeted. This reduces disproportionate burdens, addresses the "cliff edge" faced by smaller firms, and converts today's patchwork into a predictable, interoperable compliance environment that lowers costs and barriers to market entry.

Ensure risk-based proportionality and harmonization across Member States (Enel SpA)

It is important to ensure a proportionate, balanced and streamlined approach, with a logical and easily compatible interplay of the requirements of these separate legislations. (DigiFinland)

Remove Article 29 (1) sentence 4 of FSR which states that "In a multi-stage procedure, the notification or declaration shall be submitted twice, first with the request to participate and then as an updated notification or updated declaration with the submitted tender or final tender." (Ibec)

Common Specifications should be limited to exceptional cases, specifically when European Standard Organisations decline EC standardisation requests. (Amazon)

DigiFinland: Advocates a proportionate, balanced, and streamlined, risk-based interplay across separate EU laws to ease adoption while safeguarding safety and data protection. Calls for simplification that accelerates commercialization and competitiveness without lowering protections.

It is important to ensure a proportionate, balanced and streamlined approach, with a logical and easily compatible interplay of the requirements of these separate legislations.

Enel SpA: Urges harmonized, risk-based proportionality across Member States so obligations avoid unnecessary complexity and resource burdens. Emphasizes consistent, proportionate rules over prescriptive approaches.

Ensure risk-based proportionality and harmonization across Member States

France Digitale: Calls for a systemic, cross-regime evaluation of digital rules to ensure alignment that supports startups and scaleups. Seeks coherence that limits cumulative burdens across frameworks.

We encourage the Commission to conduct a systemic evaluation of how existing and upcoming EU digital rules affect startups and scaleups.

Amazon: Recommends limiting mandated Common Specifications and relying on harmonised guidance and voluntary standards to avoid overregulation. Seeks clear, consistent implementation rules, especially for cybersecurity.

Common Specifications should be limited to exceptional cases, specifically when European Standard Organisations decline EC standardisation requests.

Ibec: Advocates risk-based, evidence-driven alignment across regimes like FSR and FDI, removing duplicative procedures and ensuring coherent Member State enforcement. Prioritizes consistency, certainty, and proportionality to reduce burdens.

Coherent application of all digital regulation at Member State level should also be prioritised (see principles in Section 3b) with enforcement risk based.

Adigital (Asociación Española de la Economía Digital): Proposes replacing fragmented regimes with a single horizontal framework and applying proportional obligations with common technical guidelines. Aims to harmonise rules to support innovation and SMEs while maintaining protection.

Replace the ePrivacy Directive with a single horizontal framework.

Entrust SAS: Calls to harmonise overlapping frameworks to reduce disproportionate compliance burdens, particularly for SMEs and small mid-caps. Highlights fragmentation and inconsistencies as core drivers of unnecessary costs.

We appreciate the opportunity to contribute to this consultation, recognising its potential to harmonise overlapping frameworks and reduce disproportionate compliance burdensparticularly for SMEswhile maintaining high standards of security and trust.

European AI Forum: Highlights that fragmentation and lack of clarity create compliance risks and disproportionate costs for startups and SMEs. Urges clearer, harmonised alignment across regimes to lower barriers to innovation.

For startups with limited resources, this fragmentation turns compliance into a major operational challenge and translates into disproportionate costs.

iProov Ltd: Warns that rigid, mandated approaches risk excluding innovators and advocates inclusive, harmonised standards. Seeks cross-regime alignment that remains proportionate and implementation-agnostic.

ITI - Information Technology Industry Council: Supports alignment around risk-based, internationally harmonised standards to minimise fragmentation. Encourages interoperable, global approaches that reduce duplicative compliance.

DOT Europe: Recommends streamlining and aligning risk assessment and documentation duties across laws to reduce duplication. Promotes harmonised obligations that scale with risk.

Federation of European Securities Exchanges: Advocates EU-level coordination for TLPT frameworks with proportional requirements to ensure consistency. Aims to avoid duplicative national processes and align supervisory expectations.

Confederation of European Security Services (CoESS): Urges reaffirming GDPR's risk-based approach across related frameworks to ensure proportionate, consistent obligations. Promotes harmonised enforcement to avoid fragmentation.

Association des Constructeurs Européens de Motocycles: Calls for a coherent, proportionate regulatory framework aligning cross-regime requirements to prevent unnecessary burdens. Emphasizes predictability and consistency for industry.

Independent Retail Europe: Requests SME-friendly GDPR standards and simplified, harmonised guidance across Member States. Seeks reduced administrative burdens through consistent application.

ACT | The App Association: Notes that overlapping and inconsistent rules hinder SMEs and advocates harmonised, risk-based alignment to streamline compliance. Encourages simplification to foster innovation.

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: Stresses that regulatory fragmentation and complexity impose costly burdens on SMEs. Supports greater harmonisation and simplification for cross-regime consistency.

Meetic Group, a Match Group Company: Supports proportionate implementation and open, interoperable standards to align rules across regimes. Aims to ensure consistency and avoid overbearing obligations.

DER MITTELSTANDSVERBUND - ZGV e.V.: Urges eliminating overlapping and redundant requirements across regimes to ease SME compliance. Promotes harmonisation and proportionality to reduce unnecessary burdens.

1.3.3 Risk-Tiered Scope, Thresholds & Exemptions

This category advances a risk-tiered approach: regulatory scope and obligations should scale with the level of risk, the size and complexity of the provider, and the specific activity. Stakeholders propose objective triggers (e.g., size thresholds and gateway behaviors) for heightened duties, alongside exemptions or reduced requirements for low-risk or well-established technologies and products (e.g., simple medical calculators). Sector examples include simplified ICT risk management for small and non-complex insurers and lighter regimes for non-systemic investment firms. Contributors warn against overly broad definitions that capture services of limited criticality, and they call for tailoring by context (e.g., B2B vs B2C) and by risk vector (e.g., limiting supply-chain security duties to direct suppliers). They also note that owner-based SME exemptions can have drawbacks, arguing that proportionality should hinge on risk, scale, and activity to avoid disproportionate costs, reduce formalistic enforcement, and preserve innovation by microbusinesses, startups, and nascent technologies.

To avoid overwhelming businesses and SMEs, it is important that any measure is proportionate to their scale and level of risk posed. (EMMA-ENPA)

Regulatory obligations should be proportionate to risks and scale of operations, carefully calibrated to minimize unintended burdens on microbusinesses, fintech innovators, or nascent technologies. (Mastercard Europe SA)

Limit supply chain security obligations to direct suppliers. (Vodafone Group)

Ensure that the Data Act and the AI Act clearly distinguish between B2B and B2C because the level of required protection, the need for details and standards and the coverage of already existing legal framework is different. (UNIFE)

ZVEI e.V.: Proposes a tiered approach that designates certain low-risk items as benign and subjects them to lighter or no obligations.

Introduce the concept of benign products for low-risk items.

DigiFinland: Urges revisiting how software calculators are classified, excluding simple calculators from medical device rules to reflect low risk.

Review the qualification and/or classification of software calculators ('medical calculators'): simple calculators should not be classified as medical devices or IVDs (as in the U

EMMA-ENPA: Calls for obligations scaled to company size and the actual level of risk, to avoid overwhelming SMEs.

To avoid overwhelming businesses and SMEs, it is important that any measure is proportionate to their scale and level of risk posed.

ALFI - Association of the Luxembourg Fund Industry: Requests specific exemptions for non-systemic Class 2 investment firms and management companies, reflecting their lower risk profile.

Specific consideration and exemptions should be foreseen, for Class 2 investment firms and management companies for these entities are neither systemically relevant, nor part of the banking sector.

German Insurance Association: Advocates extending the simplified ICT risk management framework to small and non-complex undertakings already under proportional regimes.

The simplified ICT risk management framework should be made avail- able to a broader group of entities, such as small and non-complex un- dertakings (SNCUs) already defined under Solvency II, who are already subject to proportional requirements.

Siinda: Recommends scoping covered services using objective size thresholds and defined gateway behaviors mapped to specific activities.

Define covered services by objective criteria (size thresholds + gateway behaviours: bundling, self-preferencing, tying of services, refusal to interoperate) and map these criteria to SIP activities (search index, discovery, app stores, ad intermediation).

Vorwerk SE & Co. KG: Urges differentiation between small service businesses and large platforms so smaller players are not subjected to one-size-fits-all rules.

Such businesses share very little in common with large gig economy platforms, yet without intervention, they will be subject to the same heavy-handed regulations.

Seznam.cz, a.s.: Notes drawbacks of provider-size or ownership-based exemptions and advocates more effective criteria for proportional treatment.

While the DSA already provides exemptions for small and micro providers in certain areas of regulation, this owner-based approach has several drawbacks.

Mastercard Europe SA: Supports calibrating regulatory duties to risk and operational scale to minimize unintended burdens on microbusinesses and innovators.

Regulatory obligations should be proportionate to risks and scale of operations, carefully calibrated to minimize unintended burdens on microbusinesses, fintech innovators, or nascent technologies.

Leading Baltic tech and other businesses and professional associations listed in the submission: Warns that current approaches impose disproportionate compliance costs and shift enforcement toward formalities rather than real risks.

This leads to disproportionate compliance costs and enforcement actions focused on formalities rather than real threats to data protection.

ISP Alliance a.s.: Asks that any AI-related obligations for communications providers reflect operator scale and risk profile to avoid overburdening small players.

Accordingly, we have no specific proposals for improvement in the AI domain, beyond observing that any obligations imposed on providers of electronic communications that might involve AI should take account of the scale of operations and the risk profile, to avoid overburdening small operators.

Adigital (Asociación Española de la Economía Digital): Supports liability frameworks that are balanced and aligned with the operator's scale.

Apply balanced liability frameworks consistent with the operator's scale.

Vodafone Group: Supports limiting supply-chain security duties to direct suppliers to keep obligations proportionate and enforceable.

Limit supply chain security obligations to direct suppliers.

Almega: Highlights that AI Act obligations fall disproportionately on SMEs and startups and urges more proportionate implementation.

Obligations under the AI Act disproportionately impact small and medium- sized enterprises (SME's) and startups, potentially stifling European Al innovation.

Alcon Laboratories Inc: Proposes reduced requirements for well-established technologies and low-risk devices within a risk-based framework.

Apply reduced requirements for well-established technologies and low-risk devices.

ACEA (European Automobile Manufacturers' Association): Argues that overly broad scoping captures services of limited criticality and calls for narrowing coverage to what is truly critical.

Finally, Implementing Regulation (EU) 2024/2690-intended to harmonise reporting rules for digital service providers under NIS 2-creates an additional challenge, as its definitions of the services it is intended to cover are overly broad, capturing services of limited criticality.

UNIFE: Urges differentiating between B2B and B2C contexts because protection needs and applicable standards differ.

Ensure that the Data Act and the AI Act clearly distinguish between B2B and B2C because the level of required protection, the need for details and standards and the coverage of already existing legal framework is different.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Advocates targeting protections where needed while avoiding unnecessary burdens on intra-group activities.

This approach would ensure that the DSA's protections are applied where they are most needed, without imposing unnecessary burdens on intra-group activities.

1.3.4 Predictable, Phased Timelines & Fair Transitions

This category emphasizes predictable, phased timelines and fair transitions grounded in risk-based, SME-friendly proportionality. Stakeholders call for realistic implementation schedules tied to the availability of harmonised standards, stable requirements over time, and clear transitional periods to avoid cliff-edge effects. They argue that obligations and documentation should scale with risk rather than company size, with regulators considering firm size and innovation potential when supervising or sanctioning. Coherence across the digital acquis is urged to reduce uncertainty and administrative load, including time-boxed enforcement delays and opportunities to correct first-time, non-harmful mistakes. Key implementation levers include phasing obligations to let SMEs and mid-caps adapt, longer adaptation timelines, simplified technical documentation and self-assessments, reduced audit fees, and support mechanisms like vouchers, open compliance tools, and free templates. A technical feasibility clause and recognition of best-effort measures until interoperable standards are available can provide workable bridges. Safeguards are needed to prevent the cascading of compliance duties along supply chains. Proportionality is reinforced by focusing on high-criticality products, lighter regimes for low-risk activities, and targeted exemptions (e.g., “benign products”). Alignment and sequencing across regulations (e.g., CRA/RED/NIS-2) can avoid double regulation and allow businesses to integrate compliance efficiently. Concepts like distinguishing a product’s “digital lifetime” from its physical lifetime add legal certainty and economic viability. Collectively, these measures reduce costly disruptions, help smaller actors scale, and maintain competitiveness while preserving safety and cybersecurity objectives. They aim to maximize real transparency and risk reduction without overwhelming SMEs, thereby supporting innovation and practical compliance across diverse sectors.

That requires realistic implementation timelines tied to the availability of harmonised standards, standards-based conformity that companies can actually use in practice, and SME-appropriate documentation and reporting so effort scales with risk and not with company size. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Obligations should be phased in to allow SMEs and mid- caps to adapt, with lighter regimes for lower-risk activities. (Association française de normalisation (AFNOR))

Article 3(4a): "benign product" means a product which cannot cause a cybersecurity risk because it is technically too limited to do so." (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)

The European Com- mission should introduce a "digital lifetime" concept, defined and transparently declared by the manu- facturer, to allow for risk-based and economically viable support obligations. (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)

Assuralia: Argues that digital rules like DORA place disproportionate burdens on smaller firms, signaling the need for calibrated requirements and transition relief for SMEs.

DORA's requirements disproportionately burden smaller firms.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Calls for proportionate, risk-based timelines tied to the availability of harmonised standards, with extended entry-into-application for high-risk AI, SME-appropriate documentation, and practical support such as feasibility clauses, vouchers, and first-time error correction to ensure fair transitions.

That requires realistic implementation timelines tied to the availability of harmonised standards, standards-based conformity that companies can actually use in practice, and SME-appropriate documentation and reporting so effort scales with risk and not with company size.

Association française de normalisation (AFNOR): Urges phased-in obligations with lighter regimes for lower-risk activities so SMEs and mid-caps can adapt, coupled with safeguards to prevent cascading compliance duties down supply chains.

Obligations should be phased in to allow SMEs and mid- caps to adapt, with lighter regimes for lower-risk activities.

Verisure: Welcomes burden reduction for SMEs but warns that staggered CRA applicability without timely standards and guidance creates uncertainty, advocating clearer, predictable timelines to avoid disproportionate SME impacts.

The CRA's staggered applicability creates uncertainty, especially as harmonised standards and guidance may arrive too close to the reporting start date (September 2026).

ISP Alliance a.s.: Stresses that frequent regulatory changes strain small and micro enterprises, urging stable requirements, clear guidance, and transitional periods to minimize disruption.

Therefore, we urge the Commission to ensure that any new requirements under the Digital Omnibus are stable over time, with guidance, transitional periods, and minimal disruptive changes.

Schneider Electric: Notes that regulatory complexity impedes smaller companies from scaling and supports incremental, pragmatic implementation that advances ecosystems without overwhelming SMEs.

Such a pragmatic approach would allow incremental but consequential progress across entire ecosystems without overwhelming smaller actors.

Adigital (Asociación Española de la Economía Digital): Supports a phased rollout of transparency indicators so mid-sized firms can prioritize what is most relevant to their sector, improving proportionality and impact.

A phased approach would allow mid-sized companies to focus on the most relevant indicators for their sector and business model, maximizing the real impact of transparency.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Requests realistic, standards-linked CRA transition periods, delays where vertical standards are not ready, and proportional obligations focused on high-criticality products, including exemptions and simplified documentation to avoid undue burdens and cliff effects.

The link of transition periods to the availability of harmonized European standards and the introduction of the concept of "benign products" (see below) would mitigate this risk.

Business & Science Poland: Proposes temporary relief for firms newly crossing into medium size to avoid cliff-edge effects, enabling a fair, phased transition from SME provisions.

Healthtech Finland: Calls to curb cliff-edge transitions by extending SME-supportive provisions and phasing obligations so growing firms can adapt without disproportionate shocks.

European DIGITAL SME Alliance: Advocates aligning AI Act enforcement schedules with SME readiness and standards availability, ensuring predictable timelines and proportionate compliance paths.

Zentralverband der deutschen Werbewirtschaft (ZAW): Supports proportionate, phased compliance relief tailored to SMEs, emphasizing gradual timelines that scale obligations with risk and capacity.

: Warns that overly strict, abruptly applied rules cause costly disruptions, underscoring the need for predictable, phased transitions that spare SMEs from sudden burdens.

SaferAI: Recommends a time-boxed delay in enforcement for SMEs to provide a fair transition window while maintaining overall policy objectives.

1.3.5 Proportionate Reporting, Documentation & Transparency

This category calls for proportionate, risk-based reporting, documentation, and transparency obligations that scale with the nature of the service and the size of the provider, prioritizing SMEs. Insights emphasize streamlining and avoiding duplicated reporting, simplifying complex registers and templates, and tailoring documentation requirements (including AI Act quality management and DORA registers) to materiality and actual risk. Clear, specific rules are favored to prevent overly expansive interpretations that impose undue burdens or stifle innovation, while focusing internal records and logs on essentials. Burden-reduction practices include shorter retention periods for public reports, reduced cost accounting and data requests (especially across long supply chains), and standardized, user-friendly privacy notices. Proportionality also means omitting low-value transparency database imports, limiting prescriptive translation mandates, and scaling back ex-ante obligations where authorities can request information as needed. Automation/RegTech and consent frameworks with safeguards are promoted to deliver transparency and accountability efficiently without unnecessary administrative overhead.

> *Ensuring that obligations remain risk-based and practical, so that reporting requirements are meaningful and manageable for all actors, including SMEs.* (Docusign)
>
> *This is especially important for SMEs, who should not be burdened with duplicated reporting processes, nor required to disclose unnecessary sensitive information to competing market participants.* (FIGIEFA aisbl)
>
> *This effectively means that hardware and software vendors are required to translate all technical documentation in all 23 official EU languages, including the documents issued by third-party conformity assessment authorities.* (Emerson Electric Co.)
>
> *In view of that, as well as in view of administrative burden on the side of the providers to establish the API or send the individual statements of reasons (after excluding personal data) via the web interface manually, the added value of the DSA Transparency Database by smaller online platforms is rather minimal, so importing the data into the Commission's database can be omitte* (Seznam.cz, a.s.)

FIGIEFA aisbl: Urges streamlining incident reporting to cut costs and avoid duplication, especially for SMEs, and to protect sensitive information from competitors.

> *This is especially important for SMEs, who should not be burdened with duplicated reporting processes, nor required to disclose unnecessary sensitive information to competing market participants.*

Docusign: Advocates proportional, risk-based reporting obligations so requirements remain meaningful and manageable for all, including SMEs.

> *Ensuring that obligations remain risk-based and practical, so that reporting requirements are meaningful and manageable for all actors, including SMEs.*

German Insurance Association: Calls to simplify DORA register documentation, arguing current complex models and subcontractor documentation are disproportionate to benefits.

> *The current requirements for creating and maintaining the register of in- formation - e.g. complex data model and subcontractor chain documen- tation - are disproportionate to the actual benefits and should be simplified.*

Seznam.cz, a.s.: Seeks to reduce administrative burdens via simpler rules and templates while preserving privacy, and argues smaller platforms should omit low-value transparency database imports.

> *In view of that, as well as in view of administrative burden on the side of the providers to establish the API or send the individual statements of reasons (after excluding personal data) via the web interface manually, the added value of the DSA Transparency Database by smaller online platforms is rather minimal, so importing the data into the Commission's database can be omitte*

Centre for Democracy and Technology Europe: Highlights that some AI Act duties do not add new documentation and endorses documentation proportional to provider size with simplified options for microenterprises.

> *In a further accommodation to providers, the AI Act states that the extent of the documentation under the quality management system shall be proportionate to the size of the provider's organisation84 and*

that microenterprises may comply with certain elements of the quality management system in a simplified manner.85

Bolt: Proposes shorter public retention periods to reduce burden while keeping older information accessible to authorities on request.

We propose reducing the public retention period to one year, with older reports made available upon request to competent authorities or interested parties.

Ibec: Recommends explicitly recognizing proportionality and a risk-based approach in GDPR compliance to provide certainty and reduce burdens.

Explicitly recognise proportionality and a risk-based approach in measures applied to demonstrate compliance with GDPRXvi.

Namirial Spa: Asks for a proportional documentation regime for low-risk services, with simplified templates and risk-based reporting for micro and small QTSPs.

Define a proportional documentation regime for low-risk services, allowing micro- and small-enterprise QTSPs to use simplified templates and risk-based reporting, as recommended in the BDI simplification framework.

Emerson Electric Co.: Warns that blanket translation of all technical documentation into all EU languages is overly prescriptive and burdens smaller vendors.

This effectively means that hardware and software vendors are required to translate all technical documentation in all 23 official EU languages, including the documents issued by third-party conformity assessment authorities.

Meta Platforms Ireland Limited: Calls for clear, proportionate provider obligations and scaling documentation and compliance burdens according to risk, with standardized, user-friendly notices.

Reduce Excessive Compliance Burdens: Scale back documentation and compliance requirements according to risk, provide clear guidance on data subject requests, and encourage standardised, user-friendly privacy notices to focus on meaningful information for citizens.

Adigital (Asociación Española de la Economía Digital): Flags disproportionate cost accounting and CSRD reporting burdens on smaller firms, urging reduction of required data and more efficient compliance tooling.

The information structure required by the CSRD is similar for both large corporations and SMEs, creating a disproportionate load.

: Promotes practical user instructions and training to minimize misuse, aligning documentation with effective, risk-based mitigation rather than volume.

Manufacturers shall ensure that the information (instructions for use) includes recommended profile and training for the user and that the risk of user error when manipulating the device and interpreting the results is minimised.

ACEA (European Automobile Manufacturers' Association): Argues ex-ante Data Act reporting generates unnecessary administrative burden and should be replaced by on-demand information requests from authorities.

These requirements may create an unnecessary administrative burden on data holders as they require generating and communicating extensive documentation, which is likely to overwhelm competent authorities, and is unnecessary as competent authorities are empowered to request any information they deem necessary from data holders to verify compliance with the Data Act (Art. 37(14)).

Business & Science Poland: Supports proportionate documentation using simplified formats to ease compliance, particularly for SMEs.

Bayerische Motoren Werke Aktiengesellschaft: Urges limiting internal compliance documentation to essentials that are risk-relevant to avoid unnecessary burdens.

EHIMA: Advocates proportionate logging and reporting aligned to risk levels, avoiding excessive detail and overhead.

VDMA - Advancing Europe´s machinery industry: Calls to cap obligations and limit reporting/retention duration to reduce administrative load while preserving oversight.

Japan Business Council in Europe (JBCE): Seeks balanced limits on data-related obligations to prevent disproportionate documentation burdens across companies.

IBM: Opposes burdensome non-technical certification/documentation add-ons for high-risk tiers, favoring proportionate requirements.

Confederation of Industry of the Czech Republic: Recommends removing disproportionate subcontracting chain documentation and reporting obligations.

Ministry of Industry and Trade of the Czech Republic - this entry represents the official position of the Czech Republic for the section "Targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules: Proposes proportionate, simplified documentation and targeted exemptions for low-risk or small providers.

DOT Europe: Prefers targeted transparency safeguards over rigid structural separations, emphasizing proportionate transparency obligations.

Association des Constructeurs Européens de Motocycles: Supports risk-based carve-outs for low-risk documentation and limiting internal-use obligations to essential elements only.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Calls for proportionate information duties and access rules tailored to SMEs' capacities.

Sdružení pro internetový rozvoj (SPIR): Proposes excluding minor content changes from reporting and exempting small services from burdensome transparency reports.

secunet Security Networks AG: Advocates risk-based, proportionate notification thresholds to focus reporting on material issues.

Orgalim - Europe's Technology Industries: Urges simplified documentation for low-risk products with digital elements, aligned to proportionality.

PPC: Warns that excessive compliance burdens can undermine real protections, calling for proportionate obligations.

Charter of Trust: Supports risk-based, proportionate incident notification requirements to prioritize significant events.

Insurance Europe: Seeks stronger proportionality under DORA and simplification of overlapping reporting channels.

LinkedIn Ireland: Encourages flexible, standards-based transparency requirements to keep reporting meaningful and workable.

PensionsEurope: Promotes proportionality and materiality filters in documentation and reporting to avoid undue burdens.

European Publishers Council: Calls for proportionate advertising transparency and labelling that are practical for smaller publishers.

Alliance Digitale: Recommends exempting SMEs from onerous record-keeping and simplifying reporting obligations.

DIGITALEUROPE: Warns that overly strict safeguards create disproportionate burdens and urges risk-calibrated documentation duties.

AMETIC: Promotes automation and self-assessment to streamline compliance documentation and reduce reporting workload.

AER - Association of European Radios: Seeks proportionate simplification to avoid heavy administrative burdens for radio broadcasters.

BUGLAS e.V.: Argues mandated retention periods waste provider resources and should be right-sized and time-limited.

Too Good To Go: Supports flexible, risk-based documentation obligations with explicit proportionality clauses to protect SMEs.

VAUNET - German Association of Private Media: Notes GDPR reporting and documentation duties are disproportionate and should be right-sized to risk.

1.3.6 Proportionate Oversight & Enforcement

This category advocates proportionate, risk-based oversight and enforcement calibrated to actual risk, market evidence, and organizational capacity—especially for SMEs and startups. It rejects blanket or overly prescriptive obligations and duplicative checks, urging that enforcement, guidance, and audits remain necessary, targeted, and predictable. Authorities should recognize existing business risk practices, focus on significant impacts, and assess compliance on a best-efforts, outcomes-based basis, with legal safeguards to prevent disproportionate penalties. Operationally, it promotes limiting audit rights and monitoring to what is strictly needed, enabling mutual or alternative assurance mechanisms, and leveraging regulatory equivalence to avoid re-auditing. It supports targeted audits and maturity assessments, self-assessment or self-certification for lower-risk cases, flexible and time-bound monitoring with handbrakes, scope confined to direct suppliers, and evidence-based deregulation where markets function. Concrete measures include lifetime or conditional risk-based certification to cut burden, risk-based penetration testing to avoid service disruptions, “tell-and-do” urgent changes with no safety impact, and tailored complaint and verification systems for smaller entities, alongside reversed or outcomes-focused oversight that concentrates on residual risks.

It is thus important to ensure that the AI Act's provisions are enforced proportionately. (The International Center for Law & Economics)

Audit rights should also be limited to what is necessary and proportionate, ensuring they do not exceed the scope mandated by DORA. (GSMA)

Repeal regulated wholesale rates given market data (from BEREC) indicates market prices are at the competitive level. (Vodafone Group)

Introduce the possibility of having changes that will be classified as tell and do to avoid delays in implementation e.g. manufacturing changes that will not affect safety or performance but are urgent for the manufacturer. (Alcon Laboratories Inc)

DigiFinland: Advocates shifting to lifetime, risk-based or conditional certification with clear criteria to reduce redundant oversight and burdens when evidence is limited.

Evaluate the need for re-certification every five years, considering a shift to lifetime risk-based certification to reduce duplication and administrative burden.

GSMA: Calls for DORA oversight that relies on existing NIS2 compliance, limits audits to what is necessary and proportionate, and tailors testing to risk to avoid disruptions.

Audit rights should also be limited to what is necessary and proportionate, ensuring they do not exceed the scope mandated by DORA.

Seznam.cz, a.s.: Urges that fee shifting obligations in dispute procedures be removed or applied only to large platforms to avoid disproportionate burdens on smaller services.

Therefore, this obligation should apply only to large or very large online platforms, or be omitted altogether.

The International Center for Law & Economics: Supports proportionate AI Act enforcement that preserves innovation capacity, especially for startups, and scrutinises implementing guidance to avoid overreach.

It is thus important to ensure that the AI Act's provisions are enforced proportionately.

Finnish Food and Drink Industries´ Federation (ETL): Requests regulators recognise companies' existing business-driven risk management under CER as sufficient where appropriate, avoiding duplicative oversight.

Regarding risk management obligations, particularly under the CER Directive, companies' existing business- driven risk management practices should be recognised and accepted.

Vodafone Group: Proposes deregulating wholesale roaming where competition is proven, signalling that oversight should be lifted absent market failure.

Simplification of wholesale roaming process will send a strong signal that ex ante regulatory obligations will only be imposed and maintained where there is evidence of market failure.

Alcon Laboratories Inc: Asks for tell-and-do pathways for urgent low-risk manufacturing changes to prevent enforcement bottlenecks when safety and performance are unaffected.

Introduce the possibility of having changes that will be classified as tell and do to avoid delays in implementation e.g. manufacturing changes that will not affect safety or performance but are urgent for the manufacturer.

FEDIL, the Voice of the Luxembourg's Industry: Seeks predictable, proportionate, risk-based enforcement with clear criteria to ensure compliance focus matches actual risk.

: Recommends targeted, risk-based restrictions instead of blanket bans to avoid unnecessary burdens while addressing specific harms.

DigitalTrade4.EU: Argues that scoped, risk-based oversight can justify deregulation where risks are low, fostering innovation and competition.

Test and Measurement Coalition: Supports allowing self-assessment and streamlining conformity checks to prevent enforcement bottlenecks and focus oversight on higher risks.

The European Lotteries Association: Advocates prioritising effective enforcement against bad actors while reducing undue compliance burdens on compliant operators.

BusinessEurope: Calls for proportionate CRA obligations, outcome-focused monitoring, and calibrated penalties aligned with actual risk and company size.

U.S. Chamber of Commerce: Urges strong legal safeguards and due process around fines to prevent disproportionate penalties, especially for SMEs.

Confederation of Industry of the Czech Republic: Proposes flexible monitoring and stronger regulatory handbrakes to pause or adjust rules when impacts prove excessive.

Confederation of Norwegian Enterprise (NHO): Requests limits on monitoring duration and flexibility to adapt obligations over time, aligning oversight with evolving risk.

ITI - Information Technology Industry Council: Supports proportionate, risk-based compliance and enforcement that avoids duplicative audits and recognises global best practices.

Salesforce, Inc.: Endorses supplementary checks only for residual risks, keeping oversight targeted and proportional.

CPME: Asks authorities to value and recognise SMEs' good-faith compliance efforts, tailoring enforcement accordingly.

Verband der Automobilindustrie e.V.: Recommends risk-based oversight with exceptions and alternative pathways where equivalent safeguards exist.

Sdružení pro internetový rozvoj (SPIR): Seeks proportional limits on complaint handling for small providers and confines trader verification to reasonable efforts to avoid excessive burdens.

Google: Urges presumption for compliant self-assessments and evidence-based, proportionate interventions before imposing intrusive oversight.

Business Software Alliance: Requests that any new contract penalties be proportionate and calibrated to the severity and risk of non-compliance.

Orgalim - Europe's Technology Industries: Proposes sanctions only where companies refuse to comply, favouring corrective guidance over punitive measures for cooperative firms.

ACT | The App Association: Advocates SME-friendly enforcement and a Digital Fitness Check to screen new proposals for proportionality and burden.

Filter and assess new legislative proposals.

Digital Currencies Governance Group (DCGG): Suggests risk-based offline monitoring protocols to reduce false positives and concentrate enforcement on high-risk activity.

INVERCO: Calls to reinforce proportionality in supervision and streamline oversight to reduce redundant reporting and inspections.

Computer & Communications Industry Association (CCIA Europe): Urges proportionality in both interpretation and amendments, opposes strict liability expansions, and assesses compliance on best efforts rather than perfection.

Danish Industry: Warns that some DPAs apply insufficiently risk-based oversight and calls for more consistent, proportionate supervision.

Free ICT Europe Foundation: Supports proportionate allocation of cybersecurity responsibilities across the lifecycle, avoiding one-sided burdens.

DIGITALEUROPE: Asks to allow tailored monitoring rather than a uniform template and to use a reversed mechanism for targeted oversight when risks materialise.

ECIS, European Committee for Interoperable Systems: Advocates proportionate oversight for core technology providers and enabling self-certification where risk is low.

Mirakl: Calls for predictable, proportionate enforcement with clear guidance to support compliant marketplaces.

Estonian Ministry of Justice and Digital Affairs: Proposes targeted audits and maturity assessments to align supervisory intensity with actual risk exposure.

Adyen: Supports outcomes-based, proportionate, risk-adjusted oversight that avoids prescriptive rules.

Schaeffler AG: References US precedents to argue for flexible, risk-based oversight that encourages innovation.

Confederation of Swedish Enterprise: Promotes risk-based accountability frameworks that safeguard innovation while ensuring proportionate enforcement.

1.3.7 Level Playing Field, Fair Costs & Burden Sharing

This category argues for a risk-based, SME-friendly proportionality that delivers a genuine level playing field through fair cost and burden sharing. Stakeholders warn that compliance complexity and one-size-fits-all obligations disproportionately hit SMEs, startups, small platforms, municipal midcaps, and smaller public

actors, while large platforms and often non-EU firms retain structural advantages (e.g., data access, scale, and resources). The consequences include higher per-unit compliance costs, market exits, chilled innovation, slower operations (e.g., insurance claim handling), and even unintended distributional effects where burdens fall on smaller actors or their users (e.g., P2P participants), rather than those best placed to shoulder them. Proposed remedies include ambitious administrative-cost reductions, targeted deregulation, and upstream-focused duties that reduce burdens downstream. Concrete tools highlighted across the insights are tiered or capped fees (e.g., cost-only SME compensation under the Data Act), SME preferences in data access, support for certification and notified-body fees, and refined definitions to ensure municipal SMEs and midcaps benefit from relief. Stakeholders call for avoiding prescriptive or mandatory standards/templates that raise compliance costs, fixing asymmetric reimbursement and expense-shifting rules, and calibrating obligations and sanctions to the scale and risk profile of services. The goal is to preserve protections while removing disproportionate burdens so SMEs, researchers, and smaller platforms can compete, comply, and innovate on fair terms.

> *Sole traders and SMEs face disproportionate costs for compliance (DPIAs, consent mechanisms, technical anonymisation) relative to gatekeepers.* (Siinda)
>
> *The net effect of this burden of regulation is that only larger companies - which are often non-EU based - have the financial capacity and incentive to bear the costs of complying.* (Digital Poland Association)
>
> *When the DMA was enforced against Google's hotel-search features, European hotels experienced a 30% drop in direct booking traffic and a 36% decline in direct bookings.* (The International Center for Law & Economics)
>
> *A medium-sized company with 500 employees incurs an average cost of €1.3 million to comply with the GDPR, with an additional €1.1 million annually for ongoing compliance.* (Adigital (Asociación Española de la Economía Digital))

Verband kommunaler Unternehmen e.V.: Calls for proportionate regulatory relief for municipal SMEs and midcaps, noting they are excluded from SME benefits due to public ownership thresholds. Seeks to prevent disproportionate bureaucratic burdens on local utilities.

> *The digital omnibus must therefore also create tangible regulatory relief in data regulation for municipal SMEs and mid-caps and must not continue to burden them disproportionately with bureaucratic hurdles.*

Neogy.cz: Warns that restrictions hit smaller players harder while large platforms retain data advantages through accounts and dominance. Advocates measures that restore a level playing field in access and compliance burdens.

> *Large digital platforms and corporations, by contrast, maintain access to user data through account-based systems and market dominance, and thus are not equally affected by the restrictions.*

ZVEI e.V.: Supports ambitious reductions in administrative costs, especially for SMEs, to ensure proportionate compliance. Emphasizes cost-cutting as necessary for competitiveness.

> *The goal of a 25% reduction of administrative costs for all businesses and 35% for SMEs by 2030 is ambitious and necessary.*

Digital Poland Association: Argues that heavy regulatory burdens skew the market toward large, often non-EU, firms able to absorb costs. Calls for proportionality to keep SMEs competitive.

> *The net effect of this burden of regulation is that only larger companies - which are often non-EU based - have the financial capacity and incentive to bear the costs of complying.*

France Digitale: Highlights that regulatory complexity risks pushing startups into inadvertent non-compliance. Urges a clear, proportionate framework to avoid unfair burdens on young firms.

> *As a result, young companies risk falling into non-compliance not out of negligence, but due to the sheer difficulty of interpreting and implementing the rules.*

Unipol Assicurazioni S.p.A.: Notes disproportionate compliance demands on insurers, particularly SMEs, which may delay claims and increase penalties risk. Calls for proportional obligations aligned with sector realities.

Moreover, the current framework places disproportionate compliance burdens on insurers, especially SMEs, and risks delaying claim settlements, potentially exposing companies to administrative penalties under sectoral supervisory rules.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Calls for the Data Act to enable innovation without imposing disproportionate duties on data holders and users. Flags rising administrative and expertise costs across regulators.

The Data Act must support data-driven innovation without imposing disproportionate obligations on data holders and users.

Airbus: Urges avoiding disproportionate, counterproductive burdens on development teams. Stresses proportionality to protect innovation capacity.

It is essential to avoid imposing a disproportionate and counter-productive burden on our development teams.

Siinda: Notes that SMEs face higher relative costs for compliance tasks than gatekeepers. Seeks proportionate requirements that reflect firm size and capacity.

Sole traders and SMEs face disproportionate costs for compliance (DPIAs, consent mechanisms, technical anonymisation) relative to gatekeepers.

Seznam.cz, a.s.: Small platforms face disproportionate burdens and sanction risks relative to their minimal scale, and unfair exposure to dispute costs. These pressures can force exits from the market.

This leads to a disproportionate burden and has already forced some of these platforms to cease trading.

Alliance for Responsible Data Collection: Proposes an approach that empowers SMEs and researchers with traceable data practices without exclusionary rights. Emphasizes avoiding disproportionate burdens on smaller actors.

It enables downstream users to know where, when, and how data was collected and whether the collection met responsible-sourcing principles-without granting exclusionary rights or imposing disproportionate burdens on smaller actors.

Sheridans, on behalf of Awin AG: Suggests deregulation to ease entry for SME affiliate marketers who lack resources for complex compliance. Notes CPA models help SMEs manage predictable marketing costs.

It would also encourage new entrants to affiliate marketing, especially SMEs, who often do not have the resources to implement more complex compliance measures and may be deterred by the risk of enforcement.

The International Center for Law & Economics: Warns that ignoring business user impacts harms SMEs and startups reliant on standard analytics and ads tools, with sectoral losses as seen in hotels. Calls for proportionate remedies that do not undercut smaller actors.

This is particularly problematic for SMEs and startups that depend on standard web analytics and advertising technologies to compete effectively in digital markets.

Adigital (Asociación Española de la Economía Digital): Advocates strengthening existing instant payments over costly new infrastructures and reducing burdens on platforms and small operators. Highlights very high GDPR compliance costs for mid-sized firms.

A medium-sized company with 500 employees incurs an average cost of €1.3 million to comply with the GDPR, with an additional €1.1 million annually for ongoing compliance.

Alcon Laboratories Inc: Recommends tiered notified body fee structures by device complexity and company size to reduce SME burdens. Seeks cost-reflective, proportionate certification.

Introduce tiered fee structures based on device complexity and company size, benefiting SMEs

ACEA (European Automobile Manufacturers' Association): Notes existing EU data rules that cap or prefer SME compensation to ensure proportional access and costs. Points to these as models for fair burden sharing.

For example, the compensation requested for the provision of data to an SME pursuant to the Data Act cannot exceed its cost for the data holder and thus may not include a margin under (Article 9(4)).

FEDIL, the Voice of the Luxembourg's Industry: Calls for proportionate deregulation across firm sizes so obligations do not overburden SMEs. Emphasizes risk-based tailoring for fairness.

European Law Institute: Opposes contractual practices that shift regulatory burdens downstream to smaller parties. Seeks safeguards against superfluous burden shifting.

Telekom Austria AG: Urges reducing disproportionate obligations on non-platform providers to maintain fair competition. Calls for scope and duty calibration by risk and role.

Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs (VÖWG): Seeks a fair SME definition that does not exclude publicly owned local enterprises from reliefs. Aims to level the playing field for municipal providers.

VDMA - Advancing Europe´s machinery industry: Warns that compliance and reporting hit SME machinery firms disproportionately. Requests risk-based proportionality and streamlined obligations.

European Signature Dialog: Argues that overly prescriptive standards entrench large incumbents and disadvantage SMEs. Calls for balanced standards to avoid undue barriers.

ITI - Information Technology Industry Council: Highlights that mandatory standards and layered rules inflate compliance costs and deter SME entry. Advocates proportionality and flexibility to lower barriers.

Association des Constructeurs Européens de Motocycles: Notes regulatory burdens cascade onto SMEs and dealers in the motorcycle sector. Seeks calibrated requirements that reflect actor size and capacity.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: States current interpretations disadvantage craft SMEs. Calls for SME-friendly proportional application of rules.

Sdružení pro internetový rozvoj (SPIR): Warns that DSA compliance templates and expense-shifting duties overburden small platforms and businesses. Calls to limit overreach and protect SMEs from disproportionate costs.

Digitalexperte: Proposes shifting compliance obligations upstream to manufacturers to relieve SME customers and sellers. Aims for fairer allocation of duties by control and capacity.

Google: Argues blanket self-preferencing bans can unintentionally harm SME business users who benefit from integrated services. Seeks risk-based, proportionate rules.

Centre for Cybersecurity Belgium: Finds NIS2 annex requirements disproportionate for smaller entities. Recommends scaling security obligations by risk and size.

Suomen Yrittäjät - The Federation of Finnish Enterprises: Urges proportionate SME obligations and bans on unfair transfers of costs or liability down the chain. Seeks clearer protections for small enterprises.

BDSI: Warns that expanding ESG duties impose rising burdens on SMEs. Calls for simplification and supportive measures to keep compliance proportionate.

SGI Europe: Notes complex compliance frameworks strain smaller public service providers. Advocates proportionate implementation to avoid undue burdens.

Seznam.cz, a.s.: Reports that burdens are pushing small platforms out of the market and seeks limits on Article 21(5) cost obligations. Aims to prevent unfair expense shifting to smaller providers.

ACT | The App Association: Stresses that cumulative regulatory demands impose excessive burdens on app economy SMEs. Calls for SME-centric proportionality to sustain innovation.

Renault Group: Notes certain mandates raise costs disproportionately for smaller EV products and suppliers. Requests proportionate timelines and flexibility to avoid penalizing smaller actors.

CLOUD INFRASTRUCTURE SERVICES PROVIDERS IN EUROPE: Advocates support and scaling for certification costs so SME cloud providers can comply affordably. Seeks fair access to assurance schemes.

Charter of Trust: Calls for fair allocation of compliance and remediation duties across supply chains. Aims to avoid overburdening SMEs relative to larger partners.

Bundesverband Digitale Wirtschaft (BVDW): Supports reducing compliance costs while preserving user protections to keep rules proportionate for SMEs. Emphasizes competitiveness and practicality.

Computer & Communications Industry Association (CCIA Europe): Flags discriminatory and asymmetric fee and obligation designs that unfairly burden certain operators. Urges even-handed, risk-based cost sharing.

Danish Industry: Observes that smaller firms bear higher relative compliance loads. Calls for simplification and proportionate thresholds.

Alliance Digitale: Advocates consistent, proportionate GDPR application to reduce burdens that hinder SME competitiveness. Seeks clearer, risk-based enforcement.

Middle Tech Europe: Supports proportionate, targeted obligations for very large platforms that avoid spillover burdens on mid-sized European tech. Emphasizes balanced enforcement.

Mirakl: Warns equal obligations across diverse marketplaces can create dependence and disproportionate costs for smaller actors. Calls for calibrated transparency and duties.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Recommends focusing obligations upstream on dominant actors to lighten burdens on downstream SMEs. Seeks more equitable distribution of compliance tasks.

Council of European Municipalities and Regions (CEMR): Urges ending discrimination in SME definitions that exclude publicly owned local entities from reliefs. Calls for fair access to proportional measures.

Schaeffler AG: Notes SaaS compliance and certification costs can deter SME-oriented product launches. Requests proportionate schemes to keep offerings viable.

The European Network of Expertise on Omics: Highlights that complex data rules can overburden smaller research actors. Calls for proportionate requirements that support innovation without excessive costs.

1.3.8 SME Simplification, Guidance & Support Tools

This category advances risk-based, SME-friendly proportionality by pairing lighter obligations with concrete simplification, guidance, and support tools. It promotes scaled pathways for low-risk use (e.g., Codes of Conduct), clear templates and helpdesks/toolkits, and practical legal guidance across the AI Act, GDPR, the Data Act, and sectoral rules. It also seeks accessible sandbox participation and proportionate support for microenterprises and sole traders, standardized voluntary frameworks that reduce administrative load and ease supplier data exchange, and streamlined onboarding (KYC/AML) so small firms can adopt compliant practices efficiently. Reinforced SME and competitiveness checks and graduated compliance aim to prevent a "compliance cliff" where only large firms can fully implement rules. Stakeholders flag persistent pain points—

unclear or broad regulations that raise costs and deter small teams, definitional and verification hurdles that exclude certain SMEs (e.g., municipal utilities) or shift burdens to data holders, and founders' concern that the AI Act is a disproportionate barrier. Proposed remedies include technical-feasibility clauses and best-effort compliance until interoperable standards exist, proportionate obligations backed by practical support and simplified templates, and verifiable mechanisms to confirm SME status—so simplification is both inclusive and trustworthy.

Facilitate Codes of Conduct for low-risk cases to give SMEs scalable compliance tools. (Technology Industries of Finland)

Protect sole traders with proportionate obligations and practical support. (Siinda)

However, due to the reference to the SME definition, which excludes companies in which the public sector has a direct or indirect stake of 25 percent or more, local public utility companies do not benefit from these measures. (Verband kommunaler Unternehmen e.V.)

Only 20% of founders expect a positive impact. (Meta Platforms Ireland Limited)

FERMA - Federation of European Risk Managers Associations: Advocates enhanced proportionality measures and scaled compliance tailored to SMEs.

Enhance further proportionality measures, notably for SMEs.

Verband kommunaler Unternehmen e.V.: Notes that proposed EU simplifications hinge on an SME definition that excludes municipals with public ownership. Urges amending the definition so local utilities can benefit.

However, due to the reference to the SME definition, which excludes companies in which the public sector has a direct or indirect stake of 25 percent or more, local public utility companies do not benefit from these measures.

Neogy.cz: Observes small firms typically have only basic analytics and cannot identify individuals. Suggests obligations reflect their lower-risk, aggregated data use.

They are therefore unable to identify specific individuals such as "John Smith, living at Random Street 4, Exampletown, viewed this page."

Technology Industries of Finland: Calls to facilitate codes of conduct for low-risk cases to give SMEs scalable compliance tools. Emphasizes aligning GDPR, Data Act, and AI Act with operational realities.

Facilitate Codes of Conduct for low-risk cases to give SMEs scalable compliance tools.

FIGIEFA aisbl: Seeks clear guidance on the interplay between the AI Act and sectoral rules to provide legal certainty. Aims to make compliance practical for SMEs.

Clear guidance on the interplay between the AI Act and sectoral rules (e.g. type approval, product safety) is essential.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Warns that broad or unclear rules create legal uncertainty and high compliance costs. Notes this deters small teams from using or releasing open-source components.

Broad or unclear regulations may discourage small teams from using or releasing open-source components because of legal uncertainty and high compliance costs.

Siinda: Advocates proportionate obligations and practical support for sole traders. Calls for access to regulatory sandboxes with lower initial burdens and fast feedback.

Ensure sole traders can use regulatory sandboxes to test interoperable features or data-sharing models with lowered initial compliance burdens and fast feedback.

Mastercard Europe SA: Highlights cumbersome, time-consuming onboarding for SMEs in financial services. Proposes the EBW to streamline KYB and AML compliance for business customers.

We understand that onboarding in particular SMEs can still be a very cumbersome and time-consuming exercise, leading to many inefficiencies.

The International Center for Law & Economics: Supports reinforcing SME and competitiveness checks in EU rulemaking. Aims to simplify and speed processes while protecting smaller firms.

In the already-cited communication on "A Simpler and Faster Europe", the Commission highlighted that "improving how we make rules" will be a priority, and that this will include "reinforced SME and competitiveness checks".

Meta Platforms Ireland Limited: Reports startups and SMEs view the AI Act as a disproportionate barrier. Notes very few founders expect a positive impact.

European startups and SMEs, already struggling under heavy compliance demands, view the AIA largely as a disproportionate barrier.

Adigital (Asociación Española de la Economía Digital): Urges reducing administrative burdens and aligning with SME simplification initiatives. Proposes a voluntary, simplified SME standard to ease reporting and support standardized supplier data.

Small and medium-sized enterprises, especially those outside the directive's scope, need a simplified framework that minimizes administrative burden.

: Calls for a graduated compliance regime to avoid cliff-edge effects for smaller firms. Also seeks clarity on SME obligations when developing AI systems.

Similar to the EU's recognition of a "cliff edge" for all business from big-tech to small and mid-cap firms, ASRIC urges a graduated compliance regime that allows African ALL to demonstrate progressive conformity with simplified EU rules, avoiding exclusion due to cost and technical barriers.

European AI Forum: Recommends a technical feasibility clause and best-effort compliance until interoperable standards exist. Aims to make requirements proportionate to SME capabilities.

Introduce a technical feasibility clause for SMEs.

ACEA (European Automobile Manufacturers' Association): Proposes an SME verification and certification mechanism. Seeks to reduce burden on data holders and streamline SME data requests.

A verification and certification mechanism for SMEs should be developed.

: Emphasizes SME-accessible simplification through proportionate obligations, templates, and guidance. Aims to prevent a compliance cliff favoring large firms.

Proportionate obligations, simplified templates, and guidance can prevent a compliance cliff where only large companies can afford full implementation.

: Advocates shared infrastructure and common tools to help SMEs meet compliance affordably.

Business & Science Poland: Calls for targeted SME support and service improvements to ease compliance and adoption.

European Law Institute: Notes that broad GDPR obligations burden smaller players. Suggests risk-focused simplification to right-size requirements for SMEs.

DigitalTrade4.EU: Supports streamlined, proportionate compliance frameworks and dedicated support for small and mid-sized companies.

Free Trade Europa: Argues regulatory burdens fall disproportionately on SMEs and calls for simplification and risk-based relief.

European Signature Dialog: Highlights complex rules overburdening SMEs and seeks clearer, simpler obligations and tools.

Nordic Financial Unions - the Nordic financial trade unions confederation: Endorses scalable compliance mechanisms that fit SME capacities within risk-based frameworks.

VDGH – Verband der Diagnostica-Industrie e.V.: Notes heavy administrative demands strain SMEs and supports simplification to protect innovation.

Healthtech Finland: Warns regulatory burdens jeopardize SME innovation in healthtech and urges proportionate, supportive tools.

Confederation of Industry of the Czech Republic: Stresses SMEs bear disproportionate compliance costs and calls for proportionality and guidance.

Brighten Digital: Requests practical tools and clear guidance to help SMEs navigate AI Act requirements efficiently.

Deutscher Steuerberaterverband e.V. (DStV): Advocates user-friendly processes and templates tailored to small market participants.

Outpacr / VAICE: Proposes leveraging EU programs to provide tools and training that support SME compliance.

ENCIRCLE Research Consortium: Calls for clear guidance and sector-ready toolkits to streamline SME compliance.

CPME: Supports simplification to reduce SME burdens and provision of support tools for smaller healthcare providers.

Advertising Information Group: Supports proportionate obligations and practical tools so SMEs can comply without excessive cost.

Plateforme de la filière Automobile: Suggests mechanisms to verify SME status to streamline processes and reduce burdens.

Google: Encourages SME and consumer impact tests to ensure simplification and usability in regulation.

MVFP Medienverband der freien Presse e.V.: Calls for proportionate, risk-based measures tailored to SME capacities in media.

Suomen Yrittäjät - The Federation of Finnish Enterprises: Proposes holistic helpdesks and simplification of GDPR processes to assist SMEs.

secunet Security Networks AG: Advocates support for SME compliance and equitable access to security resources and sandboxes.

EFCA - European Federation of Engineering Consultancy Associations: Seeks simplification to counter DGA complexity and provide SMEs with manageable compliance pathways.

International Information System Security Certification Consortium, Inc.: Notes heavy compliance burdens on SMEs and recommends simplified frameworks and capacity-building.

Business Software Alliance: Recommends standardized toolkits and funding to build SME compliance capabilities.

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: Urges binding SME-focused impact assessments to minimize disproportionate burdens.

Danish Entrepreneurs: Calls for practical implementation guides and proportionate obligations for startups and SMEs.

DECATHLON SE: Requests flexible compliance options and clear compensation guidance benefiting SMEs in supply chains.

European Entrepreneurs CEA-PME: Advocates proportional cybersecurity requirements and tailored support for SMEs.

Hugging Face: Suggests extending SME-friendly provisions to open-source communities maintaining AI tools.

PensionsEurope: Supports lighter, risk-based obligations for smaller entities to ensure feasibility.

Danish Industry: Promotes risk-based proportionality and SME-friendly simplification across the regulatory landscape.

Zentralverband Deutsches Baugewerbe: Calls to simplify procedures and extend SME relief across sectors.

Alliance Digitale: Notes GDPR imposes heavy burdens on SMEs and urges targeted simplification without reducing protections.

European DIGITAL SME Alliance: Seeks practical simplifications and cost reduction measures enabling SME compliance.

Free ICT Europe Foundation: Supports SME-friendly AI rules and tools like the Business Wallet to streamline obligations.

Dedalus S.p.A.: Encourages provision of compliance tools and guidance tailored to small healthtech providers.

AMETIC: Advocates centering simplification and guidance on SMEs to foster innovation and compliance.

Shopify: Proposes risk-based GDPR reforms that reduce SME burdens while preserving user protections.

Chamber of Commerce and Industry for Munich and Upper Bavaria: Supports lighter, more practical regulation and targeted support for SMEs.

Dutch Startup Association: Urges proportionate requirements aligned with startup capacities, avoiding stifling innovation.

Esomar: Calls for proportionate deregulation and simplified processes to aid SME research activities.

BUGLAS e.V.: Supports efficient, proportionate security requirements and argues simplification helps SMEs refocus on core tasks.

Estonian Ministry of Justice and Digital Affairs: Notes omnibus simplification packages can reduce SME burdens and improve regulatory coherence.

Veridas Digital Authentication Solutions: Requests clear guidance and standardized templates to streamline SME compliance.

Schaeffler AG: Warns that aspects of the Data Act may harm SMEs and calls for proportionate relief.

1.3.9 Miscellaneous

This category emphasizes risk-based, SME-friendly proportionality in regulation. Laws should be proportionate, cost-effective, and grounded in robust impact assessment from the outset, avoiding complex or disproportionate requirements that later need simplification and impose avoidable costs. Clear, consistent, and proportionate rules enable firms of all sizes to innovate, compete, and deliver value while achieving regulatory objectives

efficiently. The approach prioritizes efficiency over bureaucratization: obligations should scale with risk and organizational capacity, especially for SME-heavy sectors (e.g., EdTech), so compliance remains practical without diluting high standards. By right-sizing requirements and assessing impacts early, policymakers can sustain trust, protect consumers, and support sustainable innovation across markets.

> *To ensure that regulatory objectives are achieved efficiently and sustainably, legislation should be accompanied by robust impact assessments and should consider cost-effectiveness and proportionality from the outset.* (Assuralia)
>
> *Clear, consistent, and proportionate regulation is essential to enable companies of all sizes to innovate, compete, and deliver trusted products to consumers across Europe and beyond.* (AIM - European Brands Association)
>
> *More broadly, while the intention to uphold high standards is appreciated, introducing complex or disproportionate legal requirements that later require simplification can result in significant and avoidable costs for companies.* (Assuralia)

Assuralia: Advocates designing regulation that is proportionate and cost-effective from the outset, grounded in robust impact assessments to avoid unnecessary complexity and costs. Emphasizes efficient, sustainable achievement of regulatory objectives.

> *To ensure that regulatory objectives are achieved efficiently and sustainably, legislation should be accompanied by robust impact assessments and should consider cost-effectiveness and proportionality from the outset.*

AIM - European Brands Association: Argues that clear, consistent, proportionate rules are key to enabling firms of all sizes—including SMEs—to innovate and compete. Positions proportionality as a driver of consumer trust and market performance.

> *Clear, consistent, and proportionate regulation is essential to enable companies of all sizes to innovate, compete, and deliver trusted products to consumers across Europe and beyond.*

Johnson & Johnson: Calls for minimizing bureaucratic burdens and applying proportionality to streamline regulatory processes. Prioritizes efficiency to ensure compliance efforts are commensurate with risk.

Software & Information Industry Association (SIIA): Highlights the diverse scale of the EdTech sector, stressing the need for SME-sensitive, proportionate approaches. Suggests tailoring requirements so smaller providers can comply without undue burden.

1.4 Competitiveness & Innovation Enablement

Reducing regulatory and administrative friction through proportionate, predictable, and harmonised rules—and once-only compliance—is the strongest lever to convert innovation into competitiveness across the Single Market. Technology-neutral clarity and fit-for-purpose checks lower costs and build trust. Open, contestable markets reinforce this by ensuring neutral governance, fair treatment of functionally similar business models, switching, and modernised antitrust that avoids new gatekeepers while preserving value-adding services for SMEs. Capital formation and scaling benefit from low-bureaucracy, outcomes-based funding, a completed Capital Markets and Banking Union, streamlined listings, and RegTech, while pan-EU sandboxes and TEFs should feed deployment through presumptions of conformity and fast-track, mutually recognised licensing. Competitiveness also depends on fluid talent mobility, portable credentials, inclusive upskilling, and AI tools that ease language and training barriers. Balanced AI/data governance must align regimes, preserve open-source pathways, and avoid unrealizable obligations, and data access frameworks should protect trade secrets, contractual freedom, and enable responsible reuse of public data. Infrastructure-ready, performance-based standards, report/certify-once mechanisms, innovation-oriented procurement, faster permitting, and open, interoperable wallets help solutions scale. A pragmatic industrial strategy should back European champions without autarky, pairing sovereignty with openness. User-centric design, low-friction onboarding, responsible personalization, and data-driven measurement convert innovation into tangible outcomes, from telematics insurance to AI-supported diagnostics, while streamlined market mechanisms improve efficiency. Across sub-categories, common threads are simplification, harmonisation, evidence-based experimentation-to-deployment, contestability, legal certainty, and execution excellence. The dominant trend is outcome-based, learning-first governance that reduces friction and enables EU-wide scale.

1.4.1 Industrial Strategy, Sovereignty & Global Competitiveness

This category articulates a pragmatic European industrial strategy that pairs digital sovereignty with global competitiveness. It emphasizes building robust European alternatives in critical infrastructure and cyber by mobilizing private-sector capabilities, fostering sectoral champions, and treating technology, data, and AI as strategic assets. Stakeholders call for an ambitious, pro-innovation agenda—leveraging instruments like the Digital Omnibus, simplifying and harmonizing EU digital rules, and reducing compliance frictions (e.g., DSTs and uneven data-sharing obligations)—to reinforce leadership in health, life sciences, maritime technologies, and advanced connectivity, consistent with the EU's Resilience 2.0 goals. At the same time, the insights warn that exclusionary or overly restrictive approaches risk undermining competitiveness, ceding de facto standards to global Big Tech, and accelerating the lead of other regions. The proposed path balances sovereignty and openness: develop interoperable European solutions in strategic domains, avoid autarkic cul-de-sacs, and enable scale through fair competition and regulatory simplification. High ambition and targeted support for vertical champions are framed as essential to strengthen European players and ensure the EU catches up with faster-moving global peers.

> *While the EU's current infrastructure is overwhelmingly controlled by non-Eu- ropean actors, it is entirely feasible to build robust Euro- pean alternatives by mobilising private-sector capabi- lities without resorting to a centralised or state-heavy approach.* ()
>
> *As organisations cooperating in CEE Digital Coalition, a gathering of digital and advanced technologies industry organisations from Central-Eastern European Member States, bringing the region together on its digital path and working together to boost the digital transformation of the region's economy and informational society, we urge the European Commission to set ambitious goals for simplifying EU digital regulations to boost competitiveness and prosperity, and we stand ready to support this agenda.* (Digital Poland Association)
>
> *Europe's digital sovereignty will be under greatest risk if it excludes foreign technologies and pursues an autonomous cul-de-sac set of technologies which cannot compete globally, as Japan experienced.* (AI & Partners B.V.)
>
> *At the same time, while Europe decides and regulates increasingly complex systems, global Big Tech players continue to establish de facto standards through simple, userfriendly solutions rapidly adopted by European citizens.* (Namirial Spa)

: Suggests the EU can develop robust European alternatives to foreign-controlled infrastructure by leveraging private-sector capabilities, bolstering sovereignty and competitiveness without a state-heavy model.

> *While the EU's current infrastructure is overwhelmingly controlled by non-Eu- ropean actors, it is entirely feasible to build robust Euro- pean alternatives by mobilising private-sector capabi- lities without resorting to a centralised or state-heavy approach.*

SIEMENS AG: Warns that divergent data-sharing obligations create asymmetric burdens that could put EU industrial manufacturers at a competitive disadvantage versus non-EU vendors.

> *Manufacturers of industrial goods will be getting into disadvantageous competition w/ non-EU vendors, as different data sharing obligations might be exploited against the vendor with place of business in the EU.*

Assuralia: Supports proposals that enhance resilience and digitalisation to help the EU remain competitive and innovative amid uncertainty, aligning with strategic foresight.

> *These proposals directly contribute to the European Commissions Strategic Foresight report entitled Resilience 2.0, which calls for adaptability in crisis, digitalisation and a coherent approach to help the EU thrive (i.e. becoming more competitive and innovative) amid turbulence and uncertainty.*

EUROMOT - The European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers: Calls for targeted support to maintain and grow the global competitiveness of European maritime technology providers within the industrial strategy.

> *Support the competitiveness of European maritime technology providers*

EFPIA: Views the Digital Omnibus as a chance to streamline rules, removing barriers to life sciences innovation and improving Europe's competitiveness.

In conclusion, the Digital Omnibus offers a key opportunity to remove barriers to life sciences innovation.

Digital Poland Association: Advocates ambitious simplification of EU digital regulation to boost competitiveness and prosperity, with CEE industry organisations ready to support.

As organisations cooperating in CEE Digital Coalition, a gathering of digital and advanced technologies industry organisations from Central-Eastern European Member States, bringing the region together on its digital path and working together to boost the digital transformation of the region's economy and informational society, we urge the European Commission to set ambitious goals for simplifying EU digital regulations to boost competitiveness and prosperity, and we stand ready to support this agenda.

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Sees the Digital Omnibus Package as an opportunity to reinforce Europe's leadership and competitiveness in digital health.

The Digital Omnibus Package presents a significant opportunity to reinforce Europe's digital leadership in health.

GSMA: Urges a high level of ambition in reform to drive real change and strengthen European players' global competitiveness.

We believe that only a high level of ambition will result in real change and will strengthen European players

Telefonica, S.A.: Cautions that restrictive measures on 5G equipment could harm industrial competitiveness and cybersecurity, allowing other regions to advance faster.

This in turn, could harm industry competitiveness, high level of cybersecurity of such equipment, and result in other regions advancing more rapidly in smarter and more secured 5G networks due to the absence of such restrictions.

Airbus: Calls for fostering sovereign European cyber solutions to enhance competitiveness and resilience across industrial design, supply chains, and operations.

Support the emergence of alternative European solutions in cyber, which are vital for our competitiveness and resilience in digital initiatives across design, supply chain, and operations.

Leading Baltic tech and other businesses and professional associations listed in the submission: Argues that technology, data, and AI are strategic assets for strengthening Europe's economy, democracy, and security, underpinning competitiveness.

Technology, data, and AI should be seen not as potential threats, but as strategic assets that can strengthen Europe's economy, democracy, and security.

The International Center for Law & Economics: Criticizes enforcement approaches toward personalized advertising that overlook its economic role, potentially undermining the competitiveness of Europe's digital ecosystem.

EU data-protection authorities have demonstrated growing hostility to personalised advertising, refusing to recognise the economic nature of the relationship among online platforms, their users, and business users (advertisers).

Namirial Spa: Warns that complex EU regulation risks ceding standards to global Big Tech, weakening Europe's digital sovereignty and competitiveness.

At the same time, while Europe decides and regulates increasingly complex systems, global Big Tech players continue to establish de facto standards through simple, userfriendly solutions rapidly adopted by European citizens.

Meta Platforms Ireland Limited: Highlights that global peers follow pro-innovation paths, implying the EU must adjust to remain competitive.

In contrast, global peers are pursuing pro-innovation paths.

: Warns the EU is falling behind faster-moving global regions, jeopardizing competitiveness and growth.

The EU is not the world, and the rest of the world, i.e. the majority of humans are advancing much faster than we are and is now developing much better than us.

Finnish Food and Drink Industries´ Federation (ETL): Emphasizes regulatory simplification to keep legislation current and support the competitiveness of Europe's food system.

Simplification is essential to ensure legislation remains up to date and supports the competitiveness of Europe's food system.

Adigital (Asociación Española de la Economía Digital): Notes that national digital services taxes disproportionately burden advanced EU digital firms, raising compliance costs and dampening competitiveness.

Many European companies with advanced digital models get caught by the thresholds and sectoral criteria of national DSTs, significantly increasing their compliance costs and reducing taxable profits in their home countries.

AI & Partners B.V.: Argues that excluding foreign technologies in the name of sovereignty can create an uncompetitive cul-de-sac; Europe must stay open and globally competitive.

Europe's digital sovereignty will be under greatest risk if it excludes foreign technologies and pursues an autonomous cul-de-sac set of technologies which cannot compete globally, as Japan experienced.

Doctrine: Suggests building European champions in specific verticals rather than competing broadly, focusing industrial strategy to enhance competitiveness.

At Doctrine, we firmly believe that this goal can be achieved by fostering the development of European champions in specific verticals rather than engaging in an overly broad international race.

Fédération des Industries Ferroviaires: No specific insight about industrial strategy, sovereignty or competitiveness is available from the provided excerpt.

Business & Science Poland: No specific insight about industrial strategy, sovereignty or competitiveness is available from the provided excerpt.

European Law Institute: No specific insight about industrial strategy, sovereignty or competitiveness is available from the provided excerpt.

DigitalTrade4.EU: No specific insight about industrial strategy, sovereignty or competitiveness is available from the provided excerpt.

Cisco: No specific insight about industrial strategy, sovereignty or competitiveness is available from the provided excerpt.

1.4.2 Open Markets & Fair Competition

Open Markets & Fair Competition centers on keeping the EU Single Market open, contestable, and predictable by ensuring a genuine level playing field. Stakeholders call for competition-enhancing policies that lower barriers to entry, enable switching, and preserve infrastructure-based rivalry, while rejecting protectionism and regulatory asymmetries. Market governance should remain neutral and market-driven (e.g., avoiding public monopolies), and rules should balance horizontal and sectoral approaches so that functionally similar business models—such as platforms and direct sales—are treated fairly. To keep markets contestable, policymakers should assess impacts on challenger firms and SMEs, remove unnecessary restrictions (such as limits on price transparency), and avoid compliance designs that entrench incumbents or privilege pre-selected actors. A resilient ad-supported ecosystem is seen as pro-competitive: targeted advertising tools are vital for SMEs and publishers, so interventions should not degrade them without weighing collateral effects on business users or media pluralism. Finally, competitive openness is linked to innovation dynamism: accept firm exit and resource reallocation, modernize antitrust for digital infrastructure and interoperability, allow value-added services, and

favor operational alternatives over structural separation mandates. The aim is a coherent, light-touch framework that streamlines the Single Market, prevents new gatekeepers, addresses contractual imbalances without bias, and sustains cross-border trade and investment.

> *The main objective of this initiative should be to ensure a level playing field and find a better balance between horizontal and sectoral regulation when developing digital rules.* (Unipol Assicurazioni S.p.A.)
>
> *European digital industrial policy should aim to improve, rather than limit, competition - for example by lowering barriers to entry and ensuring customers are free to switch to different options that better meet their needs.* (AI & Partners B.V.)
>
> *National rules unnecessarily restrict ride-hailing platforms from transparently displaying prices and availability, creating barriers to consumer choice and market efficiency.* (Bolt)
>
> *This uncertainty can potentially reduce collaboration between startups, researchers and civil society and risks shifting innovation towards large proprietary platforms.* (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

ZVEI e.V.: Urges more ambitious reforms beyond the Commission's proposals to foster a competitive, innovation-driven Digital Single Market.

This initiative must be used to take bold but necessary measures that go beyond the EU Commissions proposed measures to build a truly competitive and innovation-driven Digital Single Market.

: Advocates a stronger business environment for publishers so they can capture fair value, particularly through advertising, reflecting fair competition with platforms.

Publishers put in a lot of hard work developing audiences and they should be the ones to reap the rewards from that work, notably in the form of correspondingly high advertising prices.

FEBIS: Warns that a centralized European Business Wallet could distort competition by privileging select entities and sidelining existing business information providers, calling for open, neutral governance.

If the Wallet's governance and operational frameworks are skewed toward a small number of state-backed or pre-designated entities, it could disrupt the market by creating an uneven playing field, where only a few selected actors benefit from privileged access and legitimacy.

Unipol Assicurazioni S.p.A.: Calls for a predictable, coherent framework that ensures a level playing field across sectors, enabling secure innovation and competitiveness in the Digital Single Market.

These targeted adjustments are vital for creating a level playing field and a coherent and predictable regulatory environment that serves as a catalyst, not an impediment, for a secure, innovative, and competitive digital Single Market.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Highlights that regulatory uncertainty can deter collaboration and shift innovation toward large incumbents, undermining competitive openness for startups and researchers.

This uncertainty can potentially reduce collaboration between startups, researchers and civil society and risks shifting innovation towards large proprietary platforms.

Snap Inc.: Recommends impact assessments explicitly consider effects on challenger platforms to avoid entrenching incumbents and preserve competitive digital markets.

Expand impact assessments to explicitly examine the effects of new legislation on challenger companies in digital markets, in addition to traditional SMEs.

Bolt: Argues that national limits on price transparency in ride-hailing impede consumer choice and market efficiency, harming fair competition.

National rules unnecessarily restrict ride-hailing platforms from transparently displaying prices and availability, creating barriers to consumer choice and market efficiency.

The International Center for Law & Economics: Contends that enforcement curbing targeted advertising risks collateral harm to SMEs and new entrants who depend on efficient audience targeting, undermining competitive parity.

Many EU businesses-particularly SMEs-simply could not function without cost-effective ways to target relatively niche audiences.

Namirial Spa: Advocates a market-driven European Business Wallet interoperable with trust services, rejecting a public monopoly to keep competition open.

The forthcoming European Business Wallet must be conceived as a market-driven initiative, not a public monopoly.

Adigital (Asociación Española de la Economía Digital): Calls for tax and regulatory neutrality so online platforms are not disadvantaged versus equivalent direct-sales models, ensuring a level competitive field.

DSTs unfairly penalize online platforms compared to direct sales models (such as hotel chains), even though both forms of operation are functionally similar.

AI & Partners B.V.: Urges policies that lower barriers to entry, enable customer switching, and embrace market dynamism rather than protecting incumbents, to keep markets open and competitive.

European digital industrial policy should aim to improve, rather than limit, competition - for example by lowering barriers to entry and ensuring customers are free to switch to different options that better meet their needs.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Seeks a level playing field with Big Tech while safeguarding infrastructure-based competition to spur innovation and efficient investment.

Infrastructure-based competition must remain a cornerstone of the legal framework, ena- bling different infrastructure providers to coexist, and at the same time best safeguarding innovation, and continuous and efficient investments in infrastructure.

American Chamber of Commerce to the EU: Urges the EU to reject protectionism and maintain openness to trade and investment as the foundation for competitive markets.

iProov Ltd: Criticizes proposals that compromise technology neutrality and entrench legacy providers, warning they would stifle innovation and fair competition.

European Travel Retail Confederation (ETRC): Argues that overly strict rules impede market access and limit competition in travel retail, calling for proportionate, open-market policies.

Business & Science Poland: Proposes replacing blanket bans on gatekeepers with targeted coercive tools to address abuses while preserving competitive dynamics.

carVertical: Favors market-based solutions over state-run platforms to encourage competition and innovation in digital services.

DigitalTrade4.EU: Advocates freedom for businesses to choose IT solutions, modernized antitrust suited to digital infrastructure, and streamlined cross-border trade to strengthen the Single Market's competitiveness.

Free Trade Europa: Supports liberalization and free trade as drivers of competitive markets and consumer welfare in Europe.

Federation of Austrian Industries: Calls for the EU to remain open and globally connected and to avoid protectionism to sustain competitive industry.

U.S. Chamber of Commerce: Urges addressing protectionist and extraterritorial EU measures that fragment markets and hinder fair competition.

Intesa Sanpaolo: Highlights contractual imbalances with big tech and seeks rules that restore fair bargaining and competition.

Kompetenznetzwerk Datentreuhandmodelle (DatNet): Recommends allowing value-added services in data trustee models to stimulate competition and innovation while safeguarding trust.

ITI - Information Technology Industry Council: Promotes operational remedies over structural separation to address competition concerns without undermining efficient market structures.

Advertising Information Group: Stresses that ad-funded online services support growth and should be preserved to sustain competitive, open digital markets.

eyeo GmbH: Urges simplification to strengthen the advertiser–publisher marketplace, enhancing competition and transparency in digital advertising.

Fedoweb - Federazione Operatori Web: Warns that current pressures risk closures of media outlets and calls for policies that promote competition and media pluralism.

Google: Warns that conflicting regulations can unintentionally harm competition, and advocates balanced changes that foster contestability and innovation.

Connect Europe: Backs deregulation to correct asymmetries and open markets, improving competitive conditions across the digital economy.

Prosus Group: Argues that a presumption of suspicion toward large tech firms deters investment and innovation, undermining competitive markets.

Computer & Communications Industry Association (CCIA Europe): Warns that structural separation mandates would deter intermediaries and reduce market efficiency, advocating less distortive competition tools.

European Publishers Council: Claims certain rules distort the digital advertising market and exacerbate platform dominance, calling for fairer competitive conditions for publishers.

SAP SE: Asserts that in SaaS markets parties can negotiate on equal footing, suggesting ex ante restraints may be unnecessary to ensure fairness.

ACT (Association of Commercial Television and Video on Demand Services in Europe): Notes that compliance burdens disproportionately favor gatekeepers and crowd out investment, weakening competition and diversity in media markets.

European DIGITAL SME Alliance: Calls to open digital markets and remove barriers so SMEs can compete on equal terms and scale in the Single Market.

Zentralverband der deutschen Werbewirtschaft (ZAW): Argues data-driven advertising sustains an open internet and warns that consent and AI rules or labeling obligations could distort competition if miscalibrated.

AMETIC: Advocates alternatives to blanket structural separation mandates to maintain competition while enabling innovation and investment.

OpenAI: Supports streamlining and deregulatory measures to reduce fragmentation in the Single Market and boost competitive innovation.

Mirakl: Warns that current regulations burden startups and favor incumbents, calling for competition-friendly rules that nurture digital marketplaces.

Dutch Startup Association: Urges policymakers to avoid creating new digital gatekeepers and to keep markets open for startups and challengers.

Esomar: Highlights risks of market concentration in AI and calls for safeguards that preserve competition and innovation.

1.4.3 Proportionate, Predictable Regulation

Proportionate, Predictable Regulation centers on making EU rules clearer, lighter, and more consistent so innovation and competitiveness can flourish. Stakeholders call for technology-neutral, proportionate implementation that recognizes existing sectoral frameworks and operational realities, with predictable, clear rules and recurring "fit-for-purpose" checks to keep legislation up to date. Proposals include embedding an innovation principle and explicit economic/innovation objectives, streamlining and clarifying across files via the Digital Omnibus, and decisively cutting administrative burdens while withdrawing provisions that needlessly impede European champions. They warn that today's overlapping horizontal and sectoral acts create a complex compliance ecosystem that absorbs resources, raises costs, and deters international engagement—sometimes derailing ongoing projects—while Europe's compliance burden remains heavier than other regions. A smarter simplification agenda should target rules that truly hinder innovation (e.g., ePrivacy/cybersecurity overlap), account for indirect effects on business users, and balance competitiveness with robust risk mitigation. Above all, regulatory clarity builds trust and reduces costs; early, coherent steering can ensure regulation facilitates rather than hampers innovation.

However, implementation must remain proportionate, technology-neutral, and recognising existing EU and sectoral frameworks, as well as operational realties. (Eurofinas)

If we want European companies to succeed in global competition, the rules must be predictable and clear. (FiCom ry)

The proliferation of horizontal and sectoral acts - including the NIS 2 Directive, Cyber Resilience Act (CRA), Artificial Intelligence Act (AI Act), revised eIDAS Regulation, Data Act, and GDPR - has created a complex ecosystem that absorbs resources, slows innovation, and limits the competitiveness of European digital service providers. (Namirial Spa)

However, a slight easing of the compliance burden will not unlock the innovation Europe needs to adapt to a fast-changing technological landscape. (Meta Platforms Ireland Limited)

: Advocates embedding an Innovation Principle into EU treaties to ensure regulation systematically considers innovation impacts. This aims to make rules more predictable and proportionate for competitiveness.

The integration of the "Innovation Principle" in the EU treaties as proposed by the ESPC in 2016 is also important.

Verband kommunaler Unternehmen e.V.: Welcomes swift, significant reductions in administrative burdens to strengthen competitiveness. Calls for practical, proportionate regulation for local public utilities.

The Commission's proposal to quickly and significantly reduce the administrative burden on businesses to strengthen Europe's competitiveness is explicitly welcomed by the local public utilities sector.

SIEMENS AG: Urges the Commission and Member States to use the Digital Omnibus to remove provisions that hinder European tech champions. Seeks a coherent, predictable framework that enables innovation.

The Commission must now spearhead this Digital Omnibus package jointly with Member States to withdraw provisions harmful for European tech champions.

Enel SpA: Warns that regulatory complexity deters international business and raises compliance costs. Calls for simplification to improve competitiveness and predictability.

The complexity of the current regulatory framework may discourage international business engagement and increase compliance costs.

Technology Industries of Finland: Supports recurring fitness checks to keep rules up to date and fit for purpose. This iterative approach promotes proportionate, predictable regulation.

Iterate via continuous "fit for purpose" evaluations by making the fitness check a recurring exercise to keep regulations up to date.

Workday: Notes that Europe's legislative and compliance burden remains heavier than other regions. Argues that predictability and proportionality must improve to remain competitive.

Even with these recommendations, Europe's legislative environment and compliance burden will remain significantly heavier than other regions.

CGI Inc.: Commits to a coherent, practical, innovation-friendly digital regulatory environment. Supports proportionate, predictable rules to foster competitiveness.

We appreciate the opportunity to contribute to this consultation and remain committed to supporting the EUs efforts to build a coherent, practical, and innovation-friendly digital regulatory environment.

Dun & Bradstreet: Backs a simplification agenda focused on smarter regulation that achieves outcomes efficiently. Emphasizes enabling responsible innovation, including AI and privacy-enhancing technologies.

Our position is that the simplification agenda is about smarter regulation that delivers intended outcomes more effectively and enables responsible innovation, including the adoption of AI and privacy-enhancing technologies.

Unipol Assicurazioni S.p.A.: Stresses balancing competitiveness with robust risk mitigation. Warns that recent legislative actions risk unintended barriers to economic and technological development.

Achieving the right balance between competitiveness and robust risk mitigation is paramount, particularly as recent legislative actions risk creating unintended barriers to economic and technological development.

Eurofinas: Insists on proportionate, technology-neutral implementation that respects existing frameworks and operational realities. Seeks predictable compliance for financial services.

However, implementation must remain proportionate, technology-neutral, and recognising existing EU and sectoral frameworks, as well as operational realties.

German Insurance Association: Highlights the significant resource demands of DORA implementation. Urges proportionate timelines and requirements to manage compliance costs.

The implementation of DORA has required insurance companies to invest in sig- nificant resources.

GSMA: Calls for more ambition in removing barriers that hinder innovation and competitiveness. Targets ePrivacy and cybersecurity framework simplification.

In this regard, we believe that the Commission can be more ambitious in tackling regulation that truly hinders innovation and competitiveness, particularly with regard to the ePrivacy Directive and cybersecurity framework simplification.

LSEG: Argues that regulatory clarity fosters trust, reduces compliance costs, and promotes innovation. Predictable rules support digital resilience and competitiveness.

Such clarity would also foster greater trust among stakeholders, reduce compliance costs, promote innovation and support the EU's broader objectives of digital resilience and competitiveness.

The International Center for Law & Economics: Urges simplification efforts to consider indirect effects on business users of platforms. Warns that restrictions can harm downstream competitiveness.

Simplification efforts must consider significant indirect effects, including how restrictions on digital platforms harm their business users.

Namirial Spa: Notes that proliferating digital acts create a complex, resource-absorbing ecosystem. Calls for coherence and simplification to avoid slowing innovation and competitiveness.

The proliferation of horizontal and sectoral acts - including the NIS 2 Directive, Cyber Resilience Act (CRA), Artificial Intelligence Act (AI Act), revised eIDAS Regulation, Data Act, and GDPR - has created a complex ecosystem that absorbs resources, slows innovation, and limits the competitiveness of European digital service providers.

Meta Platforms Ireland Limited: Maintains that minor easing of compliance burdens will not unlock needed innovation. Calls for deeper, predictable regulatory reform to enable competitiveness.

However, a slight easing of the compliance burden will not unlock the innovation Europe needs to adapt to a fast-changing technological landscape.

: Critiques overuse of legislation under the pretext of citizen protection. Advocates restraint and proportionality to avoid overregulation.

It would be high time for the EU to adopt legislation on everything on the pretext of protecting the citizens of the different countries.

Adigital (Asociación Española de la Economía Digital): Proposes embedding an economic and innovation objective into all digital regulation. Aims to align rules with competitiveness and innovation enablement.

Likewise, it is proposed to incorporate into the principle of all digital regulation (Article 1) an "economic and innovation objective."

FiCom ry: States that predictable, clear rules are essential for European companies to succeed globally. Calls for regulatory certainty to boost competitiveness.

If we want European companies to succeed in global competition, the rules must be predictable and clear.

Akava: Seeks regulatory reform that expands access to EU digital services, accelerates business growth, and reduces costs. Advocates proportionate, pro-innovation rules.

the reform of regulation should promote access to European digital services, the rapid growth of the European business sector and reduce the costs brought by regulation,

ACEA (European Automobile Manufacturers' Association): Welcomes the Digital Omnibus as a step toward coherent, business-friendly regulation. Proposes measures to foster innovation and strengthen competitiveness in automotive digital transformation.

ACEA welcomes the Commissions Digital Omnibus Package as a vital step toward a coherent, business-friendly regulatory environment and proposes measures to foster innovation, strengthen competitiveness, and maintain Europes leadership in automotive technology and digital transformation.

AI & Partners B.V.: Calls for rapid adoption of Draghi's recommendations to enhance competitiveness. Seeks faster regulatory modernization to enable innovation.

all of which demands more rapid adoption of most of Mario Draghi's recommendations.

UNIFE: Warns that current timelines and scope for digital regulations risk cost increases and delays in rail projects. Calls for adjustments to keep regulation proportionate and feasible.

Without adjustments to timelines and scope, the application of these digital regulations to ongoing rail projects will significantly drive up costs, cause delays due to the possible consequences on vehicle authorisation, and jeopardise compliance with existing contracts and funding conditions.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Rejects bureaucratic, planned-economy approaches. Supports market-oriented, proportionate regulation that fosters innovation.

Any bureaucratic and planned economy approaches should be entirely avoided.

: Criticizes excessive regulations that degrade user experience. Calls for simple, proportionate rules that support usability and innovation.

Thank you for stopping creating absurd regulations that kill the user experience on the internet.

: Emphasizes early steering to ensure regulation facilitates rather than hampers innovation. Advocates proactive, predictable governance.

It can steer early and ensure that regulation does not hamper innovation, but facilitates it.

1.4.4 Infrastructure, Standards & Public Procurement

This category links infrastructure readiness, interoperable and market-relevant standards, and innovation-oriented public procurement to unlock competitiveness. Stakeholders call for alignment with international, performance-based, and technology-neutral standards—preferably voluntary and industry-led—while using harmonised approaches where they cut compliance friction (e.g., "report once" and "certify once") and improving cross-border consistency among national authorities. They caution against overly prescriptive specs that reduce flexibility, and propose tiered, evidence-based standardization and infrastructural neutrality so diverse solutions can compete on merit. On procurement, they highlight Europe's underuse of its buying power for innovation and urge innovation-promoting tenders—especially for AI—combined with stronger public-private partnerships, faster permitting for critical digital infrastructure, and sustainability and cost-benefit assessments for major wallet and identity investments. Infrastructure priorities include removing regulatory barriers to data centers and broadband, recognizing telecoms as an enabler for AI, cloud, and cybersecurity, and closing the gap between policy enthusiasm and actual deployment of edge computing. Around the EU Business Wallet, industry supports an open, flexible design that allows private actors to build value-added services, link individual and business wallets, and leverage certified business information providers and qualified attribute authorities to help SMEs manage risk. Practical ecosystem enablers—such as affiliate networks that standardize implementations—can improve scalability and security, but current legal frameworks can still hinder adoption of large-scale innovative, anti-fraud, and security technologies; clearer IP incentives and skills investment are also needed.

> *Maintaining a global perspective: Align with international standards to ensure European businesses remain globally competitive.* (Dun & Bradstreet)
>
> *Meanwhile, the EU's digital innovation stra- tegy has too often prioritised replicating existing digital services within captured digital infrastructures instead of fostering novel digital ecosystems, and has not leve- raged public procurement well enough, resulting in mis- sed opportunities to cultivate early-mover advantages.* ()
>
> *Introduce a Sustainability Assessment requirement for Member States, ensuring that public investments in Wallet infrastructures are backed by cost- benefit analyses and realistic adoption metrics, leaving space for market operators to build new business models with added value and without defining state monopolists instead of competitive market operators.* (Namirial Spa)
>
> *There remains potential for edge computing to develop in the context of AI, but for now enthusiasm for the technology in Europe has not been met with significant commercial deployment.* (AI & Partners B.V.)
>
> **:** The EU has underleveraged public procurement to drive novel digital ecosystems, prioritising replication within entrenched infrastructures and missing early-mover advantages.
>
> *Meanwhile, the EU's digital innovation stra- tegy has too often prioritised replicating existing digital services within captured digital infrastructures instead of fostering novel digital ecosystems, and has not leve- raged public procurement well enough, resulting in mis- sed opportunities to cultivate early-mover advantages.*
>
> **FEBIS:** Leveraging certified Business Information Providers within the EU Business Wallet can reduce SME information gaps and trade credit risk, enhancing competitiveness in commerce and procurement.
>
> *By leveraging certified BIPs, the EBW can help SMEs mitigate information gaps and reduce trade credit risk.*
>
> **Dun & Bradstreet:** Aligning with international standards and strengthening cooperation among national authorities will keep European businesses globally competitive through consistent implementation.
>
> *Maintaining a global perspective: Align with international standards to ensure European businesses remain globally competitive.*
>
> **Telefonica, S.A.:** Restrictive legal frameworks impede rollout of large-scale innovative services and advanced security tools, undermining infrastructure-driven consumer protection and competitiveness.

As a consequence of this, the current legal framework casts limitations on the adoption of large-scale innovative services, such as the GSMA Open Gateway initiative, advanced anti-fraud and security-related technologies that could add significant benefits to enhancing consumer protection.

Association française de normalisation (AFNOR): Streamlined report-once and certify-once processes grounded in harmonised standards and automated compliance can boost EU competitiveness and digital sovereignty.

By institutionalising the principles of « report once > and « certify once », grounding obligations in harmonised standards, and embracing automation and AI tools for compliance, Europe can strengthen both its competitiveness and its digital sovereignty.

Mastercard Europe SA: EBW infrastructure should allow design flexibility and linkage between individual and business wallets to unlock private-sector innovation in payments and contracting.

Allow design flexibility, including for payments, so private sector actors can build innovative, value-added services on top of EBW infrastructure.

Sheridans, on behalf of Awin AG: Affiliate networks provide standardised technical implementations that scale and enhance security and standard maintenance, while improving publisher-advertiser discoverability.

Affiliate networks also allow for more standardised technical implementations, which in addition to offering enhanced scalability also allows for better for information security and standard setting and maintenance.

Namirial Spa: Member States should assess wallet infrastructure sustainability via cost-benefit analyses and realistic adoption metrics, while supporting standards like ETSI TR 119 479-2 to spur private business models.

Introduce a Sustainability Assessment requirement for Member States, ensuring that public investments in Wallet infrastructures are backed by cost- benefit analyses and realistic adoption metrics, leaving space for market operators to build new business models with added value and without defining state monopolists instead of competitive market operators.

Adigital (Asociación Española de la Economía Digital): Allowing providers to define supply-chain standards preserves flexibility in complex ecosystems and fosters innovation without rigid mandates.

Allow providers to define their own standards within complex supply chains.

Vodafone Group: Robust telecoms infrastructure enables EU ambitions in AI, cloud, and cybersecurity, requiring supportive policy and investment.

Telecoms is an enabler of the Commission's wider goals on Al, cloud and cybersecurity.

WKÖ - Austrian Federal Economic Chamber: Innovation-oriented public procurement should prioritise AI applications built on public data infrastructures to accelerate adoption and competitiveness.

Building on public data infrastructures, innovation-promoting public procurement must focus on AI applications.

AI & Partners B.V.: Regulatory barriers impede rollout of data centres and broadband, and stronger IP regimes are needed to reward innovation. Despite policy bets on edge computing, enthusiasm has not translated into significant commercial deployment.

For example, regulatory barriers continue to pose significant constraints on the rollout of important infrastructure and assets like data centres and broadband networks, and EU regulation needs to provide a reliable and effective system of intellectual property rights ensuring sufficient rewards are available for innovating.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: German industry supports creating an EU Business Wallet as shared infrastructure to streamline business identity and transactions.

In addition, German industry supports the creation of an EU Business Wallet.

iProov Ltd: Performance-based, technology-neutral standards would maintain security while giving innovators flexibility across infrastructure and services.

European Signature Dialog: Permitting fee-based business identity services within the EU Business Wallet would incentivise private investment and expand sustainable offerings.

ITI - Information Technology Industry Council: Overly prescriptive specifications reduce flexibility; voluntary, evidence-based standards are preferred to drive interoperability and innovation.

ASNEF: Market-led, voluntary schemes should be favoured over mandatory approaches to keep standards adaptive and competitive.

Google: Greater investment in compute, connectivity, and digital skills is needed to enable innovation and sustain global competitiveness.

Bayer AG: Strengthening public–private partnerships with targeted funding can accelerate deployment of critical research and industrial infrastructures.

Dassault Systèmes: A market-based approach to standardisation prevents fragmentation and ensures interoperable, scalable infrastructures for innovation.

Computer & Communications Industry Association (CCIA Europe): Supporting industry-led initiatives and flexible frameworks allows standards to evolve with technology and market needs, speeding infrastructure innovation.

BioMed Alliance: Public institutions form the backbone of research infrastructure and require sustained support to translate discoveries into competitive innovations.

OpenAI: Fast-tracking permits for AI compute and data centres and modernising procurement with agentic public-sector innovation would accelerate infrastructure and service delivery.

The European Crypto Initiative (EUCI): Affirming infrastructural neutrality in distributed ledgers avoids lock-in and fosters competitive, interoperable innovation ecosystems.

Mistral AI: Tiered, proportionate standards can sustain competitiveness while enabling rapid scaling of AI infrastructure and products.

1.4.5 Capital, Scale-Up & Investment Climate

The Capital, Scale-Up & Investment Climate insights emphasize outcomes-based, low-bureaucracy funding that prioritizes commercially viable EU infrastructures and rationalizes fragmented tech funds into clear growth pathways to prevent relocation of scale-ups. Completing the Capital Markets Union and Banking Union—with common insolvency and tax rules and a unified EU Listing Act—together with a stronger single market and improved access to capital, would cut cross-border costs, streamline IPOs, and enhance Europe's competitiveness. Proposals like a dedicated "28th regime" to simplify labor, tax, and insolvency for innovative firms, plus more strategic investment behind European champions, aim to unlock EU-wide scaling and better returns. Insights warn that regulatory complexity, overlap, and fragmentation deter investors and favor incumbents, while uncertainty pushes startups to relocate or delay launches. Simplification and the adoption of RegTech can reduce compliance and reporting burdens, improve interoperability, and accelerate innovation—especially for SMEs—via accessible hubs, sandboxes, and collaboration platforms. Clarifying Data Act contractual rules is vital to protect SaaS recurring-revenue models that underpin fundraising and valuation, and evidence-based, transparent financing pilots (e.g., citizen stress indices and open EU datasets) can distinguish cooperative models that enable innovation from extractive ones, while reforms to approvals, InvestEU efficiency, and retroactivity safeguards further strengthen the investment climate.

A cornerstone of this second reform package, as ad- vocated for by Mario Draghi and Enrico Letta, must be the completion of the Capital Markets Union (e.g. com- mon insolvency as well as tax laws and a unified EU Lis- ting Act to streamline initial public offerings) and Ban- king Union to further reduce inefficiencies and costs in cross-border investment. ()

And such funds should be available without too much bureaucracy. ()

The key problem is the lack of a properly functioning single market - barriers to trade in services within the EU are estimated by the IMF to be the equivalent of a 45% tariff - and to capital markets in Europe. (AI & Partners B.V.)

In particular, the Commission proposes in its Competitiveness Compass a '28th regime' to streamline labour, tax and insolvency rules for certain types of innovative firms. (AI & Partners B.V.)

: Advocates outcomes-based, less bureaucratic EU funding focused on scalable, commercially viable infrastructures and a consolidated growth programme to keep scale-ups in Europe. Also urges completing the Capital Markets and Banking Unions and streamlining IPOs to cut cross-border investment frictions.

A cornerstone of this second reform package, as ad- vocated for by Mario Draghi and Enrico Letta, must be the completion of the Capital Markets Union (e.g. com- mon insolvency as well as tax laws and a unified EU Lis- ting Act to streamline initial public offerings) and Ban- king Union to further reduce inefficiencies and costs in cross-border investment.

Technology Industries of Finland: Calls for an EU programme to develop and deploy RegTech, with targeted funding for SMEs and startups and shared platforms to reduce compliance burdens. This would lower costs and unlock capital for scaling across Member States.

Prioritise funding for companies innovating in this space, especially SMEs and startups using AI-powered systems, to enhance automation in compliance checks, data privacy, and conformity assessments.

France Digitale: Warns that unclear Data Act contractual rules could destabilize SaaS revenue models, undermining startups' ability to raise capital and scale. Seeks clarifications to preserve long-term contracts underpinning investment and valuation.

certain contractual rules, if not clarified, risk undermining the business models of thousands of European startups and scaleups that are not cloud providers.

Adigital (Asociación Española de la Economía Digital): Argues that simplifying regulatory requirements is critical to create an agile environment that attracts investment into digital infrastructure. Streamlining would enable faster innovation and capital deployment.

Simplifying such requirements is essential to fostering a more agile and efficient regulatory environment, which is critical to encouraging investment and innovation in the digital infrastructure ecosystem.

European AI Forum: Highlights that regulatory fragmentation and uncertainty consolidate incumbents' advantages and deter investors, pushing early-stage AI ventures to relocate or delay scaling. Calls for coherent, predictable rules to enable EU-wide growth and financing.

This environment discourages startups from scaling EU-wide and deters international investors who view regulatory unpredictability as a structural risk.

: Proposes an EU-wide pilot to classify and compare public financing models, publishing an open dataset to guide evidence-based policy. The goal is to promote cooperative funding structures that support innovation and avoid extractive models.

It strengthens the evidence base so that the EU can better assess which types of funding support innovation and which stifle it.

AI & Partners B.V.: Identifies the malfunctioning single market and fragmented capital markets as core obstacles, with service trade barriers akin to a high tariff. Backs a streamlined regime to harmonize key rules so innovative firms can scale and attract investment.

The key problem is the lack of a properly functioning single market - barriers to trade in services within the EU are estimated by the IMF to be the equivalent of a 45% tariff - and to capital markets in Europe.

Fédération des Industries Ferroviaires: Urges limiting retroactive application of new rules to protect prior investments and provide legal certainty. This would safeguard capital planning and encourage long-term commitments.

DigitalTrade4.EU: Supports improving the efficiency and targeting of InvestEU to channel capital into competitive digital projects and scale-ups. Better leverage and faster deployment would strengthen Europe's investment climate.

Federation of Austrian Industries: Calls for streamlined funding and permitting processes to reduce delays and unlock private investment. Faster, predictable approvals would help firms scale and innovate in Europe.

Confederation of Industry of the Czech Republic: Stresses that heavy administrative burdens chill investment and hinder scaling, especially for SMEs. Advocates reducing red tape to improve Europe's competitiveness and capital flows.

ITI - Information Technology Industry Council: Warns that regulatory complexity and overlap deter innovation and private investment by increasing uncertainty. Recommends coherent, risk-based policy to enable faster R&D and market scaling.

IAB Europe: Argues that lowering compliance costs and ensuring predictability will improve the investment climate in digital markets. This would attract capital and support sustainable innovation.

Suomen Yrittäjät - The Federation of Finnish Enterprises: Advocates simplifying access to EU innovation funding for SMEs to improve capital availability. Easier, faster processes would accelerate scaling across the single market.

SGI Europe: Notes that outdated rules stifle investment in services of general interest and hamper modernization. Calls for regulatory updates that mobilize capital and enable innovation.

Prosus Group: Urges strategic public and private investment behind European champions and reforms that enable scaling. A more supportive framework would help EU firms compete globally.

Europe needs to invest more strategically behind its champions

Danish Industry: Calls to make the EU market more attractive for investment by reducing burdens and rebuilding trust, while addressing cuts to R&D spending. A stronger pipeline of public and private R&D would crowd in private capital and scaling.

DIGITALEUROPE: Emphasizes that simplifying rules and reducing uncertainty are essential to spur investment and innovation, particularly in AI. Warns that overregulation hampers scaling and commercialization in the EU.

Wolt: Argues that recalibrated, proportionate governance and clearer accountability would attract investment and support European leadership in digital services. Predictable rules would facilitate scaling across markets.

OpenAI: Advocates advancing the Capital Markets Union and tackling fragmentation to unlock financing for EU innovators. A deeper single market for capital would help AI and tech firms scale.

ECIS, European Committee for Interoperable Systems: Highlights the need for pricing flexibility that allows recovery of R&D investments to sustain innovation. Predictable returns improve the investment climate for interoperable systems.

TopCashback Group Limited: Supports policies that incentivize investment in consumer-facing digital tools, strengthening competition and innovation. A favorable climate would draw capital into EU platforms.

Schaeffler AG: Notes that high AI training costs hinder startups' ability to scale and raise capital. Calls for support to reduce compute and data costs or provide shared infrastructure.

1.4.6 Talent, Skills & Cross-Border Collaboration

This category captures how Europe can attract, retain, and fluidly deploy talent across borders to strengthen competitiveness. It emphasizes deregulation and harmonization to remove mobility barriers, including fast-track pathways for third-country ICT professionals, automatic recognition of qualifications from EU-recognised foreign institutions, smooth transitions from temporary permits to permanent residency, tax incentives for highly skilled workers, and simplified cross-border work arrangements. It also warns that regulatory complexity and compliance demands exacerbate skilled-labor shortages and that talent concentration can disadvantage smaller firms. Cross-border collaboration is enabled by legal frameworks that recognize public bodies as co-creators and data providers and that foster targeted cooperation with academia and business. Aligning simplification and deregulation with ERA priorities, alongside internationally harmonized and inclusive research frameworks, helps multinational teams and SMEs participate on equal footing. A resilient European skills base requires prioritizing upskilling and reskilling, multilingual onboarding to reduce friction, and portable, verifiable skills credentials. Emerging AI tools—such as live translation and personalized learning—can lower language and training barriers, while committed industry–EU partnerships and collaborative initiatives aim to scale these capabilities responsibly to advance Europe's innovation workforce and competitiveness.

> *Despite its world-class quality of life, the EU is losing ground in the global race for tech talent, held back by sluggish digitalisation, regulatory fragmentation, and barriers to mobility.* ()
>
> *This initiative would remove barriers to mobility, introduce tax incentives for highly skilled EU workers, and simplify cross-border working arrangements within the EU.* ()
>
> *By automatically approving qualified candidates from EU- recognised foreign universities and training institutions, the EU could drastically cut red tape, too.* ()
>
> *The carriers are not only users, but active co-creators and data providers: They develop their own data-based applications, e.g. for prevention or fraud detection, while providing valuable social data for research and innovation.* (German Social Insurance European Representation)

: Proposes an EU Tech Skills Acquisition Program and streamlined residency pathways to attract and retain ICT talent, including automatic recognition of top foreign qualifications. Recommends tax incentives and simplified cross-border work arrangements to boost mobility and keep skilled workers in the Union.

> *This initiative would remove barriers to mobility, introduce tax incentives for highly skilled EU workers, and simplify cross-border working arrangements within the EU.*

German Social Insurance European Representation: Calls for a legal framework that explicitly supports targeted cooperation between social insurance carriers, academia, and business. Emphasizes co-creation and data-sharing roles to drive innovation and skills development.

> *The legal framework should recognise this role and promote cooperation with academia and business in a targeted manner.*

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Warns that new compliance demands force companies to retool processes and hire specialized staff, worsening existing skilled labor shortages. Highlights the strain this places on competitiveness and talent availability.

> *Furthermore, they have to adapt their internal processes and hire specialised staff, which presents companies with additional challenges in the context of the acute shortage of skilled workers.*

American Chamber of Commerce to the EU: Notes that high-value talent clusters in large firms can disadvantage SMEs. Urges policies that distribute skills development and access more evenly across the ecosystem and borders.

Japan Business Council in Europe (JBCE): Advocates multilingual onboarding and support to reduce friction for workers and firms operating across EU markets. This would lower language and administrative barriers to cross-border collaboration.

Federation of Austrian Industries: Urges prioritization of upskilling and reskilling to address skills gaps and sustain innovation. Recommends scalable training initiatives through industry-led and public-private partnerships.

The Guild of European Research-Instensive Universities: Recommends aligning regulatory simplification with European Research Area priorities to ease researcher mobility. Streamlined, consistent rules would strengthen cross-border collaboration and talent flows.

Google: Commits to partnering with EU stakeholders to cultivate digital skills and support innovation ecosystems. Emphasizes cross-border research and training programs that include SMEs.

European Federation for Market Research Organisation (EFAMRO): Supports broad, inclusive, and internationally aligned research standards to enable cross-border studies. Such harmonization facilitates talent mobility and shared innovation capacity.

SAP SE: Advocates multi-stakeholder collaboration to build digital skills and strengthen Europe's competitiveness. Promotes cross-border project teams and partnerships between industry, academia, and government.

OpenAI: Proposes AI-powered live translation to remove language barriers and portable skills credentials to verify competencies across jurisdictions. These tools would enhance worker mobility and cross-border collaboration.

Esomar: Calls for a harmonized, inclusive EU research framework aligned with international norms. Consistency across borders would ease talent movement and collaborative research.

Software & Information Industry Association (SIIA): Highlights AI-assisted personalized learning to accelerate upskilling and reskilling. Personalized pathways can scale talent development across regions and sectors.

1.4.7 Data Access, IP & Legal Certainty

This category captures the tension between enabling data access for innovation and ensuring intellectual property and trade secrets are protected, with a premium on legal certainty. Stakeholders call for clear, predictable rules that preserve contractual freedom, empower individuals with control and transparency, and allow responsible business use of data. Strengthening trade secret protections, avoiding forced disclosure of sensitive assets like source code, robust R&D exemptions, and opening more public data are seen as levers to unlock new business models, support SMEs, and help create European champions. Risks flagged include heavy and unclear Data Act obligations that create bureaucracy, legal uncertainty, and disincentives to generate or share industrial data, potentially dampening B2B data-driven activity. Mandates that entrench robots.txt can cement a pay-per-crawl internet, disadvantaging SMEs and non-profits, while extraterritorial copyright exposure may deter frontier model availability in the EU. These dynamics risk chilling open-source participation, restricting access to state-of-the-art AI, and harming competitiveness unless reforms prioritize legal certainty, balanced data access frameworks, and protection of sensitive know-how.

By fostering an environment where there is legal certainty that data can be leveraged for innovation, new business models, and improved services, the EU can unlock significant economic potential and drive the growth of a thriving macroeconomy. (Meta Platforms Ireland Limited)

The DA creates legal uncertainty due to its often-unclear terminology and requirements. (SIEMENS AG)

By endorsing robots.txt as an access-control mechanism, the Code of Practice risks cementing a "pay-per-crawl" model of the internet. (Alliance for Responsible Data Collection)

For example, a model trained outside the EU with non-European content could face EU copyright obligations simply because it's later distributed in Europe. (Anitec-Assinform)

SIEMENS AG: Argues the Data Act imposes heavy bureaucracy and legal uncertainty, distorts contracts and markets, and reduces data generation and sharing, harming EU competitiveness and innovation.

It is thus proving to be a massive obstacle to the emergence of a European data economy in relevant industry segments and a heavy burden on competitiveness in international competition.

Technology Industries of Finland: Calls for explicit trade secret protections and confidentiality in Commission oversight of GPAI providers to ensure legal certainty for data handling.

Art. 91: Add protection for trade secrets, ensuring confidentiality of information obtained from GPAI model providers by the Commission under Art. 78.

Alliance for Responsible Data Collection: Warns that mandating robots.txt compliance creates an anti-competitive, pay-per-crawl data access regime that disadvantages SMEs, entrenches incumbents, and chills innovation.

This creates a discriminatory two-tiered system that advantages incumbents, undermines innovation, and contradicts the EU's goal of supporting SME participation in Al development.

Meta Platforms Ireland Limited: Advocates clear, predictable rules so data can be leveraged for innovation and competitiveness, while ensuring user control and avoiding premature regulation that undermines legal certainty.

By fostering an environment where there is legal certainty that data can be leveraged for innovation, new business models, and improved services, the EU can unlock significant economic potential and drive the growth of a thriving macroeconomy.

Finnish Food and Drink Industries´ Federation (ETL): Urges stronger protection of trade secrets to retain data-driven know-how within European companies and support innovation.

Protection of trade secrets and retention of data-driven expertise within European companies must be strengthened.

Anitec-Assinform: Cautions that extending EU copyright obligations to models trained outside Europe could deter distribution of frontier models and discourage international participation in the EU market.

This approach risks limiting availability of the best frontier models in the Union and discouraging international developers from serving the European market.

Doctrine: Notes the legaltech market remains open and that expanding access to public data could enable European champions and spur innovation.

This market is not yet dominated by one or more technological players, providing Europe with an opportunity to enable the emergence of a European champion by opening up more public data.

FEDIL, the Voice of the Luxembourg's Industry: Stresses the need for legal certainty to foster innovation and competitiveness across industry.

Free Trade Europa: Warns that disclosure obligations risk exposing trade secrets, which would undermine competitiveness and deter data-driven innovation.

Mafex – Spanish Railway Association: Calls for reform of the Data Act to reduce burdens and improve competitiveness, ensuring balanced data access without harming IP and trade secrets.

MedTech Europe: Advocates stronger trade secret protections in health technology to safeguard IP and maintain innovation incentives and competitiveness.

ITI - Information Technology Industry Council: Opposes compelled source code access, arguing it would compromise IP, security, and legal certainty and deter innovation.

AI Standards Lab: Argues that imposing compliance burdens on open-source developers is inappropriate and would chill participation, harming innovation and competition.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Highlights that legal uncertainty around open-source deters investment and adoption, especially for SMEs, weakening innovation capacity.

Bayer AG: Seeks clearer and broader R&D exemptions for data use to provide legal certainty and enable research and innovation without undue risk.

Prosus Group: Emphasizes the importance of accessible state-of-the-art AI models to drive innovation and competitiveness across the EU.

European Publishers Council: Contends that data access underpins publisher monetization and innovation, and that limiting to contextual-only ads and curbing personalization would threaten sustainability and competitiveness.

Danish Industry: Calls to strengthen trade secret protections, limit mandatory disclosure, and preserve contractual freedom to reduce legal uncertainty that restricts AI innovation.

Dedalus S.p.A.: Urges robust protection of IP and trade secrets to safeguard competitive advantage and enable trusted data-driven innovation.

DIGITALEUROPE: Warns that the Data Act, as implemented, harms competitiveness due to burdens and uncertainty, and calls for adjustments to restore a pro-innovation data economy.

Chamber of Commerce and Industry for Munich and Upper Bavaria: Advocates preventing competitive harm from the Data Act by ensuring proportionate obligations and legal certainty around data access and IP.

TopCashback Group Limited: Supports data-sharing improvements that enable faster onboarding and streamlined attribution, helping businesses innovate and compete.

WindEurope: Calls to safeguard trade secrets and IP to protect EU industry's competitiveness while enabling responsible data access.

1.4.8 Innovation-Friendly AI & Data Governance

Innovation-Friendly AI & Data Governance couples strong, trustworthy safeguards with pro-innovation levers. It calls for balanced, predictable, and harmonised rules that reflect the cross-sector nature of research and innovation, align AI policy with data and competition law, preserve open-source pathways, and pair regulation with pragmatic tools (e.g., codes of practice, templates, sandboxes) to accelerate safe uptake. By simplifying and clarifying frameworks like the AI Act and data/consent regimes, policymakers can reduce administrative burden, restore legal certainty, and enable diffusion of trustworthy AI across sectors while maintaining a level playing field across the Single Market. Contributors warn that the current European approach—spanning GDPR/ePrivacy and the AI Act, especially GPAI model rules—has grown overly complex and risk-averse, creating chilling effects, barriers to entry, and the risk of shifting R&D and investment abroad. They flag unintended harms to open-source developers and SMEs, constraints on data-driven and privacy-enhancing innovation, and sectoral headwinds in healthcare, finance, manufacturing, and safety. At the same time, tangible benefits (e.g., more inclusive insurance risk assessment) illustrate why governance should strengthen competitiveness, economic welfare, and societal outcomes. The throughline is to protect fundamental rights while enabling innovation: align and streamline obligations, avoid technically unrealizable requirements, and treat proportionate compliance as a trust and competitiveness advantage.

We also see the need and added value of effective regulation that strikes the right balance between safeguarding individuals' fundamental rights and enabling innovation and competitiveness. (GSMA)

The right balance, therefore, is not to reopen the AI Acts legal foundations but to couple strong regulation with pragmatic tools that promote uptake. (AI & Partners B.V.)

By embedding technically unrealisable requirements into binding law, the EU has risked converting its flagship AI regulation from a competitive advantage into a structural disadvantage - an innovation ceiling disguised as a safety floor. (Meta Platforms Ireland Limited)

The combined application of the AI Act, GDPR and ePrivacy Directive risks creating unintended barriers for open-source development and early-stage innovation. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

European Alliance for Research Excellence: Stresses data governance that mirrors the cross-sector nature of modern research to better enable innovation across domains.

Similarly, a modern data strategy must reflect the cross-sector nature of todays research and innovation ecosystem.

Unipol Assicurazioni S.p.A.: Argues that AI-driven risk assessment boosts accuracy and inclusion in insurance, and that regulatory barriers would harm customers and innovation.

Introducing barriers to the adoption of AI in the risk assessment and pricing of insurance policies would thus result in worse customer outcomes.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Warns that overlapping AI and data rules risk creating unintended barriers for open-source and early-stage innovation.

The combined application of the AI Act, GDPR and ePrivacy Directive risks creating unintended barriers for open-source development and early-stage innovation.

GSMA: Calls for regulation that balances fundamental rights with the need to enable innovation and competitiveness.

We also see the need and added value of effective regulation that strikes the right balance between safeguarding individuals' fundamental rights and enabling innovation and competitiveness.

Siinda: Urges aligning AI policy with competition and data rules to keep the EU globally competitive without overburdening innovators.

Align Al policy with competition and data rules so the EU remains a global leader without unduly constraining innovators.

Leading Baltic tech and other businesses and professional associations listed in the submission: Contends that Europe's cautious, complex AI and data rules constrain innovation and competitiveness, urging simplification and adjustment to the AI Act to prevent lagging behind.

We are concerned that the Al Act's broad scope and prescriptive compliance regime, if implemented without adjustment, could hamper Europe's Al ecosystem and leave us lagging behind more nimble competitors (be it U.S. tech giants or state-backed efforts in Asia).

Sheridans, on behalf of Awin AG: Proposes easing consent requirements to incentivize investment in CPA-based products, linking lighter data constraints to greater innovation.

Exemption or exclusion from the consent requirement of ePD regulation 5(3) would give greater incentive to invest in product development in consumer content and services that may be monetised by CPA, as the revenue return on this investment would be higher.

European Tech Alliance: Advocates simplifying the complex digital framework to restore legal certainty, rebuild trust, and unlock data- and AI-led innovation and competitiveness.

The current outdated framework hinders innovation and competitiveness for European companies.

The International Center for Law & Economics: Warns that a rushed AI Act and its implementation could hamper EU AI adoption and overlook AI's contribution to economic welfare.

The rush to regulate artificial intelligence in the EU-combined with last-minute changes to the legislative proposals made in response to ChatGPT's emerging market success-resulted in legislation (the AI Act) that may significantly hamper the EU's adoption of these pivotal technologies.

Meta Platforms Ireland Limited: Argues that complex, technically unrealistic AIA/GPAIM requirements chill innovation, deter entrants and investment, and risk turning regulation into a structural competitive disadvantage.

By embedding technically unrealisable requirements into binding law, the EU has risked converting its flagship AI regulation from a competitive advantage into a structural disadvantage - an innovation ceiling disguised as a safety floor.

Finnish Food and Drink Industries´ Federation (ETL): Calls for clarifications to the AI Act so European companies can effectively adopt and benefit from AI.

The AI Act should be clarified to ensure that European companies can benefit from AI.

AI & Partners B.V.: Recommends pairing strong AI rules with pragmatic uptake tools to reduce administrative burden and spread trustworthy AI, strengthening competitiveness.

That strengthens competitiveness by reducing administrative burden and enabling diffusion of trustworthy AIwithout undermining its role.

ENSHPO - The European Network of Safety and Health Professional Organizations: Highlights AI's potential to improve physical safety monitoring while noting that data rules can create adoption barriers, urging more enabling governance.

Bayerische Motoren Werke Aktiengesellschaft: Cautions that overly burdensome regulation could hinder industrial AI use, calling for proportionate, innovation-friendly rules.

Japan Business Council in Europe (JBCE): Urges that AI Act implementation avoid stifling medical innovation, keeping pathways open for safe, life-improving AI.

Intesa Sanpaolo: Supports incorporating AI into credit processes under clear, workable governance to improve efficiency and financial inclusion.

Ecommerce Europe: Emphasizes that data-driven personalized advertising underpins growth and innovation, advocating governance that preserves this capability.

kaiko.ai: Suggests prioritizing investment and capacity-building before heavy regulation in healthcare AI to accelerate beneficial innovation.

AFME: Calls for proportionate, harmonized rules to support AI uptake in finance while managing risks to competitiveness.

Bocconi University: Argues that well-designed data governance can protect rights and enhance efficiency, reinforcing innovation rather than opposing it.

CLOUD INFRASTRUCTURE SERVICES PROVIDERS IN EUROPE: Positions practical compliance as a trust and competitiveness lever, seeking workable obligations that do not stifle cloud innovation.

Siemens Healthineers AG: Warns that AI Act burdens could slow life-saving medical innovation, urging proportionate, feasible requirements for health AI.

European Publishers Council: Asserts that current rules can stifle privacy-preserving innovation in advertising, undermining sustainable media and digital services.

SAP SE: Notes that Data Act complexity risks heavy compliance burdens that slow data-driven innovation, calling for simplification.

Skyscanner: Highlights that effective tracking and measurement enable free, innovative services, urging balanced consent and privacy rules.

Alliance Digitale: Warns that restrictive consent and data rules deter privacy-enhancing ad-tech innovation, advocating realistic frameworks.

OpenMined: Promotes privacy-preserving technologies to enable data use and innovation consistent with EU values, calling for enabling governance.

DIGITALEUROPE: Urges preserving open-source exemptions and freedoms in AI regulation to sustain ecosystem-wide innovation.

Verband Österreichischer Zeitungen (VÖZ): Calls to enable data-driven advertising that sustains media and innovation while respecting privacy.

Wolt: Supports governance that builds trust in AI and strengthens European competitiveness for digital platforms and services.

ECIS, European Committee for Interoperable Systems: Endorses open-source compliance tooling to reduce burdens and foster interoperable, innovative systems.

Schaeffler AG: Warns that rigid oversight requirements can hinder automation efficiency and industrial AI innovation, seeking proportionate rules.

1.4.9 Experimentation & Sandboxes

This category explains how regulatory sandboxes and test-and-trial facilities turn experimentation into a systematic, low-risk engine for competitiveness and innovation. Stakeholders advocate pre- and post-regulatory sandboxes, often integrated with European Digital Innovation Hubs, to generate real-world evidence, accelerate bidirectional learning between regulators and innovators, and provide legally secure environments with reduced initial compliance burdens. Access should extend to SMEs, startups, scaleups, and sole traders, with automation to scale testing, and expansion toward pan-European and transnational AI sandboxes and TEFs targeting key verticals (e.g., automotive, manufacturing, energy, telecoms, agriculture, aerospace, defence). Responsible experimentation and transparency are emphasized to build trust. A second theme links experimentation to deployment: sandbox outputs should be recognized and weighted in assessments, with presumptions of conformity, incentives for participation, and better valuation of documentation, alongside explicit R&D and low-risk processing carve-outs up to market entry. Policymakers are urged to integrate proven models into the rulebook, enable fast-track and mutually recognized licensing that reuses sandbox evidence to cut time and cost without weakening oversight, and adopt a learning-first, light-touch approach that lowers compliance friction—moving toward a once-only vision where interoperability and data sharing reduce administrative burden while innovation scales.

Second, experimentation with sandboxes or controlled regulatory trials allows companies-especially SMEs, startups, and scaleups-to test innovative models under limited supervision. (Adigital (Asociación Española de la Economía Digital))

Pre- and post-regulatory sandboxes, integrated into the existing European Digital Innovation Hubs (EDIHs), would help to produce real-world data for public authorities, drive regulatory learning on both sides, and foster experimen- tation in a legally secure environmen ()

Mutual recognition of results would allow part of the licensing file (e.g., technical tests, business model validation) to be replaced by the evidence generated in the sandbox, reducing timelines and costs without sacrificing rigorous supervision. (Adigital (Asociación Española de la Economía Digital))

The solution is not more regulation but faster learning from what already works. ()

: Proposes pre- and post-regulatory sandboxes integrated with EDIHs to gather real-world evidence, accelerate regulatory learning, and enable legally secure experimentation, enhanced with automation tools.

Pre- and post-regulatory sandboxes, integrated into the existing European Digital Innovation Hubs (EDIHs), would help to produce real-world data for public authorities, drive regulatory learning on both sides, and foster experimen- tation in a legally secure environmen

Siinda: Calls for enabling sole traders to access regulatory sandboxes to test interoperability and data-sharing with reduced initial compliance and rapid feedback.

Ensure sole traders can use regulatory sandboxes to test interoperable features or data-sharing models with lowered initial compliance burdens and fast feedback.

Adigital (Asociación Española de la Economía Digital): Advocates sandbox-based experimentation for SMEs and startups to trial innovative models under limited supervision. Urges integrating successful models into regulation and creating fast-track, mutually recognized licensing based on sandbox evidence.

Second, experimentation with sandboxes or controlled regulatory trials allows companies-especially SMEs, startups, and scaleups-to test innovative models under limited supervision.

WKÖ - Austrian Federal Economic Chamber: Urges using and expanding AI sandboxes and TEFs to help companies meet AI Act requirements through practical, sector-focused testing across key industries.

In addition to the existing national regulatory AI sandboxes, we advocate the creation of additional European and transnational regulatory sandboxes and more targeted European test and trial facilities (TEFs) with a particular focus on vertical AI applications in key industries such as the automotive industry, advanced manufacturing, energy, telecommunications networks, agriculture, aerospace and defence, etc ..

: Promotes a learning-first approach that reduces compliance burdens and accelerates innovation via a practical lab within the EU's digital agenda rather than adding regulation.

The solution is not more regulation but faster learning from what already works.

U.S. Chamber of Commerce: Calls for an explicit R&D exemption to protect experimentation from premature compliance burdens and enable innovation.

Ministry of Industry and Trade of the Czech Republic - this entry represents the official position of the Czech Republic for the section "Targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules: Seeks clear, aligned R&D exemptions until market placement and recognition of sandbox outputs in regulatory assessments.

Ireland - Department of Enterprise, Tourism and Employment: Supports EU-level sandboxes to advance trustworthy innovation and enable controlled testing across the Union.

Independent Retail Europe: Suggests that successful sandbox participation should carry a presumption of conformity to ease subsequent compliance and market entry.

Business Software Alliance: Advocates scaling up regulatory sandbox programs to broaden access and impact for innovators.

Eurochambres: Backs the support and expansion of sandbox initiatives to foster experimentation and competitiveness.

Global Data Alliance: Encourages the expansion of regulatory sandbox programs to facilitate cross-border testing and innovation.

INVERCO: Supports pan-European AI sandboxes to enable responsible innovation and smoother certification pathways.

Danish Industry: Recommends allowing low-risk R&D data processing to enable experimentation without onerous compliance.

DIGITALEUROPE: Urges presumption of conformity and incentives for sandbox participants, and better regulatory recognition of sandbox documentation.

Wolt: Endorses responsible experimentation with strong transparency, potentially via sandbox frameworks.

Mistral AI: Argues that sandboxes can support targeted deregulation by safely testing and validating approaches before scaling.

The European Network of Expertise on Omics: Supports sandboxes and streamlined certification to accelerate safe adoption of innovative technologies.

1.4.10 Miscellaneous

This Miscellaneous category under Competitiveness & Innovation Enablement aggregates cross-sector insights showing how reduced friction, smarter personalization/targeting, and data-driven technologies translate into better user outcomes and business performance. Low-friction onboarding accelerates adoption; improved ad

targeting strengthens ROI; telematics insurance delivers consumer benefits; and AI-enabled technologies, including diagnostic support, enhance healthcare outcomes as AI uptake grows across the ecosystem. These patterns point to practical levers—user-centric design, personalization, and trustworthy AI—that bolster competitiveness while raising acceptance and value for consumers and industry. A complementary theme is streamlining market mechanisms and governance to unlock efficiency and growth. Deprecating probabilistic compensation schemes in affiliate marketing would remove cost and complexity, while at the macro level the EU's difficulty in delivering reforms is a structural headwind to economic progress. Together, the insights advocate for execution excellence—simpler onboarding and measurement, responsible personalization, and effective policy delivery—to convert innovation into widespread economic and consumer benefit.

> *Yet they remain unaddressed - suggesting that the EU's inability to deliver reforms is itself a major headwind to economic progress.* (AI & Partners B.V.)
>
> *This would also allow probabilistic initiatives to approximate and compensate for lost publisher commissions, such as Awin's Conversion Protection Initiative, to be deprecated, therefore removing cost and complexity to affiliate marketing.* (Sheridans, on behalf of Awin AG)

Sheridans, on behalf of Awin AG: Deprecating probabilistic compensation schemes would reduce cost and complexity in affiliate marketing, improving efficiency and competitiveness.

> *This would also allow probabilistic initiatives to approximate and compensate for lost publisher commissions, such as Awin's Conversion Protection Initiative, to be deprecated, therefore removing cost and complexity to affiliate marketing.*

AI & Partners B.V.: Persistent failure to deliver EU reforms is a major headwind to economic progress, stifling competitiveness and innovation.

> *Yet they remain unaddressed - suggesting that the EU's inability to deliver reforms is itself a major headwind to economic progress.*

iProov Ltd: Low-friction onboarding speeds user adoption of new services, enabling wider innovative deployment and market uptake.

: Improved ad targeting helps businesses operate more efficiently and effectively, strengthening competitiveness.

Business & Science Poland: Policies and tools that deliver tangible benefits to users and industry reinforce innovation ecosystems and overall competitiveness.

Insurance Europe: Telematics-based insurance offers consumer benefits through tailored pricing and safer driving incentives, stimulating sector innovation.

Siemens Healthineers AG: AI-enabled technologies in healthcare improve clinical outcomes and operational efficiency, advancing innovation capacity.

Euroconsumers: Personalization yields user benefits and strong acceptance, enhancing competitive differentiation and innovation.

BioMed Alliance: AI is increasingly adopted across healthcare, providing diagnostic support and patient benefits that enhance performance and innovation.

1.5 Data Access, Interoperability & Cross-Border Transfers

Europe's data economy will scale only with a coherent, risk-based, interoperability-first framework that links trusted cross-border transfers to practical access safeguards and digital identity. Legal certainty grounded in GDPR mechanisms (e.g., adequacy and standard clauses) should avoid localization, preserve free flows of non-personal data, and resolve overlaps and extraterritorial conflicts. Open standards, secure APIs, machine-readable reporting, and common data spaces cut burdens and enable reuse, while governance avoids pitfalls like elevating robots.txt and harmonizes definitions and formats. Cloud portability should be realistic—narrower scope, clearer rights, flexible switching, and reasonable exit assistance—mindful of early-termination impacts. Public data reuse must expand with quality and licensing clarity, while B2G access remains exceptional, targeted, and fairly compensated. Proportionate, purpose-bound access safeguards privacy, IP, and

trade secrets, with exclusions for inferred/derived data and GDPR-aligned safe-access tools for SMEs. Regulatory alignment across the EU's data instruments, model clauses, and harmonized national practice reduces friction and clarifies lawful bases. Competition tools should curb gatekeeper power, enable voluntary sharing, avoid rules that facilitate collusion, and apply interoperability mandates judiciously. Sectoral calibration (energy, mobility, health, media, insurance, due diligence) relies on neutral platforms, proportionate safeguards, fair compensation, and clear territorial scope. A trusted identity layer (eIDAS 2, EUDI Wallets) using open APIs automates authorizations and reduces lock-in. AI and research need streamlined, cross-border access to high-quality, interoperable datasets with predictable legal bases and standardized exchange. Pragmatic, consent-based ecosystems and shorter supply chains already demonstrate accountability and value with constrained data. Across domains, stakeholders converge on harmonization, open standards, and trusted identity to unlock cross-border data flows while preserving confidentiality and security. The trend is risk-based governance with proportionate safeguards, sector-specific precision, and market-compatible incentives that sustain high-quality data supply and competition.

1.5.1 Regulatory Alignment & Streamlining

Stakeholders call for regulatory alignment and streamlining across the EU's data framework to enable interoperable, trusted data sharing and cross-border transfers. They urge consolidation of overlapping and inconsistent obligations (Data Act, GDPR, AI Act, DGA, PSD2, Free Flow of Non-Personal Data, FiDA), clearer scopes and definitions (e.g., connected products, data processing services), and tools such as model clauses to reduce legal uncertainty and administrative burden. Distinguishing between B2B and B2C contexts and ensuring sectoral coordination are seen as essential to reflect industrial data realities and avoid duplicative regimes. Calls also target practical barriers: harmonising national interpretations to facilitate cross-border access (including sensitive domains like health), clarifying rights and lawful bases for data use and re-use, and simplifying access frameworks for specific datasets (e.g., sole trader data). Aligning transparency and data protection requirements across instruments, while easing unnecessary restrictions on data re-use and transfers, is framed as key to unlocking data-driven innovation without compromising digital trust.

> *By streamlining data-related obligations and fostering an environment that enables trusted data flows, the Digital Omnibus can help unlock new opportunities for businesses and consumers, while maintaining Europe's leadership in digital trust and data protection.* (Docusign)
>
> *Consolidating overlapping data rules and easing unnecessary burdens (particularly on re-use of data and transfers) would make the European data economy more effective.* (LSEG)
>
> *Repeal the Data Act or at least exempt B2B cases from the Data Act,* (SIEMENS AG)
>
> *FiDA risks creating parallel financial-sector data-sharing schemes that duplicate or conflict with the DGA's model of neutral intermediaries.* (European Associations of Co-operative Banks (EACB))
>
> **SIEMENS AG:** Calls for repealing or exempting B2B cases from the Data Act to reduce legal uncertainty and burdens. Seeks differentiated, streamlined rules for industrial data access and sharing.
>
> *Repeal the Data Act or at least exempt B2B cases from the Data Act,*
>
> **ZVEI e.V.:** Warns that a uniform approach to B2B and B2C in the Data Act creates legal and technical uncertainties. Advocates differentiated regulation and clearer, practicable data-sharing rules.
>
> *However, the current approach, characterizing a uniform regulation for both B2B and B2C contexts within chapters II and III, alongside a highly simplified and impractical understanding of industrial data sharing, raises significant legal and technical uncertainties.*
>
> **Enel SpA:** Supports simplifying the Data Act and coordinating it with sectoral legislation. Aims to avoid overlaps and ensure coherent obligations across domains.
>
> *Enel supports Data Acts simplification and coordination with sectoral laws.*
>
> **Technology Industries of Finland:** Urges explicit rights for data holders to use data for diagnostics, R&D, quality, and safety. Seeks clear, aligned rules enabling responsible reuse.
>
> *Art. 4: Grant data holders the right to use the data, at a minimum, for purposes including diagnostics, research and development, quality control, and safety.*
>
> **Docusign:** Advocates streamlining data-related obligations to enable trusted data flows. Supports a coherent approach to reduce compliance friction while preserving trust.

By streamlining data-related obligations and fostering an environment that enables trusted data flows, the Digital Omnibus can help unlock new opportunities for businesses and consumers, while maintaining Europe's leadership in digital trust and data protection.

Volkswagen Group: Calls for the AI Act to be consistent with GDPR on transparency and data protection. Seeks alignment to prevent conflicting requirements.

The AI Act should ensure that its transparency and data protection requirements are consistent with the General Data Protection Regulation (GDPR).

Dun & Bradstreet: Requests clarification and simplification of rules for accessing sole trader data. Aims to remove fragmentation and legal uncertainty.

We therefore urge the European Commission and Member States to clarify and simplify the legal framework governing access to sole trader data.

German Insurance Association: Highlights that divergent national interpretations hinder cross-border collaboration and access to health data. Calls for harmonized, clear EU-level rules.

Diverging national interpretations also hinder cross-border collaboration, especially for German reinsurers who need access to health data from other countries without direct contact with the data subject.

Telefonica, S.A.: Urges clarification of the Data Act's scope, especially for connected products. Seeks predictable, streamlined obligations for device data.

Telefónica urges clarification of the Data Acts scope, especially regarding the Connected Products.

German Social Insurance European Representation: Emphasizes the need for reliable, legally secure data access in social security to ensure continuity of care. Calls for clear, interoperable frameworks.

For social security, reliable and legally secure access to data is central to ensure continuity of care.

LSEG: Advocates consolidating overlapping data rules and easing burdens on reuse and transfers. Seeks a more effective European data economy through alignment.

Consolidating overlapping data rules and easing unnecessary burdens (particularly on re-use of data and transfers) would make the European data economy more effective.

AIM - European Brands Association: Supports targeted simplification of the EU data acquis across multiple instruments. Aims to improve interoperability and reduce duplication.

We support the targeted simplification of the EU's data acquis, including the Data Governance Act, the Free Flow of Non-Personal Data Regulation, and the Open Data Directive.

Adigital (Asociación Española de la Economía Digital): Calls to reassess FiDA's scope to avoid duplication and unintended burdens. Seeks alignment with existing open data and data-sharing frameworks.

In the context of FIDA (open finance regulation), the scope of the proposal should be reconsidered.

Vodafone Group: Notes EU efforts to prohibit unjustified data localisation and remove barriers to sharing and reuse. Encourages continued coherence across the data rulebook.

his began with the Free Flow of Data Regulation, which prohibits unjustified data localisation mandates, and continued with measures to remove commercial, legal, and technical barriers to data sharing and reuse via the EU Data Act.

ING Group: Points to PSD2 obligations enabling data access for AISPs. Calls for consistent, interoperable data-sharing rules across financial regulations.

PSD2 and its technical standards oblige banks to provide AISPs with all data that is provided to the client.

European AI Forum: Warns that the Data Act overlaps with GDPR and the AI Act. Urges clarification and alignment to avoid duplicative obligations.

The Data Act aims to enable data sharing and interoperability but often overlaps with GDPR and AI Act obligations.

: Observes that legal and procedural barriers keep public data siloed, impeding sustainability and competitiveness. Calls for streamlining access and re-use.

Europes sustainability and competitiveness goals are being held back not by technology, but by legal and procedural barriers that keep public data locked in silos.

European Associations of Co-operative Banks (EACB): Cautions that FiDA could create parallel data-sharing schemes conflicting with the DGA's neutral intermediary model. Seeks coherence across financial and general data frameworks.

FiDA risks creating parallel financial-sector data-sharing schemes that duplicate or conflict with the DGA's model of neutral intermediaries.

ACEA (European Automobile Manufacturers' Association): Flags unclear definitions and requirements for data processing services under Article 32. Requests clearer, harmonized obligations to reduce complexity.

This complexity is reinforced by the lack of a clear definition of "data processing services" and the lack of clarity as to the requirements that such an entity is expected to fulfil pursuant to Article 32.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Argues for enabling a legal basis for access to and sharing of personal data within the Data Act. Seeks alignment with other laws to facilitate responsible data use.

Consequently, the statement in Recital 7 of the Data Act asserting that the regulation does not create a legal basis for access to personal data or its sharing with third parties should be removed.

American Chamber of Commerce to the EU: Advocates regulatory alignment and simplification to support data access and cross-border transfers. Seeks predictable, streamlined obligations for business.

Halle Institute of Economic research (IWH): Supports clearer, coordinated data rules to reduce uncertainty. Emphasizes streamlining for effective cross-border research and collaboration.

Business & Science Poland: Calls for coherent, simplified data regulations to enable cross-border innovation. Seeks removal of duplicative requirements.

DigitalTrade4.EU: Advocates for interoperable, aligned data frameworks that facilitate cross-border trade. Supports streamlining compliance burdens.

Bayerische Motoren Werke Aktiengesellschaft: Calls for consistency between the Data Act, GDPR, and AI Act for connected vehicles and services. Seeks clear, harmonized obligations across the EU.

EHIMA: Seeks harmonized data access rules for hearing technologies, balancing interoperability with privacy. Calls for streamlined, clear compliance pathways.

VDMA - Advancing Europe´s machinery industry: Advocates streamlined industrial data-sharing rules for machinery and IIoT. Seeks aligned definitions and obligations to enable secure interoperability.

Japan Business Council in Europe (JBCE): Calls for clear, consistent EU data rules to facilitate cross-border transfers and avoid localisation. Seeks predictable frameworks for international businesses.

European Banking Federation: Seeks alignment of FiDA, PSD2, and GDPR to enable secure, interoperable data sharing in finance. Calls for simplification to reduce overlap.

Healthtech Finland: Calls for harmonized health data frameworks enabling cross-border care and innovation. Seeks clarity on access, reuse, and interoperability.

Federation of Austrian Industries: Advocates simplifying and aligning EU data regulations to boost competitiveness. Calls for legal certainty and reduced administrative burden.

U.S. Chamber of Commerce: Urges predictable, coherent data-transfer rules to support transatlantic flows. Calls for avoiding localisation and unnecessary barriers.

Confederation of Industry of the Czech Republic: Supports aligned, streamlined data regulations to facilitate cross-border industrial operations. Seeks clarity and reduced compliance complexity.

ITI - Information Technology Industry Council: Calls for interoperable, consistent data-sharing rules across EU laws. Seeks simplification to avoid overlapping obligations for tech providers.

ENTSO-E: Seeks harmonized data access and interoperability standards to support cross-border energy operations. Calls for clear, streamlined data-governance rules.

Verband der Automobilindustrie e.V.: Calls for clear, consistent frameworks for in-vehicle data sharing across borders. Seeks alignment with privacy and safety requirements.

Association des Constructeurs Européens de Motocycles: Advocates clarity on connected motorcycle data access and sharing. Seeks alignment with GDPR and sectoral safety rules.

CECIMO - European Association of Manufacturing Technologies: Supports streamlined rules for industrial data sharing in manufacturing technologies. Calls for aligned obligations and practical interoperability.

Plateforme de la filière Automobile: Calls for harmonized data frameworks for the automotive ecosystem. Seeks simplified, predictable rules across EU markets.

Movement for an Open Web: Advocates removing barriers to data portability and interoperability through aligned regulation. Calls for clear, enforceable rules that promote open competition.

EFCA - European Federation of Engineering Consultancy Associations: Seeks simplified, consistent cross-border data-sharing rules for engineering projects. Calls for clear contractual and regulatory guidance.

Delivery Platforms Europe: Calls for harmonized data obligations enabling platform interoperability while protecting privacy. Seeks streamlined compliance for cross-border operations.

Orgalim - Europe's Technology Industries: Advocates consistent, streamlined data regulations to empower industrial data spaces and innovation. Calls for clarity and alignment across EU acts.

Connect Europe: Calls for coherent, simplified data-transfer rules to enhance connectivity and interoperability. Seeks reduced fragmentation across EU policies.

Bayer AG: Seeks harmonized health and research data rules to enable cross-border studies. Calls for clear, streamlined access and reuse conditions.

: Questions whether rules are sufficiently clear and proposes model clauses to aid compliance. Seeks streamlined cross-border data-sharing through standardized templates.

are rules clear enough or should model clauses be introduced?

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: Advocates clear, aligned data rules to facilitate cross-border wholesale and services. Calls for reduced administrative burden.

Charter of Trust: Calls for alignment between security and data regulations to enable trusted, interoperable data flows. Seeks clarity without undermining resilience.

Danish Entrepreneurs: Seeks simpler, clearer data rules for entrepreneurs and SMEs to expand across borders. Calls for predictable compliance frameworks.

Global Data Alliance: Advocates the free flow of data and regulatory alignment to avoid localisation mandates. Calls for streamlined, interoperable rules internationally.

Clever Cloud: Calls for consistent requirements for data processing services across EU member states. Seeks clearer definitions and obligations.

Siemens Healthineers AG: Advocates aligned frameworks for health data access and transfers consistent with GDPR. Seeks clarity to support medical innovation.

Dassault Systèmes: Supports interoperability and aligned data obligations enabling industrial collaboration. Calls for clear, practical rules across sectors.

Hugging Face: Calls for coherence between AI, data, and privacy laws to support responsible dataset access and transfers. Seeks streamlined obligations for developers.

European Savings and Retail Banking Group: Seeks alignment of financial data-sharing rules with GDPR to streamline access for consumers and third parties. Calls for reducing duplication.

SAP SE: Advocates simplifying and aligning EU data regulations, with clear definitions and interoperable standards. Seeks predictability for enterprise users.

Alliance Digitale: Calls for clear, harmonized cross-border data rules for digital advertising. Seeks streamlined compliance consistent with GDPR.

Dedalus S.p.A.: Advocates streamlined health data governance enabling cross-border care and analytics. Seeks clarity on access and interoperability.

DIGITALEUROPE: Calls for simplifying the EU data acquis and improving interoperability across sectors. Seeks alignment to reduce burdens.

Enedis: Seeks aligned data-access rules for energy distribution to support operational interoperability. Calls for clear, practical obligations.

WindEurope: Advocates harmonized cross-border data sharing to optimize wind energy operations. Calls for streamlined, interoperable frameworks.

APPLiA (Home Appliance Europe): Calls for clarity on data access for connected home appliances and alignment across laws. Seeks simplified, consistent obligations.

DER MITTELSTANDSVERBUND - ZGV e.V.: Seeks simplified, aligned data rules for SMEs and retail groups to enable cross-border activity. Calls for reducing legal complexity.

1.5.2 Cross-Border Transfers & Adequacy

Cross-Border Transfers & Adequacy focuses on enabling secure, reliable movement of data across borders as a foundation for Europe's digital economy, AI innovation, and seamless telecom services. Stakeholders call for legal certainty grounded in GDPR Chapter V mechanisms—especially adequacy decisions and standard contractual clauses—while urging the Commission to expand adequacy assessments for third countries and major cloud providers. They emphasize avoiding data localization and excessive national autonomy requirements, and preserving the free flow of non-personal data to support competitiveness and digital trade. At the same time, contributors highlight friction points that undermine transfers: strict supervisory interpretations that dismiss risk-based approaches, overlapping or inconsistent regimes (e.g., Data Governance Act, Data Act Article 32) that go beyond GDPR, and extraterritorial laws that risk service disruption and data leakage. Concerns also include non-reciprocity from unilateral EU data market opening and the need to strengthen protections for commercially sensitive data. The overarching ask is a coherent, risk-based, and trade-aligned framework that maintains high protections while unlocking cross-border data flows.

To reduce burdens on individual companies, the European Commission could conduct assessments and make more adequacy decisions regarding data transfers with third countries (evaluating third-country legal systems and practices) and data transfers involving significant players (e.g., Microsoft, Amazon, Google). (Technology Industries of Finland)

Docusign recognises that the ability to move data securely and efficiently across borders is fundamental to the success of Europe's digital economy. (Docusign)

Caused by more flexible and vendor-friendly data sharing schemes in other economic regions, the unilateral opening of data markets in the EU will lead to non-reciprocity in international business partnerships, i.e. the user can request data free of charge and compensation for data transfer to third parties is limited by guidelines. (SIEMENS AG)

Repeal Article 32 of the Data Act on the transfer of data to third countries; relevant GDPR provisions should exclusively apply to international data transfers (ACEA (European Automobile Manufacturers' Association))

: Proposes expanding EU free trade agreements to allied countries and embedding strong digital trade chapters to facilitate predictable cross-border data flows.

a new strategic "Free Trade Initiative" should aim to expand the EU's Free Trade Agreements to cover all Member States from the Council of Europe, NATO, and OECD, while ensuring that digital trade chapters are included in each of those deals.

SIEMENS AG: Warns that the EU's unilateral data market opening versus more vendor-friendly regimes elsewhere creates non-reciprocity in international data sharing, undermining fair cross-border cooperation.

Caused by more flexible and vendor-friendly data sharing schemes in other economic regions, the unilateral opening of data markets in the EU will lead to non-reciprocity in international business partnerships, i.e. the user can request data free of charge and compensation for data transfer to third parties is limited by guidelines.

Enel SpA: Calls to bolster protections for commercially sensitive data in cross-border contexts to prevent undue exposure.

Strengthen protections for commercially sensitive data.

Technology Industries of Finland: Urges the Commission to increase adequacy decisions for third countries and major cloud providers to reduce company-level transfer burdens.

To reduce burdens on individual companies, the European Commission could conduct assessments and make more adequacy decisions regarding data transfers with third countries (evaluating third-country legal systems and practices) and data transfers involving significant players (e.g., Microsoft, Amazon, Google).

Workday: Flags that the Data Governance Act imposes transfer rules beyond GDPR, creating inconsistencies that complicate international data flows; seeks alignment with GDPR.

The Data Governance Act introduces inconsistent requirements for data transfers that go above and beyond the GDPR's established framework for personal data transfers.

Docusign: Stresses that secure, efficient cross-border data movement is foundational to Europe's digital economy and requires supportive policy.

Docusign recognises that the ability to move data securely and efficiently across borders is fundamental to the success of Europe's digital economy.

France Digitale: Emphasizes that unhindered data circulation is essential for AI and tech development, implying the need for enabling cross-border frameworks.

The circulation of data is crucial for AI and technological development in Europe.

German Insurance Association: Criticizes supervisory authorities' strict reading of GDPR Chapter V and rejects abandoning a risk-based approach for international transfers.

Supervisory authorities interpret Chapter V of the GDPR strictly, rejecting a risk- based approach.

Video Games Europe: Asks for full legal certainty for extra-EU transfers, especially when relying on standard contractual clauses.

For data transfers outside the EU, full legal certainty is required, in particular where these depend on standard contractual clauses

Government Office of the Czech Republic: Supports free flow of non-personal data within and beyond the EU to spur innovation, product availability, and competitiveness.

Generally speaking, CZ considers it important to maintain the free flow of non-personal data both within and outside the EU, as this supports an innovative environment, broadens the range of products available to EU businesses, and strengthens their competitiveness.

Airbus: Seeks safeguards against extraterritorial laws that could disrupt services or cause data leakage, particularly for sensitive and strategic sectors.

Safeguard against extraterritorial laws and influences that could disrupt services :unselected: or lead to undue data leakage, particularly for sensitive data and strategic sectors.

Leading Baltic tech and other businesses and professional associations listed in the submission: Argues the EU's international transfer framework is overly complex and outdated, calling for modernization to match global tech realities.

Problem: The EU's framework for international data transfers is complex, outdated, and misaligned with the global technology landscape.

Ibec: Promotes policies that encourage data flows to boost digital trade across borders.

Encourage data flows, encourage digital trade.

Meta Platforms Ireland Limited: Maintains that cross-border data flows are vital for innovation but have been hindered by legal uncertainty and impractical DPA decisions; calls for clarity and consistency.

Moreover, the free flow of data across borders is essential for innovation, competitiveness, and the development of new technologies, yet legal uncertainties in recent years - stemming from national data protection authority ("DPA") decisions that challenge the GDPR's risk-based approach, ignore its derogations, and introduce impractical requirements - have complicated cross-border transfers.

Finnish Food and Drink Industries´ Federation (ETL): Recommends reconsidering obligations to share device data outside the EEA under the Data Act in light of heightened security risks.

The obligation to share device data outside the EEA under the Data Act should be reconsidered due to the changed security landscape.

Vodafone Group: Advocates accelerating cross-border telecom service deployment to provide seamless services irrespective of national borders.

Accelerate cross-border service deployment, ensuring that consumers and businesses enjoy seamless, high-quality telecommunications services regardless of national boundaries.

ING Group: Supports reliance on GDPR-level protections and opposes additional national data localization rules that fragment cross-border operations.

In order to support the single market, ING suggests to rely on protection frameworks in place at EU level, such as GDPR, and requests member states to refrain from imposing domestic localisation requirements on top.

FiCom ry: Encourages limiting national autonomy requirements that impair cross-border cooperation and data flows.

The Commission should encourage Member States to avoid excessive national autonomy requirements that hinder cross-border cooperation in the name of security.

ACEA (European Automobile Manufacturers' Association): Proposes repealing the Data Act's third-country transfer article and relying exclusively on GDPR for international transfers.

Repeal Article 32 of the Data Act on the transfer of data to third countries; relevant GDPR provisions should exclusively apply to international data transfers

1.5.3 Interoperability, Standards & Data Spaces

This category emphasizes interoperability, open standards, and data spaces as the backbone for scalable data access and cross-border coordination. Stakeholders call for digital-by-default compliance, standardized data formats, secure APIs, machine-readable reporting, and harmonized definitions, taxonomies, and thresholds to cut administrative burden, improve legal certainty, and spur innovation. Leveraging international standards (e.g., ISO 27001) with proportionate enforcement is highlighted as a pragmatic way to scale compliance without discouraging security improvements. Common European (sectoral) data spaces are framed as the key operational vehicle for trusted sharing and reuse, eliminating duplicate reporting and manual processing, automating compliance, and freeing capacity for better services. Proposals include national interoperability nodes for ESG data linked to EU data spaces, a central education data catalog under the DGA, and unifying duplicative publication formats (e.g., INSPIRE and DCAT). At the same time, contributors flag gaps and risks—such as the lack of harmonized methodologies for exchanging dynamic data in sectors like automotive, persistent re-entry of known data due to non-interoperable systems, and governance pitfalls like attempts to give robots.txt quasi-legal force—arguing instead for transparent, standards-based models that preserve openness while embedding accountability.

The adoption of open standards and comprehensive interoperability protocols will be critical mechanisms to support general compliance with the Data Act's provisions and to unlock the Data Act's tangible benefits to the EU Single Market. (GSMA)

Sectorial data spaces allow authorities and businesses to share information through common standards, eliminating duplicate reporting and manual processing. (Government Office of the Czech Republic)

Courts, regulators, and market actors may treat it as precedent, reading robots.txt as a legally enforceable signal of consent or prohibition-contrary to its original specification, which expressly disclaims legal effect. (Alliance for Responsible Data Collection)

There are currently no harmonised methodologies to measure, verify, or exchange most dynamic parameters. (ACEA (European Automobile Manufacturers' Association))

Kaspersky Labs Limited: Urges the Commission to prioritize interoperability and digital-by-default compliance, using standardized data formats, secure APIs, and machine-readable interfaces. The aim is to reduce administrative burdens and catalyze innovation.

The use of standardized data formats, secure APIs, and machine-readable reporting interfaces would reduce administrative burdens and foster innovation.

European Energy Information Sharing and Analysis Centre: Calls for harmonized definitions, taxonomies, and thresholds to enable interoperable cross-border coordination in the energy sector. Such alignment would improve information exchange and coordinated incident response.

Harmonised definitions, taxonomies, and reporting thresholds are necessary to enable meaningful cross-border information exchange and coordinated response.

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Expresses industry support to collaborate on building a secure, interoperable, and innovative European Data Union. Emphasis is on aligning standards to unlock data-driven healthcare and IT integration.

COCIR remains committed to supporting the Commission in these efforts and looks forward to collaborating to ensure a secure, interoperable, and innovative European Data Union.

GSMA: Advocates adoption of open standards and comprehensive interoperability protocols to realize the Data Act’s benefits and ensure compliance. Also supports reliance on international standards and proportionate penalties.

The adoption of open standards and comprehensive interoperability protocols will be critical mechanisms to support general compliance with the Data Act's provisions and to unlock the Data Act's tangible benefits to the EU Single Market.

Government Office of the Czech Republic: Recommends leveraging Common European Data Spaces and sectoral data spaces to standardize sharing, automate compliance, and cut duplicate reporting. Also proposes a central catalogue of educational data governed under the Data Governance Act.

In the context of reducing business compliance costs related to data access, re- use and sharing, and by limiting the fragmentation of rules and their application, the Commission should clearly explore and make use of the concept of Common European Data Spaces (announced in the European Data Strategy).

Telefonica, S.A.: Asks to reduce regulatory hurdles and simplify cross-border deployments to foster an innovative industrial data-sharing ecosystem. Emphasizes open standards and interoperability protocols to support Data Act compliance.

Further action is needed to reduce unnecessary regulatory hurdles and legal complexities, including through simplification of cross-border deployments, paving the way for a far more innovative and navigable industrial data sharing ecosystem.

Alliance for Responsible Data Collection: Warns against elevating robots.txt into a quasi-legal gatekeeper and urges a transparent, standards-based model to preserve interoperability and openness online. Highlights governance and ownership mismatches that such elevation would create.

To preserve an open, competitive, and innovation-friendly internet, policymakers should reject the elevation of robots.txt into a quasi-legal instrument and instead adopt the ARDC's transparent, standards-based model.

: Calls to unify data publication formats across INSPIRE (ISO) and the National Open Data Catalogue (DCAT) to improve interoperability. Notes that duplicative format requirements create unnecessary administrative and financial costs.

The need to unify formats for publishing data for INSPIRE (ISO) and NKOD (National Open Data Catalogue) (DCAT).

Union of Entreprenuers and Employers: Prioritizes interoperability of compliance tools and joint guidance to streamline cross-regulatory obligations. Interoperable standards would enable seamless cross-border information access and coordinated market surveillance.

Interoperable technical standards would allow national authorities to access information seamlessly and coordinate market surveillance across borders.

WKÖ - Austrian Federal Economic Chamber: Seeks standardized, cross-border reporting and data-exchange frameworks to replace fragmented proprietary questionnaires. A common, secure framework would lower burdens and support innovation across locations.

A standardized and improved framework for the cross-border exchange of data between European companies must be created immediately in order to ensure the secure, trustworthy and efficient handling of data in the EU and to enable innovation across locations.

: Urges harmonized rules enabling data reuse and the creation of national interoperability nodes for ESG and environmental data. These nodes should connect to European data spaces to scale access and coordination.

Establish national interoperability nodes for ESG and environmental data connected to European data spaces (e.g., Green Deal Data Space, ESAP).

ACEA (European Automobile Manufacturers' Association): Flags the lack of harmonized standards for measuring, verifying, and exchanging dynamic vehicle data. Ongoing standardization efforts are noted but remain incomplete, hindering interoperability.

There are currently no harmonised methodologies to measure, verify, or exchange most dynamic parameters.

: Positions interoperability as the common language to make systems communicate and eliminate duplicate data re-entry. Current gaps force citizens and SMEs to re-enter data already held by administrations.

Interoperability as the common language: all projects framed around making systems talk to each other, cutting duplication at its root.

EuroGeographics: Calls to address fragmentation in geospatial data through harmonized standards and interoperable data spaces. Better alignment would enable seamless cross-border use and reduce redundancy.

DigitalTrade4.EU: Supports legislated, practical interoperability to ensure reliable cross-border data exchange. Urges accelerating Digital Product Passport adoption to standardize product data sharing across the Single Market.

Telekom Austria AG: Highlights overlap and potential conflicts between interoperability and compatibility requirements. Recommends clearer, harmonized guidance to streamline cross-border implementations.

European Signature Dialog: Advocates deregulation and simplification to achieve practical cross-border interoperability in trust services. Emphasis is on removing barriers that hinder seamless digital signatures and identity use across the EU.

CENTR - Council of European Top Level Domain Registries: Stresses maintaining a global, interoperable DNS ecosystem to avoid fragmentation. Encourages alignment with international technical standards to preserve resilience and cross-border functionality.

Ireland - Department of Enterprise, Tourism and Employment: Encourages frameworks that facilitate cross-sector, cross-border data sharing while minimizing compliance burdens. Standardized data spaces and interoperable APIs are seen as key enablers.

ITI - Information Technology Industry Council: Promotes alignment with international standards and interoperable approaches to ensure efficient data access and cross-border transfers. Emphasizes avoiding conflicting EU-specific requirements.

Salesforce, Inc.: Recommends non-binding, practical interoperability guidelines under the Data Act to drive convergence without stifling innovation. Soft-law tools can harmonize practices while allowing flexibility.

ENTSO-E: Notes that common European data spaces can reduce administrative burden and streamline reporting. Shared standards would support cross-border energy system coordination.

Association of Finnish Cities and Municipalities: Calls for a uniform, high-quality data foundation across municipalities using common standards and shared infrastructure. This would enhance interoperability and enable scalable cross-border services.

: Proposes embedding the Data Privacy Vocabulary (DPV) into data spaces to standardize semantics for consent and compliance. This would enhance interoperability across organizations and jurisdictions.

Google: Urges recognition and reuse of mature international standards to promote interoperable data flows. Such alignment limits fragmentation and eases cross-border operations.

Agilitation: Supports interoperable consent solutions that work across platforms and borders. Emphasizes privacy-preserving mechanisms that remain technically compatible across ecosystems.

secunet Security Networks AG: Advocates open-source reference implementations and interoperable reporting APIs to cut compliance costs. Standardized, machine-readable interfaces would ease cross-border supervision.

Business Software Alliance: Recommends an interoperability-first, phased regulatory approach leveraging standards and voluntary frameworks before mandates. This reduces risk while achieving scalable cross-border interoperability.

Eurochambres: Calls for standardized interoperability frameworks to help SMEs scale across borders. Harmonized data models and interfaces would lower costs and complexity.

Connect Europe: Promotes open standards and interoperability alongside proportionate penalties to encourage secure data sharing. Aligning with international standards helps ensure EU-wide scalability.

PPC: Favors voluntary, industry-led data-sharing frameworks built on interoperable standards. This approach can deliver cross-border scalability without rigid mandates.

Bayer AG: Advocates harmonized interoperability standards and machine-readable regulatory requirements to automate compliance. Clear standards would ease cross-border data reuse in regulated sectors.

: Calls for proportionate, secure emergency interoperability obligations that balance rapid data exchange with safety. Frameworks should enable cross-border coordination without introducing new risks.

Usercentrics: Supports innovation in consent management platforms with interoperable consent signals and hybrid models. Aims to ensure user-centric, cross-ecosystem compliance without locking in vendors.

Computer & Communications Industry Association (CCIA Europe): Cautions against rigid interoperability mandates that could create security and privacy risks. Prefers flexible, standards-driven approaches to achieve safe, cross-border interoperability.

Data & Technology for Compliance Alliance: Urges development of common data standards and interoperable APIs to automate compliance workflows. This would facilitate cross-border supervision and reduce reporting burdens.

OpenMined: Promotes open, interoperable privacy-preserving protocols and computation-to-data to reduce fragmentation. Advocates moving beyond siloed bilateral frameworks toward multi-party collaboration.

Dedalus S.p.A.: Calls for targeted development to fill standardization gaps and achieve healthcare data interoperability. Focus is on pragmatic, prioritized standard work to enable cross-border exchange.

LA POSTE: Seeks a harmonized EU definition and governance model for data spaces to ensure interoperability. Clear common rules would enable trusted cross-border data sharing.

Mistral AI: Advocates interoperable data formats and reuse frameworks to support AI development and cross-border data portability. Emphasizes balancing openness with safeguards.

Adyen: Endorses openness and interoperable standards to ensure secure, efficient cross-border payments data flows. Encourages consistency with international frameworks to foster innovation.

1.5.4 Digital Identity & Trust Infrastructure

Stakeholders call for an EU-wide digital identity and trust infrastructure that is secure, interoperable, and usable across borders for both B2B and B2G interactions. Priorities include harmonized implementation of eIDAS 2, deployment of the European Digital Identity (EUDI) and Wallets (for people and businesses), and reliance on open standards, APIs, and standardised trust services (eID, eSignature, eDelivery, eInvoicing). The aim is to reduce costs and complexity for relying parties and trust service providers, avoid vendor lock-in, and enable

predictable, scalable credential use across Member States. Concrete use cases emphasise automating compliance and authorizations: the European Business Wallet (EBW) carrying verifiable identifiers (e.g., LEI, tax IDs) to streamline VAT/CESOP reporting and licensing; automatic recognition and re-use of identity/KYC checks with consent; and cross-border updates of secondary credentials. Stakeholders also stress compatibility with national infrastructures, support for representation (natural-person wallets acting for legal entities), governance that can evolve with technology (some propose making the EBW mandatory), and alignment with global standards to enable seamless cross-border operations and a truly open, trusted data-sharing ecosystem.

> *The DSV supports the deployment of the European Digital Identity (EUDI) and the EUDI Wallet to enable secure, interoperable and cross-border identification processes.* (German Social Insurance European Representation)
>
> *Leverage industry standards and open APIs to promote interoperability and scalability.* (Mastercard Europe SA)
>
> *For VAT registration and CESOP reporting, the EBW could carry a verifiable legal entity identifier, tax identifiers, and proof of incorporation, all issued by competent authorities and automatically accepted across Member States.* (Entrust SAS)
>
> *It is recommended that identity verification processes based on the European Digital Identity (eIDAS 2.0) be automatically recognised as fulfilling KYC requirements across all regulatory frameworks.* (Adigital (Asociación Española de la Economía Digital))

Technology Industries of Finland: Calls for an interoperable EU digital identity and open data exchange backbone centered on a European Business Wallet to automate cross-border B2B/B2G processes. Seeks strong security, EU-wide interoperability, and prevention of vendor lock-in while enabling private wallet innovation.

> *The European Commission should expand and solidify the underlying "soft infrastructure" of the Digital Single Market by launching a comprehensive programme on the interoperable building blocks of the real-time European economy, including the European Business Wallet, with the aim of easing and automating B2B transactions and B2G reporting (e.g., in taxation and sustainability) across Member States.*

Docusign: Advocates an eIDAS simplification package that boosts interoperability and predictability for relying parties and QTSPs. Aims to expand qualified credential use across the EU at lower cost.

> *We support a simplification package that delivers interoperability, predictability and proportionality for RPs and QTSPs, so more users and organisations can rely on qualified credentials and signatures with confidence, across the bloc, and at lower cost.*

Government Office of the Czech Republic: Requests continued allowance for natural-person EUDI Wallets to act on behalf of legal persons. Maintains practical representation and continuity in digital identity usage.

> *At the same time, the Regulation should continue to allow the use of EUDIW issued to natural persons when acting on behalf of a legal person.*

German Social Insurance European Representation: Supports EUDI Wallet deployment for secure, interoperable cross-border identification with compatibility to existing national systems to avoid duplication. Encourages EU-wide management and automatic updates of secondary credentials.

> *The DSV supports the deployment of the European Digital Identity (EUDI) and the EUDI Wallet to enable secure, interoperable and cross-border identification processes.*

Mastercard Europe SA: Promotes leveraging industry standards and open APIs for interoperable, scalable business identity, with harmonized eIDAS 2 implementation. Seeks global interoperability aligned with cross-border operations.

> *Ensure harmonized implementation of elDAS2 across Member States.*

Adigital (Asociación Española de la Economía Digital): Pushes interoperability across identity, data, and finance rules for AML/KYC using APIs and shared consent. Urges automatic recognition of eIDAS 2 identity verification for KYC and reuse of verified identities under safe harbour.

It is recommended that identity verification processes based on the European Digital Identity (eIDAS 2.0) be automatically recognised as fulfilling KYC requirements across all regulatory frameworks.

Entrust SAS: Proposes a mandatory, interoperable European Business Wallet with effective governance to deliver real-world simplification, especially for SMEs. Details verifiable credentials to streamline VAT/CESOP reporting and cross-border financial licensing.

The European Business Wallet must be mandatory, interoperable, and governed effectively to deliver real-world efficiencies, namely in a way that delivers genuine simplification for businesses of all sizes, especially small and mid-caps.

DigitalTrade4.EU: Outlines a union-wide DLT trust backbone to enhance traceability and border operations and facilitate cross-border trade cooperation. Envisions interoperable governance nodes and automated vLEI to streamline compliance.

Japan Business Council in Europe (JBCE): Urges alignment of EU digital identity with global standards and integrating the Business Wallet with existing systems to avoid duplication. Seeks interoperability across borders and ecosystems.

European Signature Dialog: Calls for integrating eIDAS-based identity and trust services into Digital Product Passports. Aims to secure interoperable verification across supply chains.

U.Di.Con. APS UNIONE PER LA DIFESA DEI CONSUMATORI: Supports the European Digital Identity to improve secure, user-centric identification and trust. Encourages broad adoption across the EU.

RELX plc: Backs co-creation of the European Business Wallet with stakeholders to ensure practical, interoperable identity solutions. Focuses on trusted data exchange for business processes.

Brighten Digital: Advocates simplifying integration of digital identity solutions so businesses can adopt interoperable wallets and credentials. Emphasizes ease of implementation and compatibility.

Deutscher Steuerberaterverband e.V. (DStV): Calls for EU-wide interoperability and linking national systems with the EUDI Wallet. Seeks standardized, secure identity and data flows for cross-border operations.

Association des Constructeurs Européens de Motocycles: Views EUDI Wallets as instruments for authorization and delegation in industry processes. Aims to enable secure, verifiable access.

Google: Encourages adoption of open, interoperable digital identity standards to foster cross-border trust and scalability. Supports industry-wide standardization efforts.

BDSI: Supports integrating workflows with an EU Company/Business Wallet to streamline trusted data exchange and compliance. Targets interoperable business identity across sectors.

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: Advocates clear frameworks for secure data access and reuse anchored in interoperable identity and trust infrastructure. Seeks to enable compliant cross-border data sharing.

Charter of Trust: Calls for a balanced, security-first EU Digital Identity and Wallet approach that preserves interoperability and usability. Emphasizes trust and resilience across sectors.

InfoCert: Supports integrating Business Wallets into eIDAS with tailored rules for diverse use cases. Prioritizes interoperability while accommodating business-specific needs.

Trans Sped: Urges clarifying wallet roles and attributes and tailoring Business Wallet integration within eIDAS. Focuses on secure, interoperable credential exchange for enterprises.

European Entrepreneurs CEA-PME: Promotes measures that ease SME adoption of e-identity and trust tools, reducing complexity while maintaining EU interoperability. Supports practical onboarding.

CEN and CENELEC: Promotes standardization synergies to ensure eIDAS-based identity and trust services are interoperable and aligned with European standards. Supports coordinated technical alignment.

European Savings and Retail Banking Group: Supports mechanisms for presumed authorization via EUDI Wallet credentials in banking contexts. Aims to improve trusted digital onboarding and transactions.

Data & Technology for Compliance Alliance: Backs simplifying and supporting the EU Business Wallet to reduce compliance burdens via interoperable, reusable credentials. Seeks practical adoption across industries.

Global Legal Entity Identifier Foundation (GLEIF): Promotes the globally governed LEI to reduce costs and administrative burdens and strengthen Business Wallet interoperability and trust. Encourages universal, cross-border identity anchors.

Capgemini Deutschland GmbH: Recommends mandating EUID and using eDelivery and OpenID4VP to enable secure, interoperable exchange of verifiable credentials. Seeks standardized implementation across the EU.

1.5.5 Cloud Portability & Switching

The EU Data Act's cloud portability and switching rules aim to make it easier to move between data processing services, but feedback across industry highlights a split between anticipated benefits and practical burdens. While some expect a more dynamic market with simpler switching and interoperability, many stress that B2B SaaS/PaaS environments are deeply integrated and heterogeneous, making rapid switching windows and mandatory interoperability difficult, costly, and potentially risky. Stakeholders broadly call for narrowing scope to IaaS, where standardization and open interfaces make portability more feasible, and for clarifying key definitions and obligations around "data processing services," termination rights, permissible switching charges, and reseller scenarios. They also seek flexibility on switching periods and extensions, and the ability to charge for exit assistance, to ensure continuity of service and data access without imposing exit barriers. A major concern is the new early termination right: providers fear revenue uncertainty and impaired investment recovery for innovative offerings and long-term contracts, which could undermine attractive pricing models. Several contributions ask how early termination penalties should be calculated and treated so they compensate actual losses without becoming unlawful barriers to exit, balancing customer mobility with sustainable business models.

The Data Act stipulates that customers of data processing services can easily and quickly (within 2-4 months, depending on the individual case) switch providers and take their data with them. (SIEMENS AG)

Therefore, we strongly recommend restricting the cloud switching provisions to infrastructure service providers (IaaS) and explicitly excluding Software as a Service (Saas) and Platform as a Service (PaaS) from the regulation's scope. (ZVEI e.V.)

The Data Act even provides a possibility for customers of data processing services to exit from contracts before the end of the agreed contractual term. (SIEMENS AG)

Technical measures for the switch must be implemented by the provider and extensive contractual regulations must be agreed with customers in advance - the EU model clauses for this purpose comprise almost 100 pages (unproportionally to and even longer than a usual SaaS contract). (SIEMENS AG)

SIEMENS AG: Warns that the Data Act's switching mandates, especially if applied to SaaS, impose heavy technical and contractual burdens, risk premature termination, and undermine long-term B2B business models. Argues that complex integrations make rapid switching unrealistic and may ultimately hurt customers and investment recovery.

From a customer perspective, the switch between services does not become easier, while the provider has a massive additional administrative and technical burden.

ZVEI e.V.: Urges limiting cloud switching rules to IaaS, excluding SaaS and PaaS where interoperability and portability are not technically or economically viable. Warns that applying Articles 25 and 30 to higher-level services jeopardizes long-term business models and innovation.

Therefore, we strongly recommend restricting the cloud switching provisions to infrastructure service providers (IaaS) and explicitly excluding Software as a Service (Saas) and Platform as a Service (PaaS) from the regulation's scope.

France Digitale: Seeks legal certainty that early termination penalties can lawfully compensate for the new switching rights without being treated as exit barriers. Requests guidance on how to calculate such penalties and handle development fees.

o Is it safe to assume that such early termination penalties will not be considered barriers to exit?

Vodafone Group: Supports easier switching and interoperability for data processing services, expecting a more dynamic, competitive market. Anticipates direct benefits as both a user and reseller of cloud technologies.

As a leading provider of IoT products and services we look forward to participating in a more fluid and dynamic marketplace for data sharing and as a user and reseller of cloud technologies, including those of the Hyperscalers, we expect to benefit from easier switching and interoperability for data processing services.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Calls for clearer definitions and scoping of data processing services to distinguish IaaS, PaaS, and SaaS for switching obligations. Emphasizes that unresolved ambiguities create legal uncertainty for companies.

Furthermore, a clear distinction should be provided in regard to "data processing services", which currently comprises the three com- mon, but vastly different services laaS, PaaS and SaaS.

Inter IKEA Group: Requests clarity on what switching-related charges and exit fees are permissible under the Data Act. Seeks predictable rules for compensating reasonable provider costs during customer offboarding.

DOT Europe: Opposes mandatory cloud interoperability requirements, favoring voluntary or market-led approaches to portability. Warns that prescriptive obligations could disrupt service design and innovation.

CLEPA: Stresses the need to ensure continuity of data access during provider switching so operations are not disrupted. Advocates practical mechanisms that maintain availability throughout transitions.

Connect Europe: Asks for clarification of switching obligations for resellers and intermediaries in multi-party cloud supply chains. Seeks clear allocation of responsibilities to avoid gaps or duplications during customer exits.

Dassault Systèmes: Advocates flexible switching periods with the possibility of extensions to reflect complex enterprise migrations. Argues that any interoperability standards should be limited to IaaS rather than PaaS or SaaS.

SAP SE: Proposes modifying cloud switching provisions to be workable for enterprise software, including proportionate timelines and obligations. Encourages narrowing or tailoring scope for SaaS and PaaS to avoid excessive burden.

Danish Industry: Supports allowing providers to charge for exit assistance while narrowing the switching rules' scope to where portability is feasible. Emphasizes proportionate, cost-reflective approaches to migration support.

DIGITALEUROPE: Calls for flexible, proportionate cloud portability requirements and regulatory guidance. Supports pragmatic timelines and scope that reflect technical feasibility and market realities.

ECIS, European Committee for Interoperable Systems: Seeks clarification on how termination penalties should be treated under the Data Act to ensure they compensate legitimate costs without constituting exit barriers. Requests legal certainty to align contracts with new switching rights.

1.5.6 Proportionate Access, Privacy & Trade Secrets

Stakeholders converge on proportionate, purpose-bound access that protects privacy, intellectual property, and trade secrets. They warn against blanket B2B/B2C mandates and favor calibrated obligations only where market failures or power asymmetries exist, with scope focused on lawful access to non-personal and properly anonymised data. Core safeguards include explicit exclusions for trade secrets, enriched/derived or inferred data, and sui generis databases; clear rights and workable procedures to refuse or condition access; and alignment with GDPR through robust anonymisation standards, consent guidance (including for aggregated datasets), and strict purpose limitation that differentiates access from re-use. Implementation priorities emphasize legal certainty, especially for sensitive or high-risk contexts. This includes streamlined, predictable trade-secret "handbrake" rules; clear modalities for sharing with authorities; retention guidance; and "safe access" mechanisms (standard APIs, model licences) that reduce burdens on SMEs and sole traders while ensuring non-discriminatory access. Voluntary data-sharing frameworks should be incentivised, and sectoral realities respected—e.g., trusted cybersecurity information-sharing ecosystems and cases where over-disclosure (such as detailed technical designs) could irreversibly expose proprietary know-how. The overall goal is balanced interoperability and innovation without eroding privacy or competitive advantage.

Strike a proportionate balance between data access (including machine- readable, non-personal and appropriately licensed data) and data protection (GDPR), with specific safeguards for small operators and sole traders who lack compliance resources. (Siinda)

Article 4(2) of the Data Act should explicitly confirm that Data Holders may restrict access to trade secrets, ensuring that security-related obligations do not override intellectual property protections. (Enel SpA)

These risks are amplified by requirements to store data with third parties and share it with other economic operators, leading to irreversible exposure since no technical or legal solution is available to prevent unauthorized use. (ACEA (European Automobile Manufacturers' Association))

FEBIS members would like to stress the importance of distinguishing between the access to data and the possibility to re-use the data, which should both be based on clear purposes. (FEBIS)

SIEMENS AG: Warns that blanket open-data mandates would force sharing with unrelated third parties and risk leakage of trade secrets, potentially prompting companies to redesign products to limit data. Calls for proportionate access and contractual safeguards.

Enforcing open data access and sharing could result in a revised design that provides less data to prevent unwanted data flow and associated information and loss of trade secrets.

ZVEI e.V.: Advocates removing general B2B/B2C data-sharing obligations in favor of voluntary sharing, applied mandatorily only where clear market failures exist. Criticizes current trade secret safeguards as inadequate and impractical.

In addition, the so called 'trade secret handbrake mechanism' with its required safeguards, such as technical or organisational measures are inadequate to ensure meaningful protection of trade secrets while the threshold requiring a high likelihood of serious economic damage in order to refuse a data access request is excessively high and impractical to meet in real-world scenarios.

Enel SpA: Supports incentivizing voluntary data sharing while explicitly excluding trade secrets and sui generis databases from access obligations. Emphasizes keeping sensitive assets under data holders' exclusive control.

Article 4(2) of the Data Act should explicitly confirm that Data Holders may restrict access to trade secrets, ensuring that security-related obligations do not override intellectual property protections.

European Energy Information Sharing and Analysis Centre: Calls for legal certainty and clear safeguards to enable proportionate sharing of sensitive cybersecurity information, including cross-border threat intelligence. Stresses that trusted frameworks and protections are needed to encourage participation.

Clear safeguards are essential to encourage the sharing of sensitive information between trusted partners.

FEBIS: Urges a clear distinction between access and re-use based on specific purposes, allowing access for compliance checks while limiting re-use. Seeks defined rights for business information providers to access and re-use data for legitimate interests like creditworthiness.

FEBIS members would like to stress the importance of distinguishing between the access to data and the possibility to re-use the data, which should both be based on clear purposes.

Unipol Assicurazioni S.p.A.: Requests a narrower scope for data sharing that excludes enriched and inferred data to protect proprietary know-how. Also seeks clarity on retention periods to avoid disproportionate obligations.

ii) A clearer and narrower definition of the scope of data sharing, explicitly excluding enriched and inferred data.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Supports the trade secrets handbrake but asks for greater legal certainty on its scope to avoid lengthy disputes. Aims to balance user access with effective protection of confidential information.

While we acknowledge the importance of the "trade secrets handbrake" (which frames the conditions under which a data holder can withhold, suspend or, exceptionally, refuse to share data) we consider useful to further reflect on ways to enhance legal certainty with regards to its scope, considering the risk of lengthy and complex arbitration processes between data subjects and data holders.

Siinda: Proposes a proportionate framework enabling lawful access to non-personal or anonymised data while safeguarding privacy and trade secrets, especially for SMEs and sole traders. Warns that blanket mandates can conflict with GDPR and expose sensitive information.

A balanced approach must enable lawful, non-discriminatory access to non-personal or anonymised datasets for business and information providers, while ensuring personal data protections and trade-secret safeguards.

ACEA (European Automobile Manufacturers' Association): Highlights that battery passport rules could expose sensitive technical data and create irreversible commercial risks by requiring third-party storage and sharing. Calls for clearer modalities with authorities and stronger confidentiality protections.

These risks are amplified by requirements to store data with third parties and share it with other economic operators, leading to irreversible exposure since no technical or legal solution is available to prevent unauthorized use.

UNIFE: Notes that invoking exemptions for sensitive business data is unclear and burdensome, risking high costs to protect IP. Recommends simplifying procedures to better balance openness and competitiveness.

Simplifying these provisions and streamlining the documentation burden would help strike a better balance between openness and competitiveness.

Halle Institute of Economic research (IWH): Recommends tiered access models aligned with GDPR to balance data utility with privacy and trade secret protections. Emphasizes proportionate controls tailored to sensitivity levels.

Business & Science Poland: Calls for proportionality in cross-border and domestic data transfers and limiting access obligations to what is necessary. Seeks to avoid undue burdens that could expose confidential business information.

Cisco: Opposes compulsory sharing of trade secrets under the Data Act. Supports mechanisms that protect proprietary information while enabling practical data access where appropriate.

Japan Business Council in Europe (JBCE): Seeks stronger and clearer trade secret protections within the Data Act to ensure confidential business information is not unduly exposed. Advocates balanced access rules that respect IP.

European Banking Federation: Requests safeguarding of IP and licensing terms, including respect for text and data mining opt-outs. Emphasizes proportionate access regimes that preserve confidentiality and contractual rights.

IBM: Urges limiting the Data Act's scope and reinforcing protections for IP and security-sensitive information. Supports access models that do not compromise trade secrets or system integrity.

Polish Confederation Lewiatan: Calls for clearer scope definitions and a preference for voluntary data access frameworks. Warns against mandatory sharing that could endanger trade secrets.

Ecommerce Europe: Promotes interoperable privacy-enhancing technologies to enable compliant, privacy-preserving data sharing. Encourages infrastructure that allows proportionate access without exposing sensitive data.

CECIMO - European Association of Manufacturing Technologies: Emphasizes the need to protect trade secrets in any data-sharing regime. Supports proportionate access that avoids disclosure of sensitive manufacturing know-how.

Centre for Cybersecurity Belgium: Supports proportionate information sharing and access mechanisms that balance security needs with privacy and confidentiality. Encourages clear rules to enable trusted exchanges of sensitive data.

BDSI: Advocates role-based and purpose-limited access for stakeholders to ensure proportionality. Seeks to protect confidential and personal data while enabling legitimate uses.

Orgalim - Europe's Technology Industries: Calls for strong protection of trade secrets and cautions against broad authority access that could compromise proprietary technologies. Favors limited, clearly justified data access.

E.ON SE: Supports limits on user rights under the Data Act to prevent exposure of sensitive operational or security-related information. Emphasizes proportionate access that respects trade secrets.

Cigref: Asks for clearer rules on how trade secrets are handled under the Data Act to avoid unintended disclosure. Seeks balanced mechanisms for access and protection.

Charter of Trust: Urges robust safeguards for trade secrets in data-sharing frameworks. Promotes proportionate access that does not weaken companies' security or competitiveness.

SAP SE: Favors voluntary data sharing supported by clear safeguards for privacy and trade secrets. Warns against rigid mandates that could deter collaboration.

Danish Industry: Warns that the burden to justify refusals falls disproportionately on data holders and that sharing requirements overreach, especially for mixed datasets. Seeks proportionate obligations and clarity to avoid exposing confidential data.

European DIGITAL SME Alliance: Recommends simplifying sharing processes and revising trade secret provisions to reduce complexity for SMEs. Supports access models that are secure and proportionate.

Dedalus S.p.A.: Promotes privacy-preserving data sharing using techniques that protect personal and confidential information. Advocates frameworks that enable safe, compliant access.

DIGITALEUROPE: Urges recognition of legitimate refusals based on security and trade secrets and limiting authority access to sensitive assets like source code. Seeks clear, proportionate safeguards for data holders.

LA POSTE: Calls to adjust Data Act provisions to better protect trade secrets and confidential business information. Emphasizes proportionate access and clear refusal grounds.

European Games Developer Federation (EGDF): Supports mechanisms to filter or reject abusive or excessive data requests. Aims to ensure access remains proportionate and does not compromise sensitive data.

BUGLAS e.V.: Advocates clear usage rights for data owners and holders to preserve control over sensitive information. Seeks balanced access that respects proprietary interests.

WindEurope: Calls for a balanced approach that enables innovation through data access while protecting privacy and trade secrets. Supports proportionate, purpose-bound sharing models.

APPLiA (Home Appliance Europe): Requests exclusion of derived or inferred data from mandatory sharing to protect competitive insights. Supports narrow, proportionate access obligations.

Confederation of Swedish Enterprise: Argues that access rights should be proportionate and not absolute, ensuring confidentiality and IP are preserved. Supports clear limits and safeguards against overexposure of sensitive data.

1.5.7 Competition & Fair Data Access

This category emphasizes ensuring fair, pro-competitive access to data through targeted competition tools (e.g., the DMA) and practical market mechanisms, rather than blanket privacy or access restrictions that limit lawful use for all actors. In B2B contexts, data rights are often self-regulated via tenders and contracts, and trusted intermediaries (BIPs) add verified, value-added information that enables SMEs and sole traders to engage in trade with confidence. To unlock value, policymakers are urged to reduce barriers for startups and SMEs and to explore economic incentives that make sharing viable, such as balance-sheet recognition and data-as-collateral, alongside open, non-discriminatory access and high-quality datasets. Policy design should avoid rules that inadvertently harm competition—such as mandatory disclosures of compensation calculations that risk revealing cost structures and facilitating tacit collusion—while applying interoperability mandates cautiously, given the slow pace of consensus-driven standard-setting and the possibility that competition can better spur innovation and security. A balanced approach prioritizes addressing gatekeeper power, enabling downstream and cross-sector access, protecting confidentiality, and relying on voluntary, market-led sharing with robust dispute resolution, thereby safeguarding innovation incentives and fair rivalry across the digital ecosystem.

Concerns that more proportionate data rules, as suggested above could weaken safeguards against dominant online platforms should be addressed through competition law instruments, not through restrictive interpretations of privacy rules that limit access to data to all actors alike. (Schibsted Media)

These mechanisms should be used to ensure fair access to data and prevent abuse of market power, rather than limiting lawful and responsible data use across the entire digital ecosystem. (Schibsted Media)

Thus, information on an undertaking's market behaviour, such as its cost structure and pricing policy, may allow its competitors to align or adapt their own behaviour, thereby leading to tacit collusion, illegal under Article 101(1) TFEU. (ACEA (European Automobile Manufacturers' Association))

Even at a single point of the tech stack, an approach based on openness and interoperability may be too slow to be feasible. (AI & Partners B.V.)

SIEMENS AG: Siemens argues that B2B data access is effectively governed by market-driven contracts and tenders, producing a fair balance between manufacturers and customers. They see no need for additional bureaucracy to ensure fairness.

Considering B2B business, there is already today a balance between manufacturers and customers when it comes to data.

European Alliance for Research Excellence: EARE warns that current limitations restrict data sharing and disproportionately harm startups and SMEs. Addressing these barriers is key to fair participation in data-driven markets.

This limitation restricts data sharing, impacting startups and SMEs.

FEBIS: FEBIS highlights the vital role of Business Information Providers in enabling fair, trusted trade by supplying verified, value-added data to businesses of all sizes. Policymakers should protect their data reuse functions to sustain transparency, finance, and compliance.

BIP's enable businesses of all sizes to engage in trade with confidence by providing access to verified value-added data.

France Digitale: France Digitale proposes economic incentives that make responsible data sharing viable (e.g., asset recognition, collateral, and PPPs). Such measures would widen fair access while maintaining sustainable business models.

The EU should explore mechanisms that make data sharing economically viable, such as: allowing data to be recognised as an asset on company balance sheets; enabling data to be used as collateral for financial instruments; supporting public-private partnerships that reward responsible data exchange.

Schibsted Media: Schibsted contends that fair access and checks on data concentration should be enforced via the DMA and competition law, not blanket privacy interpretations that restrict all actors. Competition tools should prevent abuses by gatekeepers while enabling lawful, responsible data use.

These mechanisms should be used to ensure fair access to data and prevent abuse of market power, rather than limiting lawful and responsible data use across the entire digital ecosystem.

ACEA (European Automobile Manufacturers' Association): ACEA warns that forcing disclosure of compensation calculation under the Data Act can expose cost and pricing strategies, creating competition law conflicts and risks of tacit collusion. They call for repealing these provisions and relying on dispute-resolution channels instead.

Thus, information on an undertaking's market behaviour, such as its cost structure and pricing policy, may allow its competitors to align or adapt their own behaviour, thereby leading to tacit collusion, illegal under Article 101(1) TFEU.

AI & Partners B.V.: AI & Partners argues that mandated openness and interoperability can be slow and counterproductive in fast-moving markets. In some contexts, fostering competition and more EU providers may better promote innovation, security, and fair access.

As explained below, competition rather than co-operation sometimes provides better incentives for firms to innovate and improve their security.

Doctrine: Doctrine notes incumbents often resist open data to maintain market power, which suppresses innovation and transparency. Policies should curb this resistance to ensure fair access.

Second, incumbent private actors often resist broader open data policies because their market power relies on exclusive or quasi-monopoly access.

European Signature Dialog: European Signature Dialog argues that greater interoperability strengthens competitiveness and facilitates fair data access across markets. Harmonized standards can reduce fragmentation and enable cross-border scalability.

Japan Business Council in Europe (JBCE): JBCE supports allowing reasonable compensation for data sharing under Article 4 to sustain incentives while enabling fair access. This balances data holders' costs with recipients' needs.

Intesa Sanpaolo: Intesa Sanpaolo favors market-led, cross-sector data sharing frameworks that build trust and ensure fair access without heavy-handed mandates. Such approaches can unlock innovation while preserving competition.

ENCIRCLE Research Consortium: ENCIRCLE contends that simplifying data access processes can catalyze growth and innovation. Easier access particularly helps smaller players compete fairly.

DOT Europe: DOT Europe backs open, non-discriminatory access to data to prevent gatekeeper control and promote competition. Equal access rules can expand opportunities across the ecosystem.

Orgalim - Europe's Technology Industries: Orgalim calls for clear rights to use and share operational industrial data across ecosystems. This would spur competitive, fair data-driven innovation among manufacturers and suppliers.

Danish Entrepreneurs: Danish Entrepreneurs urge unlocking Europe's data for startups so they can compete with incumbents and scale across borders. Lowering access barriers is key to fair competition.

Computer & Communications Industry Association (CCIA Europe): CCIA Europe seeks clarity to resolve tensions between gatekeeper obligations and retail data portability, ensuring workable, fair access. Coherent rules can protect competition while enabling data flows.

SAP SE: SAP cautions against adding new data access obligations that could distort competition or create burdens. They favor voluntary, contract-based sharing within existing frameworks.

Danish Industry: Danish Industry stresses that reliable, high-quality data access is essential for competitiveness and innovation. Improving availability and usability supports fair participation across sectors.

Middle Tech Europe: Middle Tech Europe advocates downstream access to data with reduced administrative burdens to help mid-sized firms compete fairly. Streamlined processes can level the playing field.

DIGITALEUROPE: DIGITALEUROPE supports making data sharing under the Data Act voluntary and questions restrictions on non-personal data. They argue heavy mandates risk harming competition and innovation.

OpenAI: OpenAI warns that fragmented, restrictive data access regimes hinder AI development and fair competition. Harmonized, balanced access rules are needed to lower barriers while protecting rights.

Schaeffler AG: Schaeffler calls to facilitate access to industrial data to accelerate innovation, paired with fair and secure sharing arrangements. This can strengthen competitiveness across value chains.

1.5.8 Open Data & B2G Access

Stakeholders call for a balanced framework that both opens public-sector data for reuse and tightly constrains Business-to-Government (B2G) access to private-sector data. On B2G access, they urge precise limits: government requests should be targeted, proportionate, and reserved for clearly defined, exceptional circumstances (e.g., public emergencies) and only after market-based alternatives are exhausted. To reduce uncertainty and protect innovation and trade secrets, contributors seek clearer definitions and safeguards, as well as harmonised, fair compensation rules—preferably aligned with the Data Act's cost-based model—across sectors and member states. On open data, stakeholders push to broaden and enforce access and reuse of Public Sector Information (PSI) and High-Value Datasets, including judicial data (court decisions, agendas, metadata) and core business information such as sole traders/beneficial ownership, to advance AML, KYC, anti-fraud, and legal-tech innovation. They stress the need for interoperability, quality, and clear ownership/licensing to overcome fragmentation and unlock EU-wide, cross-border value. Several warn against creating new exclusionary rights over public web data that would curb legitimate reuse, and advocate audits and monitoring to ensure full and consistent implementation of the Open Data framework, strengthening competitiveness and AI development in Europe.

As such, we reiterate the importance of targeted and proportional data access requests, made exclusively in the event that existing market-based solutions have either been exhausted or are insufficient. (GSMA)

It calls for the activation of necessary measures and mechanisms for access to and re-use of data and Public Sector Information, which is essential for BIPs to continue helping businesses and boosting the global economy. (FEBIS)

Its adoption lays the groundwork for a new category of exclusionary rights- allowing entities to privatize access to public web data that is neither private, copyrighted, nor copyrightable. (Alliance for Responsible Data Collection)

France has shown that it is possible to create a centralised flow of court decisions, balancing transparency with privacy. (Doctrine)

Enel SpA: Urges limiting the scope of public-sector data requests to avoid disproportionate burdens on critical infrastructure operators.

Limiting the scope of public sector data requests, especially where such requests may impose disproportionate burdens on critical infrastructure operators.

Technology Industries of Finland: Advocates restricting mandatory B2G data sharing to genuine public emergencies and eliminating broad, non-essential requests.

Art. 15: Limit mandatory data sharing requests to public emergencies only; delete para. (1)(b) to avoid broad, non-essential data requests.

FEBIS: Calls to activate measures enabling access to and reuse of PSI and core business data so BIPs can deliver AML, anti-fraud, and other public-interest services.

It calls for the activation of necessary measures and mechanisms for access to and re-use of data and Public Sector Information, which is essential for BIPs to continue helping businesses and boosting the global economy.

France Digitale: Urges broadening the scope of High-Value Datasets, including legal-tech relevant materials like court decisions and related metadata, to spur innovation.

In addition, we urge the Commission to broaden the scope of High-Value Datasets as much as possible.

Dun & Bradstreet: Supports recognition of access to PSI and non-PSI as legitimate and advocates including sole trader data within re-usable public-sector information to support compliance and risk assessment use cases.

In particular, we advocate for the inclusion of sole trader data within the scope of re-usable public sector information.

GSMA: Warns that opaque government access provisions threaten innovation and calls for targeted, proportionate B2G requests only after market solutions are exhausted.

As such, we reiterate the importance of targeted and proportional data access requests, made exclusively in the event that existing market-based solutions have either been exhausted or are insufficient.

Telefonica, S.A.: Seeks constrained, clearly justified government access to sensitive commercial data, limited to targeted and proportionate requests when market options are insufficient.

As such, we reiterate the importance of targeted and proportional data access requests, made exclusively in the event that existing market-based solutions have either been exhausted or are insufficient.

Leading Baltic tech and other businesses and professional associations listed in the submission: Advocates easing EU use and reuse of public data so organizations can compete with global rivals leveraging such data for AI and data-driven products.

Meanwhile, global competitors freely use such data to build new data- driven products and AI systems, placing EU organisations at a competitive disadvantage.

Alliance for Responsible Data Collection: Opposes creating exclusionary rights that privatize access to public web data, urging safeguards to preserve open access for innovation and research.

Its adoption lays the groundwork for a new category of exclusionary rights- allowing entities to privatize access to public web data that is neither private, copyrighted, nor copyrightable.

National Land Survey of Finland: Highlights that fragmented public-sector data and low interoperability hinder AI uptake, calling for interoperable, higher-quality datasets across authorities.

Since data in public administration residers often in systems maintained by different authorities, the widespread utilisation of AI in public administration requires data interoperability and improved quality.

: Points out that unclear ownership and licensing of public-sector data inhibits innovation in sectors like agriculture, health, and education, and calls for clearer reuse rules.

Lack of clarity on ownership and licensing of public-sector data limits innovation in sectors such as agriculture, health, and education.

: Promotes privacy-preserving, evidence-based approaches to enable data use for policymaking and citizen understanding while supporting Digital Package objectives.

This would provide evidence-based support for political decision-making and make it easier for citizens to understand.

ACEA (European Automobile Manufacturers' Association): Calls to harmonize compensation for B2G data provision through a cost-based model across sectors to ensure fair remuneration and consistency.

The rules for compensation of data provision should be harmonised by adopting the Data Act's cost-based model across all sectors to guarantee fair remuneration and consistent treatment.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Urges limiting exceptional-need provisions strictly to B2G access while clarifying definitions and obligations to reduce regulatory uncertainty.

It is paramount to reduce regulatory uncertainty by clarifying defini- tions, clarifying the extent of information obligations, protecting trade secrets, limiting the ex- ceptional need to use data to B2G, deleting Article 13 (4) and (5), and postponing the imple- mentation of the Data Act by two years.

Doctrine: Argues for expanding and enforcing open access to judicial data, including centralized, privacy-conscious publication of court decisions and audits of HVDS implementation.

France has shown that it is possible to create a centralised flow of court decisions, balancing transparency with privacy.

Business & Science Poland: Advocates limiting B2G access and narrowing exceptional-need routes to prevent overreach and protect business interests.

carVertical: Urges opening and digitizing public registries to improve access and reduce costs for services such as vehicle history checks.

German Property Federation: Calls for streamlined, predictable processes for public-sector data access to reduce administrative burdens and delays.

Bayerische Motoren Werke Aktiengesellschaft: Supports a harmonized, cost-based compensation framework for B2G data provision aligned with the Data Act.

Irish Farmers' Association: Seeks fair, transparent access to and use of public-sector agricultural data with clear rules that benefit farmers and rural communities.

Milestone Systems: Promotes public-private data-sharing collaborations with appropriate safeguards to unlock innovation and societal value.

Kompetenznetzwerk Datentreuhandmodelle (DatNet): Recommends maintaining no strict open-data mandates, favoring incentive-based or trust-based arrangements like data trusts for sharing.

ASNEF: Advocates automating and standardizing beneficial ownership registries to improve access for compliance and anti-fraud purposes.

DOT Europe: Calls for harmonized EU guidance on government data access requests and cross-border transfers to ensure proportionality and legal certainty.

Association des Constructeurs Européens de Motocycles: Supports standardized, sector-agnostic compensation rules for B2G data access in line with the Data Act.

Google: Urges tighter limits and clearer safeguards on government access to commercial data to protect innovation and user trust.

EFCA - European Federation of Engineering Consultancy Associations: Calls to harmonize open data access, formats, and licensing across Member States to reduce fragmentation and support cross-border projects.

Connect Europe: Endorses targeted, proportionate B2G access combined with fair and consistent compensation for data provision.

DIGITALEUROPE: Recommends deleting overbroad B2G access routes and expanding and harmonizing public data reuse to foster innovation.

Dutch Startup Association: Advocates EU-wide open data availability and consistency to empower startups and reduce barriers to scaling across borders.

Esomar: Calls for fair, transparent access to public data for research and insights while upholding privacy and ethical standards.

Estonian Ministry of Justice and Digital Affairs: Urges expanding categories of high-value public datasets and ensuring their open, machine-readable availability across the EU.

1.5.9 Sectoral Data Sharing & Compliance

This category captures sector-specific approaches to data sharing that must interoperate with cross-sector rules while preserving safety, security, and incentives to invest in data generation. Energy stakeholders propose open, interoperable protocols and dedicated data spaces to enable transactions and grid coordination at scale. Mobility and rail actors flag heavy compliance and classification burdens under horizontal rules, urging dedicated legislation for in-vehicle access, fair compensation, and cost recovery to avoid disincentivizing “smart” systems. In health, manufacturers and researchers stress that sharing raw device data outside MDR/EHDS frameworks risks misinterpretation and security issues, while the pharma sector warns that unclear, extra-territorial scopes reduce legal certainty. Media publishers argue for clearer, risk-based rules to access audience and advertising data essential for sustainability. Insurers emphasize access to aggregated, anonymized incident data as a prerequisite for expanding cyber insurance and boosting systemic resilience, while legal-tech and open-data advocates seek streamlined procedures and lower fees to unlock reuse. Other sectoral needs include harmonized B2G compensation, GDPR-compatible value-chain sharing (e.g., deforestation due diligence), and pragmatic device traceability via e-IFU and UDI integration. Compliance and cross-border alignment are recurring themes: stakeholders call for clarifying territorial scope to avoid conflicts with third-country laws, reducing administrative burdens, and setting proportionate safeguards for trade secrets and security. They favor sectoral legislation or standards where necessary, neutral platforms and common data formats, risk-based governance, and compensation mechanisms to sustain high-quality data supply—while cautioning against overly broad initiatives (e.g., aspects of FIDA) that could entrench oligopolies, create unintended costs, or hinder innovation.

Furthermore, ensuring fair access to in-vehicle data requires dedicated sectoral legislation that moves beyond the Data Act. (Unipol Assicurazioni S.p.A.)

Second, EFPIA is concerned about the EHDS extra-territorial scope, as EU-based entities could be required to share data under EHDS rules even when stored or processed entirely outside the Union. (EFPIA)

The likely consequence: Manufacturers have no incentive to build 'smart' trains - with more sensors and more data. (SIEMENS AG)

Overly strict or unclear interpretations of the GDPR have, for example, led to situations during the implementation of the EU Deforestation Regulation where necessary data sharing within the value chain has been blocked. (Finnish Food and Drink Industries´ Federation (ETL))

: Proposes an open protocol for energy markets to integrate transactions and data exchanges across producers and consumers at all scales, enabling interoperable sectoral data sharing.

The EU can further complement this new framework with an open protocol for energy markets, for instance as proposed by the Di- gital Energy Grid (DEG) initiative, allowing the integration of transactions between producers and consumers at all scales.

SIEMENS AG: Warns that the Data Act's per-item data classification and trade-secret checks for customized trains create heavy administrative burdens that disincentivize deploying smart, sensor-rich systems.

Under the Data Act, each of these data points would have to be individually classified and checked for trade secrets - for every train anew, as they are usually built to customer specifications.

Zimmer Biomet: cautions that requiring raw or uninterpreted connected medical device data sharing outside MDR/EHDS frameworks risks loss of clinical context, misinterpretation, and security breaches, discouraging investment.

Under the Data Act, manufacturers of connected medical devices may be required to share raw or uninterpreted data outside the secure frameworks of the MDR and the EHDS.

EFPIA: Urges clarifying the EHDS territorial scope to avoid extra-territorial data-sharing obligations that conflict with foreign laws, undermine legal certainty, and deter cross-border research and investment.

Second, EFPIA is concerned about the EHDS extra-territorial scope, as EU-based entities could be required to share data under EHDS rules even when stored or processed entirely outside the Union.

Unipol Assicurazioni S.p.A.: Calls to withdraw or reassess FIDA and to adopt sectoral rules that lower in-vehicle data access costs while enabling access to aggregated incident data hubs to expand cyber insurance and resilience.

A critical and necessary component of this proposal is to grant access to the aggregated data collected by the hub, as this is what allows for the diffusion of cyber insurance, a proven driver of overall resilience.

Schibsted Media: Argues media sustainability requires access to reliable user and advertising data under clearer, risk-based, harmonized rules, as purely contextual advertising is not viable for independent journalism.

It simply enables European media publishers and other responsible actors to access the data they need to operate sustainably.

Finnish Food and Drink Industries´ Federation (ETL): Notes that strict or unclear GDPR interpretations have blocked necessary value-chain data sharing for EUDR compliance, underscoring the need for clearer guidance to enable sectoral flows.

Overly strict or unclear interpretations of the GDPR have, for example, led to situations during the implementation of the EU Deforestation Regulation where necessary data sharing within the value chain has been blocked.

Alcon Laboratories Inc: Supports expanding e-IFU and integrating UDI/IFU links into EUDAMED to improve traceability and access to device information, reducing burdens and enhancing compliance.

Integrate UDI and IFU links into EUDAMED for better traceability and access

ACEA (European Automobile Manufacturers' Association): Highlights inconsistent motor-vehicle data rules and lack of compensation mechanisms that create operational complexity and costs, contrasting with the Data Act's clearer compensation framework.

In opposition to this, legislation applicable to motor vehicles currently provide for inconsistent rules which create operational complexity and significant cost for companies.

UNIFE: Warns the Data Act could impose disproportionate burdens on complex, long-lifecycle rail systems, while emphasizing the need to remove barriers to data sharing among sector stakeholders.

UNIFE believes that, to fully harness the benefits of data-focused solutions, it is indeed essential to remove barriers to information-sharing between operators (mainline and urban), infrastructure managers and suppliers.

Doctrine: Calls to simplify procedures and reduce prohibitive fees for accessing key datasets, leveraging AI to streamline processes and encourage lawful sectoral data reuse.

In Germany and Italy, important datasets can only be accessed against prohibitive charges, contradicting the principle of open data.

carVertical: Proposes centralizing EU vehicle data to improve interoperability, transparency, and cross-border access for mobility services and oversight.

DigitalTrade4.EU: Advocates integrating sectoral data like F-gases, ESG metrics, and food information into Digital Product Passports and related registries to enhance traceability, compliance, and finance linkage.

BusinessEurope: Urges aligning GDPR with AML and fraud data-sharing needs to enable compliant cross-sector cooperation, and calls to reassess and narrow FIDA to avoid unnecessary burdens.

European Signature Dialog: Seeks clearer rules on strong customer authentication interoperability and liability to ensure consistent, secure data sharing across payment ecosystem actors.

RELX plc: Calls for harmonized, simplified frameworks for sharing fraud-related data across sectors to improve detection and prevention while maintaining compliance.

Confederation of Norwegian Enterprise (NHO): Recommends broadening permissible fraud data sharing with clearer role definitions and suggests whitelisting essential services and narrowing or withdrawing FIDA to prevent overreach.

MedTech Europe: Advocates simplifying sector-specific health data-sharing rules to enable interoperable, secure exchanges aligned with existing medical regulatory frameworks.

ING: Supports enabling safe, privacy-compliant AML/CFT data sharing across institutions and borders to strengthen financial crime prevention.

ASNEF: Suggests reassessing FiDA's scope and complexity to ensure workable financial-sector data sharing without disproportionate compliance costs.

ENTSO-E: Calls to mandate a European energy data space to standardize and facilitate secure sectoral data sharing for system efficiency, innovation, and oversight.

Federation of European Securities Exchanges: Urges limiting FIDA's scope and excluding CASPs so data-sharing obligations remain targeted and proportionate within financial markets.

Google: Proposes narrowing the Data Act's definition of connected products to avoid overly broad sectoral data-sharing obligations and compliance burdens.

AFME: Advocates a market-driven approach and narrower scope for FiDA to achieve proportionate financial-sector data sharing and compliance.

EFCA - European Federation of Engineering Consultancy Associations: Calls for standardized, interoperable sector data frameworks in engineering consultancy to enable efficient sharing and compliance across projects and borders.

BDSI: Supports interoperable data transmission via ESAP to streamline regulatory disclosures and enable cross-sector access to standardized information.

Renault Group: Requests clear, practical data standards for the Battery Passport and opposes burdensome mandates for dynamic EV data sharing that could hinder innovation and feasibility.

Digital Currencies Governance Group (DCGG): Recommends tailoring data-sharing agreements and refining kill-switch requirements for blockchain contexts, clarifying the Data Act's implications for decentralized systems.

INVERCO: Supports establishing a European Financial Data Space to enable secure, standardized sharing and reuse of financial data across the sector.

European Savings and Retail Banking Group: Favors a cross-sector data-sharing framework over proliferating sector-specific regimes to ensure consistency and reduce compliance fragmentation.

Danish Industry: Calls to enable broader, compliant sharing of fraud-related data among firms and authorities to strengthen prevention and detection.

Dedalus S.p.A.: Urges aligning EHDS with existing interoperability standards and explicitly referencing them to support compliant, efficient health data sharing.

Capgemini Deutschland GmbH: Proposes neutral national platforms as trusted infrastructure to orchestrate sectoral data sharing and interoperability across ecosystems.

CrowdStrike: Supports removing regulatory barriers to cybersecurity telemetry sharing across borders and sectors to strengthen collective defense and resilience.

WindEurope: Warns that generic Data Act obligations could overburden critical energy operators and advocates tailored sectoral rules for safe, efficient data sharing.

Confederation of Swedish Enterprise: Advocates enabling broader lawful sharing of fraud-related data beyond AML/CFT frameworks to enhance prevention across sectors.

1.5.10 AI & Research Data Access

Stakeholders across Europe frame AI and research data access as foundational to excellence, innovation, and sovereignty. They call for broad, timely access to large, high-quality, interoperable datasets, including open-by-default public-sector data and equitable access for researchers, to reduce bias and accelerate scientific discovery. Open data is recast as an investment that delivers economic, social, and democratic value, underpinning robust AI models and a strong EU AI sector. A central barrier is fragmentation: overlapping and inconsistently applied rules across GDPR, the EHDS, and the Data Governance Act create duplicative safeguards, legal uncertainty, and costly compliance that slows research and weakens competitiveness. The community therefore urges a streamlined, risk-based, and predictable framework—aligned with GDPR—for cross-border transfers and research reuse, coupled with clearer legal bases for AI training and research under data protection and IP regimes. Operational priorities include harmonized implementation of the DGA, standardized data exchange, machine-readable formats and APIs, and secure, simplified access to microdata. They also promote portability, data altruism, non-exclusive access to datasets, representative global training corpora, and standardized text-and-data mining rules—ensuring responsible, rights-preserving access that scales AI and research across borders.

Researchers, startups, and innovators across the EU need a legal framework that enables easy and open access to high-quality data. (European Alliance for Research Excellence)

By creating a clear legal basis for data sharing, the Digital Omnibus can ensure a predictable environment that protects rights and enables responsible cross-border research. (EFPIA)

Finally, administrations tend to perceive open data as a cost rather than an investment. (Doctrine)

Yet the French experience demonstrates the opposite: opening court decisions under the 2016 Lemaire Law enabled the emergence of successful legaltech companies like Doctrine, which create significant economic, social, and democratic value. (Doctrine)

European Alliance for Research Excellence: Calls for an EU legal framework that ensures easy, open access to high-quality research data to reduce bias, speed discovery, and power innovation.

Researchers, startups, and innovators across the EU need a legal framework that enables easy and open access to high-quality data.

EFPIA: Warns that overlapping GDPR, EHDS and DGA rules fragment international data transfers and slow research; urges a streamlined, risk-based, GDPR-aligned framework and a clear legal basis to enable responsible cross-border research.

By creating a clear legal basis for data sharing, the Digital Omnibus can ensure a predictable environment that protects rights and enables responsible cross-border research.

Digital Poland Association: Stresses that broad data accessibility is essential to develop AI in Europe.

Wide data accessibility is crucial for AI development in Europe.

Meta Platforms Ireland Limited: Notes that AI and data-driven services require large, diverse datasets and flexible processing rules, making burdensome restrictions especially harmful.

This is especially problematic for AI and data-driven services, which rely on large, diverse datasets and flexible data processing rules.

WKÖ - Austrian Federal Economic Chamber: Advocates leveraging harmonized open data, especially official statistics, and consistent DGA implementation, making public sector data available for AI R&D.

Open data concepts should be enabled by making public sector data available for research and development.

Doctrine: Argues open data is an investment that underpins AI advances and EU sovereignty; calls to strengthen open data policies to provide the datasets needed for robust models and a strong AI sector.

Without adequate data, it is impossible to build robust, reliable, and sovereign AI models.

Halle Institute of Economic research (IWH): Calls for simplified, reliable access to microdata to boost research capabilities and European competitiveness.

Business & Science Poland: Urges limiting copyright barriers and standardizing text and data mining while removing data restrictions that impede AI development.

U.S. Chamber of Commerce: Opposes mandated IP access or disclosure for AI training datasets, emphasizing protection of intellectual property and trade secrets.

Ecommerce Europe: Supports ensuring AI can access data via machine-readable formats and interoperable APIs to enable innovation.

ITI - Information Technology Industry Council: Advocates enabling access to large-scale, high-quality datasets necessary for training advanced AI systems.

Verband der Automobilindustrie e.V.: Supports allowing the use of global datasets and models to develop competitive AI while maintaining responsible safeguards.

The Guild of European Research-Instensive Universities: Promotes open science through data sharing and interoperability to advance research and cross-border collaboration.

TikTok Technology Ltd.: Calls to ensure data access for AI and cautions against stricter copyright rules that would unnecessarily restrict legitimate training uses.

Fedoweb - Federazione Operatori Web: Asks for the ability to collect representative, diverse datasets to build fair and effective AI systems.

Bayer AG: Supports risk-based rules that facilitate cross-border sharing of research data while protecting rights and privacy.

Audience Measurement Coalition (AMC): Promotes integrating panel and census-level datasets to improve audience measurement through AI and analytics.

Mistral AI: Advocates AI model portability and pragmatic licensing exceptions, elevating data altruism and banning exclusivity that would lock up key datasets.

Council of European Municipalities and Regions (CEMR): Calls for standardized, interoperable data exchange frameworks so municipalities can deploy AI effectively.

International Federation of Library Associations and Institutions: Urges equal, non-discriminatory data access for researchers to support robust, reproducible science and AI.

Confederation of Swedish Enterprise: Seeks clearer rules on data access and legal bases for AI development to reduce uncertainty and enable innovation.

1.5.11 Miscellaneous

This category brings together cross-sector observations on how data access and interoperability are being pragmatically advanced to enable trust, efficiency, and value creation. In business information ecosystems, sole traders actively opt in to share professional data with databases to gain legal certainty and commercial visibility—an approach that relies on consent, transparency, and clear benefits rather than imposed data flows. In digital advertising, the emphasis shifts to short, controlled data supply chains that reduce exposure to sprawling intermediaries, improving accountability, consent management, and cross-border risk handling. In the energy sector, stakeholders seek to unlock operational flexibility even when data is limited, highlighting the need for targeted sharing, standardization, and governance mechanisms that extract value while respecting constraints on availability and usage.

It is important to emphasize that sole traders often voluntarily provide their professional data to BIP's databases, recognizing the benefits of enhanced legal certainty and visibility in commercial transactions. (FEBIS)

Data is shared between short supply chains rather than effectively endless matrices of intermediaries and potential advertisers. (Sheridans, on behalf of Awin AG)

This proactive inclusion reflects their clear intention to participate in a transparent and secure business ecosystem. (FEBIS)

FEBIS: Highlights that sole traders voluntarily share professional data with BIP databases to enhance legal certainty and visibility, supporting a transparent and secure business ecosystem.

It is important to emphasize that sole traders often voluntarily provide their professional data to BIP's databases, recognizing the benefits of enhanced legal certainty and visibility in commercial transactions.

Sheridans, on behalf of Awin AG: Advocates limiting data sharing to short, controlled supply chains rather than sprawling matrices of intermediaries and advertisers.

Data is shared between short supply chains rather than effectively endless matrices of intermediaries and potential advertisers.

Elia Group: Focuses on unlocking system flexibility while navigating limitations in data access and sharing.

1.6 Unified Reporting & Incident Management

The clearest path forward is a once-only, EU-wide reporting window that accepts a single, modular report per incident and automatically routes it to all competent authorities, under harmonised definitions, thresholds, and timelines across NIS2, DORA, GDPR, CRA, and the AI Act. A standardized core dataset with sector-specific annexes and a common taxonomy reduces duplication, supports interoperable identifiers, and accelerates cross-border situational awareness. Risk-based, severity-tiered timelines—favoring 72-hour windows and reserving early warnings for the most critical cases—plus phased notifications (lean initial alert, then final) keep focus on material impact and let response take precedence. Clearer, proportionate criteria and local-only reporting where appropriate curb over-reporting and legal uncertainty. Digitization is pivotal: API-first, machine-readable templates (e.g., JSON schemas), open APIs, and SIEM/GRC integration enable automated validation, evidence

re-use, group reporting, and a digital compliance registry, while ensuring confidentiality-by-design. Smart routing, mutual recognition, and unified templates cut administrative burden, including for third-party and supply-chain coordination, and transparent outputs (e.g., dashboards) help explain trends to policymakers and the public. Safe harbors, role clarity, and no forced pre-disclosure of unpatched vulnerabilities foster candid, timely reporting. Practical features—permitting estimates, excluding trivial changes, and clearer guidance and machine-verifiable metrics—improve consistency for firms and insurers alike. Across sub-categories, common threads are harmonization, once-only reporting, and automation, coupled with proportionality and trust safeguards. Together they promise faster crisis response, higher-quality data, and stronger EU-wide resilience.

1.6.1 Aligned Definitions, Thresholds, Timelines & Triggers

Stakeholders across sectors highlight fragmented, overlapping incident-reporting regimes and inconsistent definitions, thresholds, timelines, and triggers across EU laws and Member States. This misalignment causes administrative burden, legal uncertainty, and over-reporting, while making it time-consuming to decide if events are reportable and when awareness occurs; the 24-hour early-warning trigger is seen as low value and confusing. The core ask is alignment: clearly defined, harmonised criteria for what constitutes a significant or serious incident; sector-tailored, indicative thresholds (for example, using a 3- to 4-level impact scale); unified timelines and notification schedules (with default convergence around GDPR-style windows) and single-report-per-incident across regimes. Stakeholders additionally seek convergence in the information required, a unified reporting methodology, clearer AI incident classification rules, specified log-retention parameters, simplified access to national contact points, and proportionate thresholds so small providers are not disproportionately captured.

> *Clearly define criteria for classifying significant incidents, referencing the latest EU implementing regulations (e.g., Commission Implementing Regulation (EU) 2024/2690).* (Telefonica, S.A.)
>
> *We encourage the Commission to align reporting obligations across the AI Act, the NIS2 Directive, and the Cybersecurity Act-particularly regarding timelines, reporting thresholds, the type of information submitted and, where feasible, the adoption of a unified reporting methodology applicable across all regimes.* (Emerson Electric Co.)
>
> *The 24-hour early warning requirement provides minimal added value and creates confusion.* (Verisure)
>
> *Another example is that determining the exact moment of "awareness" is challenging, as initial investigative findings are often incomplete.* (Trellix)
>
> **FERMA - Federation of European Risk Managers Associations:** Highlights fragmentation in reporting obligations and deadlines that creates administrative burden; urges alignment of incident definitions and timelines.
>
> *This fragmentation not only imposes a significant administrative burden, diverting resources from actual security strengthening to compliance management, but also introduces inconsistencies in incident reporting obligations and deadlines.*
>
> **ZVEI e.V.:** Calls to simplify reporting and documentation duties through harmonized thresholds and timelines.
>
> *Simplify reporting and documentation duties.*
>
> **EFPIA:** Notes overlapping cybersecurity laws in the pharmaceutical sector that complicate incident reporting; recommends aligned definitions and thresholds.
>
> *Fourth, the pharmaceutical sector faces overlapping cybersecurity laws.*
>
> **:** Proposes a tiered severity scale with sector-specific indicative thresholds to standardize classification and triggers.
>
> *A 3- or 4-level scale (Major / Significant / Moderate or Minor) based on operational impact, people/data, systemic effect Indicative thresholds defined by sector of activity, for example.*
>
> **German Insurance Association:** Emphasizes that deciding reportability is time-consuming; asks for clearer, aligned thresholds and definitions.
>
> *Currently, determining whether an incident is reportable is highly time-con- suming.*

Telefonica, S.A.: Advocates clearly defined, harmonized criteria for classifying significant incidents, aligned to current EU implementing rules.

Clearly define criteria for classifying significant incidents, referencing the latest EU implementing regulations (e.g., Commission Implementing Regulation (EU) 2024/2690).

Verisure: Argues the 24-hour early warning adds little value and causes confusion; proposes revisiting notification timelines.

The 24-hour early warning requirement provides minimal added value and creates confusion.

Trellix: Highlights difficulty in pinpointing awareness for triggering reports; seeks clearer trigger definitions and pragmatic timelines.

Another example is that determining the exact moment of "awareness" is challenging, as initial investigative findings are often incomplete.

ENGIE: Requests simplified access to contact points and clearer AI incident classification to reduce administrative complexity and align thresholds.

Simplified access to national contact points and clearer rules on AI incident classification would reduce administrative complexity.

Centre for Democracy and Technology Europe: Notes divergent definitions of serious incidents across EU rules; urges harmonized thresholds and timelines.

Definitions of serious incidents differ on the specific context of each EU regulation.

Bolt: Urges clearer differentiation of actions due to legal obligations versus terms violations to align reporting categories and triggers.

Platforms must distinguish every action based on whether the action was due to a legal obligation or due to a violation of terms and conditions.

LSEG: Supports greater convergence of incident reporting across jurisdictions, acknowledging practical challenges.

We support greater convergence in incident reporting across EU jurisdictions, recognising the practical challenges involved.

European Tech Alliance: States current criteria for significant incidents are too low and granular, leading to over-reporting; recommends raising and simplifying thresholds.

The criteria used to classify incidents as "significant" are perceived as too low and too detailed, leading to an excessive number of minor incidents being reported.

ISP Alliance a.s.: Calls for clearly defined and harmonised reporting thresholds calibrated to provider size to avoid disproportionate burdens on small operators.

However, a point of simplification would be to ensure that thresholds for when reporting is required are clearly defined and harmonised, so that small providers are not disproportionately caught by obligations intended for larger operators.

Emerson Electric Co.: Encourages cross-regime alignment on timelines, thresholds, required information, and a unified reporting methodology.

We encourage the Commission to align reporting obligations across the AI Act, the NIS2 Directive, and the Cybersecurity Act-particularly regarding timelines, reporting thresholds, the type of information submitted and, where feasible, the adoption of a unified reporting methodology applicable across all regimes.

Meta Platforms Ireland Limited: Points to inconsistent definitions and thresholds for significant incidents across Member States and frameworks, causing uncertainty and over-reporting.

Inconsistent definitions and thresholds for what constitutes a "significant" incident across Member States and legislative frameworks create legal uncertainty and can lead to both over-reporting and ambiguity.

Finnish Food and Drink Industries´ Federation (ETL): Advocates harmonisation of reporting schedules and notification requirements across regulatory frameworks.

Reporting schedules and notification requirements should be harmonised across the regulatory frameworks.

Adigital (Asociación Española de la Economía Digital): Recommends clear thresholds for notifications and allowing a single report per incident to streamline processes.

Set clear thresholds for incident notifications and allow a single report per incident.

Entrust SAS: Seeks precise log retention specifications on scope, duration, and format to reduce costs and compliance burden within incident management.

Log retention obligations should specify what data must be kept, for how long, and in what form, to avoid excessive storage costs and monitoring burdens.

WKÖ - Austrian Federal Economic Chamber: Highlights duplicative multi-framework, multi-state reporting of the same incident; calls for unified obligations and timelines.

Companies are obliged to report the same incident to different authorities under different regulatory frameworks (e.g., NIS2, GDPR, CRA, DORA) - often in multiple Member States.

European Cyber Security Organisation: Notes variability under NIS2 in definitions, timelines, thresholds, and obligations; urges consistency and alignment.

For instance, under the NIS2 Directive, the definitions of significant incidents, the timelines for reporting, thresholds, and reporting obligations differ.

ACEA (European Automobile Manufacturers' Association): Proposes aligning general incident reporting timelines to 72 hours, consistent with GDPR, with clear criteria for exceptions.

All other incidents should be reported within 72 hours, in line with GDPR requirements.

1.6.2 Harmonized Templates, Taxonomies & Interoperability

Across sectors, stakeholders call for harmonized, interoperable incident reporting to reduce duplication and accelerate response. Current practice requires manual input into multiple templates and faces overlapping supervisory demands, while Member States apply divergent definitions (e.g., "significant incident"), fragmenting compliance and situational awareness. Proposals converge on a single-report or single-dossier approach that can satisfy multiple legal regimes and support cross-regulatory references via interoperable identifiers, while integrating with existing information-sharing channels. The preferred design is a standardized, modular EU template built around a mandatory core dataset with sector-specific annexes, anchored in a harmonized taxonomy of incident types. Coordinated by bodies like ENISA and the European Cybersecurity Competence Centre, and paired with guaranteed technical and organizational interoperability among CSIRTs and competent authorities, such a system would enable consistent thresholds, reduce administrative burden, and speed dissemination of actionable intelligence. Focusing registers and obligations on critical and important functions—and improving availability of shared data and taxonomies—are seen as key enablers for regulatory efficiency and market development.

The development of a standardised modular EU reporting template containing a mandatory core dataset and sector-specific annexes, based on a harmonised taxonomy managed by ENISA and the European Cybersecurity Competence Centre. (ENGIE)

It would also be useful to establish a standardized taxonomy of incident types across all European cybersecurity directives and regulations (e.g., data breach, unavailability, software compromise, intrusion, ransomware, exfiltration). ()

Currently, the growth of this market is hindered by two primary obstacles, as highlighted by the IAIS: a lack of shared data and a lack of a shared taxonomy. (Unipol Assicurazioni S.p.A.)

There is also a different approach among the Member States about what a "significant incident" entails. (European Express Association (EEA))

FERMA - Federation of European Risk Managers Associations: Advocates a unique EU Cyber Incident ID to ensure cross-regime interoperability so one report can be referenced across authorities and legal frameworks, reducing duplication.

unique EU- Level Cyber Incident Identifier (EU Cyber Incident ID) will be an interoperable system across authorities and legal frameworks, so that once an incident is reported under one regulatory regime, it can be referenced in other contexts without duplicating the effort.

Assuralia: Highlights that incident reporting currently requires manual entry into multiple templates, urging harmonized templates to cut administrative burden during crises.

reporting ICT-incidents currently requires manual input into multiple templates, increasing the administrative burden at the very moment resources are needed to resolve incidents.

: Calls for a standardized EU-wide taxonomy of incident types to align directives and regulations and enable consistent classification and reporting.

It would also be useful to establish a standardized taxonomy of incident types across all European cybersecurity directives and regulations (e.g., data breach, unavailability, software compromise, intrusion, ransomware, exfiltration).

European Energy Information Sharing and Analysis Centre: Supports streamlined reporting integrated with existing information-sharing mechanisms to avoid duplication and speed dissemination of actionable intelligence.

Streamlined reporting frameworks should be designed to integrate with existing information-sharing mechanisms, avoiding duplication and supporting rapid dissemination of actionable intelligence.

ALFI - Association of the Luxembourg Fund Industry: Recommends harmonizing registers of ICT third-party providers by focusing reporting and oversight on critical and important functions, aligning scope across regimes.

Adjustments to the scope of registers of ICT Third-party service providers to focus only on critical and important functions

Unipol Assicurazioni S.p.A.: Notes the cyber insurance market is hampered by a lack of shared data and a shared taxonomy, underscoring the need for common definitions and datasets.

Currently, the growth of this market is hindered by two primary obstacles, as highlighted by the IAIS: a lack of shared data and a lack of a shared taxonomy.

Telefonica, S.A.: Urges technical and organizational interoperability between national and sectoral CSIRTs and competent authorities to enable coherent incident handling and reporting.

Guarantee technical and organizational interoperability between national and sectoral CSIRTs and competent authorities.

Seznam.cz, a.s.: Proposes allowing a single report to satisfy multiple legal obligations, promoting cross-regime interoperability and reducing redundant submissions.

We propose that a single report could fulfil multiple legal obligations at the same time.

ENGIE: Advocates an EU-standard modular reporting template with a mandatory core and sector-specific annexes based on a harmonized taxonomy managed by ENISA and the European Cybersecurity Competence Centre.

The development of a standardised modular EU reporting template containing a mandatory core dataset and sector-specific annexes, based on a harmonised taxonomy managed by ENISA and the European Cybersecurity Competence Centre.

European Express Association (EEA): Points to divergent interpretations of what constitutes a 'significant incident', calling for harmonized thresholds and criteria across Member States.

There is also a different approach among the Member States about what a "significant incident" entails.

Infosys Limited: Suggests a single dossier and incident payload to eliminate duplicate workstreams across legal, security, and delivery functions.

In addition, one dossier, leading to one incident payload would remove duplicate workstreams across legal, security and delivery departments

Adigital (Asociación Española de la Economía Digital): Advocates efficiency through supervisory verification mechanisms over duplicative record-keeping, implying preference for streamlined, interoperable compliance processes.

Regarding redirection to market-specific websites: rather than requiring platforms to store every individual consent, it would be more efficient to establish a supervisory system that verifies companies' methodologies via random checks and customer complaint analysis.

ING Group: Observes multiple overlapping supervisory reporting requirements in the financial sector and calls for consolidation via harmonized templates and processes.

The financial sector faces multiple overlapping supervisory reporting requirements.

ACEA (European Automobile Manufacturers' Association): Calls for EU-wide standard incident reporting templates and unified criteria to prevent divergent national requirements.

Standardise the process for reporting relevant incidents under each instrument; EU-wide standard templates for reporting should be developed and reporting criteria should be defined that would apply to all Member States, to avoid diverging requirements at national level.

American Chamber of Commerce to the EU: The provided excerpt contains no specific insight on harmonized templates, taxonomies, or interoperability.

1.6.3 Coordinated Authorities, Routing, Group Reporting & Mutual Recognition

Stakeholders describe a fragmented EU incident-reporting landscape spanning NIS2, GDPR, DORA, the CRA and sectoral rules, compounded by divergent national practices and multiple competent authorities. Companies face duplicative notifications, conflicting thresholds, varied templates and timelines, and inconsistent cross-border supervision—conditions that raise costs, create operational inefficiencies, and increase the risk of non-compliance while discouraging proactive reporting. They call for coordinated authorities and smart routing via a single, predictable contact point and/or a centralized EU portal that accepts one submission and distributes it to the right bodies. Core proposals include harmonised definitions, templates and deadlines; automated and aligned processes across regimes; EU-wide group reporting for multinationals; and mutual recognition or cross-referencing so a report under one framework satisfies equivalent duties elsewhere. Together these measures would reduce duplication, speed crisis response, and improve regulatory coherence without sacrificing protection or accountability.

Double reporting to different authorities should be avoided and responsibilities clearly defined. (German Social Insurance European Representation)

The current cybersecurity framework lacks a single, predictable point of contact for cross-border incidents, which leads to inconsistent supervisory engagement and follow-up across Member States. (Meta Platforms Ireland Limited)

Multiple member states have done so with the rationale that NIS2 incidents are more time critical than DORA. (ING Group)

Create interoperable early-warning and threat intelligence systems between the two continents. ()

FERMA - Federation of European Risk Managers Associations: Overlapping EU cybersecurity rules create complex, duplicative reporting that diverts resources from substantive security work. Greater coordination across authorities is needed to support compliant, proactive incident management.

Indeed, the proliferation of EU cybersecurity regulations has resulted in substantial complexity and overlapping requirements, often diverting organisational resources from genuine security enhancement toward compliance administration.

Workday: NIS2, GDPR, and CRA can force companies to report the same incident to multiple authorities with different forms, thresholds, and deadlines. A single, streamlined EU pathway would reduce duplication and burden.

This may necessitate reporting to multiple authorities using different forms, content and deadlines and based on different thresholds and terminology required by each law.

Docusign: A Digital Omnibus could harmonize reporting and strengthen supervisory coordination while maintaining high protection standards. Streamlining would reduce complexity and improve coherent oversight.

Taken together, such measures would reduce unnecessary complexity, improve regulatory coherence, and strengthen supervisory coordination, while preserving the high standards of protection and trust that underpin the EU's digital landscape.

Amazon: Organizations face duplicative reporting across channels, formats, and timelines under current frameworks. Harmonization would reduce overlaps and ease routing among authorities.

Organisations face duplicative reporting through different channels, formats, and timelines.

German Social Insurance European Representation: A clear EU-wide system with defined responsibilities should prevent double reporting and improve incident routing. Consolidated processes would enable more efficient coordination across authorities.

Double reporting to different authorities should be avoided and responsibilities clearly defined.

ENGIE: Measures that cut costs and confusion while enabling coordinated crisis response would build a unified EU incident management ecosystem. Streamlined reporting strengthens collective resilience.

Together, these three measures would cut reporting costs, reduce confusion, and accelerate coordinated crisis response - transforming the current fragmented regime into a genuinely unified European incident management ecosystem.

European Tech Alliance: Incident templates and duties overlap across AI Act, NIS2, DORA, and GDPR. Aligning definitions and deadlines would harmonize reporting and coordination across regimes.

There is an opportunity to align with definitions of incidents and deadlines for reporting under NIS2, as well as harmonize deadlines between NIS2, DORA, and GDPR.

Meta Platforms Ireland Limited: The lack of a single cross-border contact leads to inconsistent supervisory engagement. Establishing predictable points of contact would improve coordinated incident management.

The current cybersecurity framework lacks a single, predictable point of contact for cross-border incidents, which leads to inconsistent supervisory engagement and follow-up across Member States.

Adigital (Asociación Española de la Economía Digital): Divergent notification channels across EU laws increase complexity; multinational firms should centralize reporting across the EU. A dedicated agency could route submissions to the competent authorities.

At the organizational level, the model proposed involves a centralized agency that channels reporting and implementation mechanisms for digital regulation and distributes already submitted documentation to the respective authorities.

ING Group: Parallel NIS2 and DORA reporting requirements imposed by some Member States increase burden. Harmonization is needed to avoid double reporting and streamline coordination.

Additionally, member states have the option to ask for double reporting next to DORA for NIS2.

: Fragmented incident reporting and limited capacity mirror EU challenges, suggesting the need for harmonized approaches. Interoperable early-warning and threat intelligence would strengthen coordinated response.

The EU's observation that multiple incident reporting obligations create duplication and confusion finds a parallel in Africa, where cybersecurity frameworks remain fragmented, and institutional capacity for incident management is limited.

Union of Entreprenuers and Employers: Cross-referencing across regimes can let one report satisfy equivalent obligations, cutting duplication. This approach addresses differing procedures across sectoral frameworks.

Cross-referencing across existing reporting regimes could further reduce duplication by ensuring that an incident reported under one framework automatically fulfils equivalent obligations elsewhere.

WKÖ - Austrian Federal Economic Chamber: Divergent national deadlines and approaches complicate compliance. Reporting should be simplified, harmonized, and automated to improve routing and mutual recognition.

Reporting obligations should therefore be simplified, harmonized, and automatized.

European Associations of Co-operative Banks (EACB): Financial institutions face overlapping EU and national incident reporting that creates duplication and inefficiencies. Consolidated, aligned obligations would enable more coherent coordination.

These obligations, while necessary for cybersecurity, can lead to duplication, operational inefficiencies and divergent interpretations across Member States.

ACEA (European Automobile Manufacturers' Association): Member States each designate their own reporting bodies, and cross-border cooperation is not guaranteed. Stronger coordination mechanisms are needed to reduce duplication.

Second, each Member State designates its own competent authority or CSIRT as the reporting body.

BusinessEurope: Advocates harmonized reporting standards and coordinated supervisory processes to streamline incident management across the EU.

IBM: Emphasizes aligning regulatory reporting with customer-first notification obligations to avoid conflicts and improve coherent routing of incident communications.

Confederation of Industry of the Czech Republic: Supports reporting to a main establishment's single competent authority with cross-border recognition to reduce administrative burden.

FEDMA: Calls to address fragmentation between ePrivacy and GDPR by unifying notification pathways and improving authority coordination.

Confederation of Norwegian Enterprise (NHO): Urges streamlined reporting and better coordination among authorities to reduce duplicative burdens for businesses.

CENTR - Council of European Top Level Domain Registries: Seeks alignment of AI, NIS2, and GDPR incident reporting to prevent conflicting requirements and enable coordinated oversight.

Ireland - Department of Enterprise, Tourism and Employment: Supports cross-referencing, streamlined processes, and aligned thresholds and timelines to reduce duplication and improve routing across regimes.

International Information System Security Certification Consortium, Inc.: Proposes cross-mapping reporting frameworks so a single incident report can fulfill equivalent obligations, reducing duplication and confusion.

SGI Europe: Highlights dual and sometimes conflicting notification burdens; calls for coordination and mutual recognition to prevent overlaps.

PPC: Advocates a unified ENISA-led reporting channel with a clear mandate to centralize submissions and coordinate Member State responses.

Meetic Group, a Match Group Company: Supports harmonized cross-border reporting with single points of contact to reduce burden and ensure consistent supervisory follow-up.

Clever Cloud: Endorses ENISA-led unified reporting to ease compliance and improve routing and coordination among national authorities.

INVERCO: Encourages DORA information-sharing and streamlined incident transmission to avoid duplication across financial and cybersecurity authorities.

DIGITALEUROPE: Calls to align CRA and NIS2 points of contact and address the multiplicity of authorities that hinders coherent reporting and routing.

1.6.4 Streamlined Obligations & Burden Reduction

Stakeholders call for streamlining and harmonising incident, security, and compliance reporting to reduce administrative burden while preserving strong resilience. Today's obligations are fragmented and duplicative across EU instruments (e.g., NIS2, DORA, GDPR, CRA, AI Act, CER, NCCS), creating parallel mechanisms, overlapping risk-management documentation, and inconsistent authority expectations. They advocate standardised formats, mutual recognition between frameworks, and ideally a single EU reporting platform to simplify obligations and remove redundancy. The emphasis is on proportional, practical requirements that do not hinder crisis response. Proposals include permitting estimates in interim incident reports, avoiding diversion of resources during remediation, excluding trivial changes from reportable events, and targeting heavy burdens like third-party risk registers. Cross-sector alignment (including telecoms) and clearer, unified criteria are seen as key to achieving "smarter compliance" that cuts cost and friction while maintaining high standards of digital operational resilience.

Documentation, reporting, and incident reporting obligations, currently fragmented across various legal acts concerning personal data protection, privacy, and cybersecurity, should be standardized. (Digital Poland Association)

Organisations operating in Europe today face a patchwork of cybersecurity reporting requirements across multiple laws including NIS2, the Cyber Resilience Act, DORA, and the GDPR. (Trellix)

Interim reports should allow the use of estimates or rounded figures ra- ther than requiring exact data, to reduce the reporting burden during crisis management. (German Insurance Association)

In the critical moments following a cyber incident, when every resource must be dedicated to investigation and remediation, current legislative frameworks force a counterproductive diversion. (Unipol Assicurazioni S.p.A.)

Assuralia: Argues that beyond ICT incident reporting, significant burden and cost reductions are possible in third-party risk reporting and related registers without lowering DORA's resilience standards.

Next to ICT-incident reporting, there is huge potential for burden and cost reduction in the reporting exercise connected to third party risk (i.e. the register of information) and other areas, without affecting the high standards of digital operational resilience that DORA currently sets.

Digital Poland Association: Calls to standardize documentation, reporting, and incident-reporting obligations across privacy, data protection, and cybersecurity laws to remove fragmentation.

Documentation, reporting, and incident reporting obligations, currently fragmented across various legal acts concerning personal data protection, privacy, and cybersecurity, should be standardized.

Volkswagen Group: Notes that multiple EU digital laws impose extensive, cumulative reporting requirements, increasing compliance burden.

Several digital legislative acts, introduced by the European co-legislators, include extensive reporting requirements.

European Energy Information Sharing and Analysis Centre: Highlights that cybersecurity and incident-reporting duties are scattered across several instruments, creating fragmentation and overlap.

Current cybersecurity and incident reporting requirements are scattered across multiple legislative instruments (e.g. NIS2, CER, GDPR, the Network Code on Cybersecurity).

Unipol Assicurazioni S.p.A.: Warns that post-incident reporting obligations divert critical resources from investigation and remediation, underscoring the need to streamline.

In the critical moments following a cyber incident, when every resource must be dedicated to investigation and remediation, current legislative frameworks force a counterproductive diversion.

German Insurance Association: Proposes allowing estimates or rounded figures in interim reports to reduce reporting burden during crisis management.

Interim reports should allow the use of estimates or rounded figures ra- ther than requiring exact data, to reduce the reporting burden during crisis management.

Government Office of the Czech Republic: Advocates simplifying legislation to cut administrative burdens that limit growth and innovation while respecting human rights.

CZ generally advocates for the simplification of legislation as an opportunity to reduce administrative burdens and other obstacles that limit business growth and the willingness to innovate while respecting human rights.

Telefonica, S.A.: Points out inconsistent incident and vulnerability reporting across multiple laws and authorities, calling for harmonised processes.

Multiple laws mandate the reporting of security incidents and vulnerabilities, but they do so inconsistently and to different authorities.

Accountancy Europe: Supports the Commission's simplification agenda to streamline compliance, eliminate duplicate or redundant reporting, and achieve goals more efficiently.

Overall, Accountancy Europe supports the Commissions simplification efforts for the purpose of streamlining compliance, removing duplicate or redundant reporting obligations, and ensuring that policy goals are achieved in a smarter way.

Seznam.cz, a.s.: Recommends excluding minor content edits from reporting requirements to avoid unnecessary administrative load.

Alternatively, the requirement to report even minor content changes (e.g., changing a sign in a comment, correction of typos, reformatting of posts to comply with technical requirements, etc. should be excluded.

Trellix: Observes a patchwork of cybersecurity reporting across NIS2, the CRA, DORA, and the GDPR, indicating a need for harmonisation.

Organisations operating in Europe today face a patchwork of cybersecurity reporting requirements across multiple laws including NIS2, the Cyber Resilience Act, DORA, and the GDPR.

ENGIE: Sees room to simplify and harmonise cybersecurity incident reporting across NIS2, CER, DORA, the AI Act, and the NCCS.

Regarding cybersecurity legislation, room for simplification and harmonisation across legislative instruments (e.g. NIS2, CER, DORA, the AI Act, and the NCCS) is also there, especially regarding incident reporting obligations.

Bolt: Notes that some DSA obligations duplicate P2B requirements, suggesting consolidation to prevent overlapping duties.

The DSA imposes obligations that partially duplicate requirements already established under the Platform-to-Business (P2B) Regulation, particularly concerning measures taken against business users who breach terms and conditions or disseminate illegal content.

Infosys Limited: Identifies overlapping information delivered in disparate formats for AI, privacy, and other reports, arguing for alignment and reuse.

For example, AI model risk assessment, detailed technical documentations, privacy specific reporting obligations and various other requirements contain overlapping information delivered through various disparate formats across the EU and member states.

The International Center for Law & Economics: Calls to streamline overlapping incident-reporting across the AI Act, GDPR, NIS2, and related frameworks to reduce redundancy.

Streamline overlapping incident-reporting obligations across the AI Act, GDPR, NIS2 Directive and other frameworks in order to reduce redundant reporting burdens.

AIM - European Brands Association: Urges the Commission to streamline cybersecurity incident reporting and ensure practical, workable implementation of AI and digital identity rules.

We encourage the Commission to streamline cybersecurity incident reporting and ensure the practical and workable implementation of the AI Act and digital identity solutions.

Meta Platforms Ireland Limited: Stresses that burdens extend beyond incident reporting to overlapping risk management requirements and lack of mutual recognition, calling for consolidation.

The compliance burden extends beyond incident reporting to include overlapping risk management requirements and a lack of mutual recognition between frameworks.

Adigital (Asociación Española de la Economía Digital): Asks to address parallel and multiple reporting mechanisms across different regulations by unifying or rationalising them.

Address the existence of parallel and multiple reporting mechanisms across different regulations.

Vodafone Group: Supports sensible reporting simplifications and urges equally ambitious simplification of telecom regulation to address asymmetry and cumulative burdens.

Our message here is straightforward: while we are supportive of common-sense modifications to reporting requirements under the EU's Digital Acquis, efforts to simplify the digital acquis must be at least matched in terms of pace and ambition with simplification of the telecoms regulatory framework; recognising the regulatory asymmetry that exists between digital services and telecoms operators, and the cumulative impact of two decades worth of excessive and fragmented regulation of our sector.

FiCom ry: Suggests harmonising reporting obligations across content moderation, disinformation, cybersecurity, sustainability, and data processing to reduce burden.

Simplifying by harmonizing reporting obligations in the areas of content moderation, disinformation, cybersecurity, sustainability and data processing would be very helpful.

European Cyber Security Organisation: Flags overlapping and unclear cyber incident-reporting requirements across EU policies and countries as a significant operational and compliance challenge.

Overlapping and unclear requirements for reporting cyber incidents across several EU-level policies and between different countries pose significant operational and compliance challenges for entities under scope.

ACEA (European Automobile Manufacturers' Association): Requests harmonised, proportionate rules, a single EU reporting platform, and simplified NIS2 criteria, alongside unified certification.

For cybersecurity, ACEA seeks harmonised, proportionate rules, a single EU reporting platform, simplified NIS 2 criteria, a group privilege under the CRA, and unified certification under UNECE R155.

: Calls to reduce information obligations in the GDPR and the Data Act to lighten compliance burdens.

Reduce information obligations e.g. in the GRPD, the Data Act.

1.6.5 Risk-Based Triage, Proportional Scope & Phased Notifications

This category advances a unified, risk-based approach to incident reporting that prioritizes material impact and operational feasibility. It emphasizes harmonized, severity-tiered timelines across regimes, limiting the scope to incidents of critical relevance and reducing duplication. Early warnings are reserved for the most critical cases, with broader alignment toward 72-hour windows to enable accurate triage, reflect OT realities, and avoid overreporting. Clarity on definitions and thresholds, local-only reporting where appropriate, and impact-focused metrics help cut administrative burden while keeping attention on the most consequential events. Notifications are phased to balance timeliness and accuracy: a minimal preliminary alert to establish situational awareness, followed by more complete updates and a final report. Some stakeholders question the value of multiple interim updates, favoring an initial and final structure to reduce noise. Across the board, entities call for reporting that is actionable and efficient, with incident response and mitigation taking precedence during crises, and for process predictability that aligns with internal playbooks. Automation for severity-based triggers and EU-level support are encouraged to streamline workflows and improve resilience without compromising safety or security.

The establishment of a unified, tiered reporting framework with harmonised deadlines based on incident severity rather than sector-specific rules. (ENGIE)

Preliminary Alert (within 24h) Minimum fields: type of incident, affected scope, impact indicators, contact person, initial measures taken. ()

The severity classification of incidents should be specified, and the required reporting should be harmonised, as well as assessing possibilities for its automation, which could ideally receive EU-level support (e.g., automatic messages to notification channels about events exceeding a certain severity class). (National Land Survey of Finland)

However, the added value of interim notifications is unclear. (LSEG)

Assuralia: Endorses simplifying digital resilience obligations to enable efficient, robust processes without unnecessary burden, aligning with a unified approach to incident management.

The Belgian insurance industry fully supports DORA's goal of digital operational resilience.

: Advocates a phased, three-step notification scheme that starts with a minimal preliminary alert and evolves as investigations progress to improve accuracy and triage.

Preliminary Alert (within 24h) Minimum fields: type of incident, affected scope, impact indicators, contact person, initial measures taken.

European Energy Information Sharing and Analysis Centre: Urges risk-based reporting calibrated to OT realities, with timelines and expectations proportionate to detection and remediation constraints and cross-border dependencies.

Incident reporting obligations should reflect the realities of OT environments, including detection capabilities, remediation timelines, and cross- border operational dependencies.

ALFI - Association of the Luxembourg Fund Industry: Calls for narrowing reporting to incidents of critical relevance and avoiding duplicate group-level submissions, emphasizing proportional scope and simplification.

Incident reporting classification review, to focus on incidents of critical relevance

Telefonica, S.A.: Supports harmonized, efficient reporting focused on timely, actionable information, reducing redundant data and multiple contact points for better triage.

The purpose of reporting should be to provide timely, actionable information while avoiding unnecessary data collection or the administrative burden of multiple points of contact.

Bitkom e.V.: Highlights fragmentation from overlapping laws and urges harmonized, streamlined reporting to reduce duplication and enable clearer risk-based triage.

Companies face parallel reporting duties, inconsistent national implementations, and regulatory duplication.

ENGIE: Proposes a unified, severity-tiered reporting framework with harmonized deadlines to ensure proportionality, predictability, and coherent phased notifications.

The establishment of a unified, tiered reporting framework with harmonised deadlines based on incident severity rather than sector-specific rules.

European Express Association (EEA): Recommends aligning definitions and extending initial notification timelines (e.g., 72 hours) to curb false positives and enable accurate triage across the EU.

Specifically, the initial report should be submitted without undue delay and, in any event, within 72 hours of becoming aware of a significant incident (replacing the current 24-hour requirement to reduce false positives and enable accurate triage; a 48 hour target may be used where feasible).

National Land Survey of Finland: Advocates harmonized severity classifications, automation, and support-focused reporting that prioritizes management and rapid assistance over administrative burden.

The severity classification of incidents should be specified, and the required reporting should be harmonised, as well as assessing possibilities for its automation, which could ideally receive EU-level support (e.g., automatic messages to notification channels about events exceeding a certain severity class).

LSEG: Supports initial and final notices but questions the value of interim reports, favoring leaner phased notifications that focus on meaningful updates.

However, the added value of interim notifications is unclear.

Emerson Electric Co.: Urges calibrated disclosure thresholds and prioritizing containment before detailed reporting, preventing overreporting and enabling risk-based triage.

Affected entities should prioritize mitigating and containing the incident as their primary responsibility, with reporting serving as a secondary consideration in the initial crisis response.

ACEA (European Automobile Manufacturers' Association): Warns that short, rigid deadlines disproportionately burden complex groups and argues 24-hour early warnings should be reserved for the most critical cases.

Early warning requirements (i.e., within 24 hours) should be limited to incidents occurring in particularly critical areas.

ENSHPO - The European Network of Safety and Health Professional Organizations: Promotes streamlined, risk-based reporting that prioritizes safety-critical information and proportionate obligations.

Bayerische Motoren Werke Aktiengesellschaft: Advocates targeted NIS2 reporting with focused early-warning mechanisms, aligning notifications to material risk and operational relevance.

IBM: Emphasizes mitigating incidents before disclosure to reduce risk, suggesting notification timing and scope should reflect containment priorities.

Confederation of Industry of the Czech Republic: Supports making only targeted notifications mandatory, ensuring proportional scope and avoiding unnecessary reporting.

Inter IKEA Group: Recommends reporting only confirmed, significant incidents to avoid noise and concentrate resources on material events.

Federation of European Securities Exchanges: Suggests proportional, simplified reporting with optional aggregation to reduce burden while preserving oversight of significant trends.

Association des Constructeurs Européens de Motocycles: Urges limiting 24-hour early warnings to essential situations, aligning obligations with risk and feasibility.

Sdružení pro internetový rozvoj (SPIR): Advocates presuming trusted flagger notices are accurate, enabling faster triage and targeted follow-up within a risk-based workflow.

Google: Calls for rigorous vetting of complaints to filter low-quality reports, enhancing triage and focusing resources on significant issues.

CLEPA: Seeks to limit the scope of reporting obligations to what is proportionate and risk-relevant for organizations.

European Association of Public Banks: Backs impact-focused reporting to cut administrative costs and warns that excessive workload diverts attention from truly critical incidents.

European Savings and Retail Banking Group: Supports extending reporting only where individuals' rights are at stake, reinforcing a proportional approach to notifications.

DIGITALEUROPE: Warns that mandatory notifications can undermine operational discretion and urges decoupling response activities from authority notification for proportionality.

1.6.6 One-Stop Portals & Once-Only Reporting

Stakeholders across sectors call for a one-stop, once-only approach to incident and compliance reporting under the EU digital acquis. Today, obligations under instruments like NIS2, DORA, GDPR, CRA and AI are fragmented, duplicative, and inconsistently applied across Member States, creating heavy administrative burden, diverting resources from incident response, and undermining resilience and competitiveness. The shared goal is to streamline and harmonise without weakening protections. Proposals converge on an EU-level single point of entry: a centralised portal offering one unified form recognized by all competent authorities and interconnected with national systems. A "one principle, one report" model would let entities submit a single report per incident valid across legal acts, supported by a Single Reporting Window, aligned timelines, and coherent guidance. Suggested design choices include relying on EU-level frameworks (e.g., GDPR), extending existing platforms (e.g., ENISA/CRA) to other regimes, enabling "certify once, comply many" where relevant, and optionally a 28th-regime opt-in. Best practices from unified national portals should inform implementation, and narrowly scoped exceptions (e.g., direct reporting of classified information) may be preserved.

This EU-level portal would interconnect with national authorities and offer one unified form, recognized by all. ()

Streamline Incident Reporting Through a "One Principle, One Report" Approach: To reduce administrative complexity and enhance regulatory efficiency, the EU should adopt a "one principle, one report" model for incident reporting. (Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique)

For instance, up to 27 separate incident notifications across 27 different jurisdictions may be triggered for only one single incident. (European Express Association (EEA))

Amend Chapter IX of the Data Act to establish a "One-Stop-Shop" at EU level, that is a competent authority that companies can voluntarily opt in to under a 28th regime. (Technology Industries of Finland)

FERMA - Federation of European Risk Managers Associations: Calls for a single EU point of entry for AI incident reporting capable of handling complex value chains. Emphasizes unified intake to manage the added AI reporting layer effectively.

The creation of a 'single point of entry' becomes even more necessary to manage the new layer of Al incident reporting and must be designed to handle the complexity of the AI value chain.

Assuralia: Urges coherent obligations across legal frameworks and elimination of duplicate reporting across instruments like DORA, GDPR, and CRA. Seeks streamlined, once-only style processes to reduce burden.

reporting obligations should be coherent across legal frameworks and duplicated reporting (e.g. under DORA, GDPR, CRA) should be eliminated.

TIC Council: Advocates streamlining reporting processes while preserving protections. Supports simplification that does not dilute safeguards.

Streamline reporting without weakening protections.

Kaspersky Labs Limited: Supports harmonizing and simplifying cybersecurity reporting obligations across the EU. Sees simplification as a major opportunity for efficiency.

In particular, we see significant potential in the harmonization and simplification of cybersecurity reporting obligations.

Enel SpA: Backs streamlined and simplified reporting obligations under the Cybersecurity Act. Argues simplification strengthens compliance.

Enel supports streamlined obligations and simplification of reporting under the Cybersecurity Act.

Technology Industries of Finland: Proposes amending the Data Act to create an optional EU One-Stop-Shop authority under a 28th regime. Aims to centralize and simplify cross-border reporting.

Amend Chapter IX of the Data Act to establish a "One-Stop-Shop" at EU level, that is a competent authority that companies can voluntarily opt in to under a 28th regime.

: Endorses an EU-level portal with one unified form, interoperable with national authorities. Seeks a single interface recognized across jurisdictions.

This EU-level portal would interconnect with national authorities and offer one unified form, recognized by all.

Dun & Bradstreet: Highlights that reporting under NIS2, DORA, and GDPR is overly complex, duplicative, and inconsistent. Calls for harmonization to reduce fragmentation.

At present, reporting requirements under instruments such as NIS2, DORA, and GDPR breach notification rules remain overly complex, duplicative, and inconsistently applied.

Unipol Assicurazioni S.p.A.: Promotes a single hub for cyber-incident reporting to streamline compliance and bolster resilience. Envisions centralized intake for efficiency.

Finally, establishing a single hub for cyber-incident reporting would represent an essential step toward streamlining compliance and enhancing collective resilience.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Recommends a one principle, one report approach to incident reporting to cut administrative complexity. Focuses on efficiency and regulatory coherence.

Streamline Incident Reporting Through a "One Principle, One Report" Approach: To reduce administrative complexity and enhance regulatory efficiency, the EU should adopt a "one principle, one report" model for incident reporting.

German Insurance Association: Notes DORA and CRA offer similar protections but diverge in implementation, implying alignment needs. Supports reducing overlap across regimes.

DORA and the CRA offer similar protection but differ in implementation.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Calls for an EU-wide single reporting channel covering data breaches, AI failures, and rights concerns. Aims to avoid redundant notifications to multiple regulators.

Introduce an EU-wide single reporting channel for digital compliance incidents, that is covering data breaches, AI system failures, or fundamental rights concerns, to prevent redundant notifications across regulators.

GSMA: Supports sensible modifications to reporting across the Digital Acquis and urges ambitious simplification of telecoms rules. Seeks to address regulatory asymmetry.

While we are supportive of common-sense modifications to reporting requirements under the EU's Digital Aquis, these efforts must be matched if not exceeded in terms of pace and ambition with simplification of the telecoms regulatory framework; recognising the regulatory asymmetry that exists between digital services and telecoms operators.

Telefonica, S.A.: Advocates a once-only compliance and reporting model to reduce complexity and boost competitiveness. Emphasizes efficiency and consistency across frameworks.

Telefónica advocates for a once-only compliance and reporting model to reduce complexity, improve efficiency and global competitiveness.

Snap Inc.: Urges simplification and coordination of incident and breach reporting across GDPR, DORA, CRA, NIS2, and sectoral rules. Calls for a unified, coherent mechanism.

We believe it is essential to simplify and/or coordinate the incident and breach reporting mechanism under GDPR, DORA, Cyber Resilience Act, NIS2, and other regulations, directives and sector-specific frameworks.

ING Romania: Suggests relying on EU-level frameworks and harmonizing supervisory reporting via a Single Reporting Window. Seeks clarity on interactions like data minimization.

Rely on EU-level frameworks like GDPR to avoid conflicting national rules, clarify how data minimisation interacts with other regulations, and harmonise supervisory reporting through a Single Reporting Window.

Association française de normalisation (AFNOR): Promotes a certify once, comply many approach so AI conformity is recognized across the EU digital acquis. Aims to avoid duplicated assessments.

Likewise, conformity assessments for Al systems should not be duplicated: a "certify once, comply many" approach would allow businesses to demonstrate compliance once, with recognition across the EU digital acquis.

Verisure: Advocates a unified reporting platform with rationalized obligations and aligned timelines. Seeks simplification while maintaining digital trust.

The company advocates for an unified reporting platform, rationalized notification obligations, and aligned timelines to ensure both simplification and robust digital trust across the EU.

Trellix: Warns that overlapping and conflicting EU requirements hinder timely incident response. Calls for simplification to refocus resources on remediation.

Timely incident reporting is vital for digital resilience, but the current EU framework complicates this with overlapping and conflicting requirements that draw resources away from response.

ENGIE: Proposes a centralized EU incident notification platform enabling a single report valid across legal acts. Aims to replace multiple parallel submissions.

The creation of a centralised EU incident notification platform allowing entities to submit a single report per incident valid for all relevant legal acts.

Mastercard Europe SA: Notes Member State fragmentation creates avoidable costs and greater vulnerabilities. Supports EU-wide harmonization of reporting.

Fragmentation across Member States introduces avoidable costs and heightens vulnerabilities.

European Express Association (EEA): Illustrates the burden of multiple national notifications for one incident across up to 27 jurisdictions. Highlights need for one-stop reporting.

For instance, up to 27 separate incident notifications across 27 different jurisdictions may be triggered for only one single incident.

Infosys Limited: Backs applying the once-only principle to improve competitiveness and reduce regulator and business burdens. Positions it as an actionable Commission step.

This proposed approach builds upon the once-only principle enshrined into EU policy making and is actionable step within the discretion of the Commission that can have an immediate effect on improving the blocs competitiveness, while enhancing transparency and reducing the burden on the EU and member state regulators.

Ibec: Prioritizes streamlining reporting obligations in the EU's digital simplification agenda. Emphasizes reducing compliance complexity for business.

A priority area for Irish business in the digital simplification process is the streamlining of reporting obligations (see Section 3).

Evotrust: Advocates simplifying the EUDI framework, aligning with unified and streamlined digital processes. Seeks reduced complexity for identity-related compliance.

This paper presents the position of Evostrust on simplifying the European Digital Identity (EUDI) Framework.

Schneider Electric: Describes EU incident reporting as fragmented and burdensome when one event triggers multiple regimes. Calls for consolidation to ease compliance.

In the current EU regulatory landscape, cybersecurity incident reporting is fragmented and burdensome, especially when a single incident falls under multiple regulations.

Meta Platforms Ireland Limited: Warns that fragmented, duplicative national implementation undermines cybersecurity effectiveness. Argues for consistent, unified approaches.

While vital EU instruments like the NIS2 Directive are establishing a high common level of cybersecurity, their ultimate effectiveness is being undermined by fragmented and duplicative implementation at the Member State level.

Finnish Food and Drink Industries´ Federation (ETL): Recommends the once-only principle so a single notification covers NIS2, CER, GDPR, and CRA. Seeks to cut administrative load on companies.

Administrative burden on companies should be reduced by implementing the once only principle, where a single notification suffices for all authorities (NIS2, CER, GDPR, CRA).

Adigital (Asociación Española de la Economía Digital): Proposes using a single platform and a single authority for each incident. Aims for clarity and reduced duplication.

Use a single platform and a single authority for each incident.

Vodafone Group: Cites Belgium and Croatia's unified portals as best practices for EU-wide adoption. Encourages scaling proven national models.

Belgium and Croatia offer unified portals and clear guidance, which should be considered best practices for EU-wide adoption.

ING Group: Advocates relying on EU frameworks and harmonizing reporting via a Single Reporting Window. Seeks consistency and reduced conflict across rules.

Data: Rely on EU-level frameworks like GDPR to avoid conflicting national rules, clarify how data minimisation interacts with other regulations, and harmonise supervisory reporting through a Single Reporting Window.

Union of Entreprenuers and Employers: Notes cybersecurity regulation is among the most fragmented areas. Supports efforts toward coherence and unified reporting.

Cybersecurity regulation remains one of the most fragmented areas.

Anitec-Assinform: Calls for an effective one-stop shop platform, extending CRA's single entry to NIS2 and GDPR using ENISA, with single Member State registration. Aims to centralize and simplify.

Implement an effective one-stop shop platform: extend CRA single point of entry to NIS 2 and GDPR, use ENISA platform as reference, ensure single Member State registration

European AI Forum: Supports an EU-wide single reporting channel for digital compliance incidents to prevent redundant notifications. Envisions cross-regime coverage in one flow.

Introduce an EU-wide single reporting channel for digital compliance incidents, that is covering data breaches, AI system failures, or fundamental rights concerns, to prevent redundant notifications across regulators.

European Cyber Security Organisation: Stresses the need for coherence across instruments and countries for effective implementation. Implies harmonized reporting to ensure consistency.

Ensuring coherence across policy instruments and countries is essential to the effective implementation of legislation.

: Promotes a once collected, multiple use principle so reported data can be reused without duplication, including for sustainability reporting. Seeks cross-purpose efficiency.

Apply the once collected, multiple use principle so data already reported to one authority can be reused for sustainability reporting without duplication.

ACEA (European Automobile Manufacturers' Association): Advocates a single European platform for incident reporting regardless of the mandating instrument. Targets a unified, instrument-agnostic process.

Develop a single European platform for reporting incidents, regardless of the instrument mandating notification.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Supports unified reporting while preserving the option for direct classified reporting to national authorities. Balances centralization with security needs.

Notwith- standing the above stated arguments, companies should still have the possibility to directly report clas- sified information to their national competent authority if deemed necessary.

1.6.7 Digital Automation, APIs & Machine-Readable Data Sharing

Stakeholders advocate an API-first, machine-readable, born-digital regulatory approach to unify incident reporting and reduce administrative burden. Common taxonomies and JSON schemas, open APIs, and interoperable reporting tools would enable real-time compliance checks, automated evidence exchange, and integration with existing enterprise systems (e.g., SIEM and GRC). Reuse of established standards (XBRL, CEF, OSCAL) and standardized templates would improve data comparability and consistency across Member States. A single reporting window—ideally at EU level—should harmonize thresholds, timelines, and formats across NIS2, GDPR, eIDAS/CRA, DORA, and the AI Act, with automated routing to the competent authority, machine-readable attachments (IOCs), and threaded updates for the same incident. A common incident payload with control mapping tables (e.g., AI Act and ISO/IEC frameworks) and automated evidence re-use would further streamline submissions. To reduce duplicated efforts, proposals include unified audits and assessment reuse (e.g., presumption under eIDAS), a digital compliance registry, and automatic information sharing among national authorities and across corporate groups. Operational digitization rounds out the vision: digitized forms and pre-filled templates, API-based uploads, AI-assisted report validation, and practical scheduling tools, complemented by real-time supervisory and security data sharing. The category also highlights current gaps in EU tooling and the need to replace manual, error-prone processes (e.g., webforms and spreadsheets) with robust, centralized, automation-ready infrastructure.

We also support the establishment of a single reporting window (API) with harmonised profiles for eIDAS, NIS2, and GDPR, automated routing to competent recipients, machine-readable attachments (IOCs, indicators), and threaded updates for the same incident within the respective legal deadlines. (Intesi Group)

We ask the Commission to (i) consider a common taxonomy and machine-readable JSON schema that is accepted across AI Act, CRA, NIS2, GDPR and data to flow automatically when required between regulators; (ii) mandate API-based conformity documentation uploads and (iii) allow automated evidence re-use across incidents and assessments. (Infosys Limited)

Whereas the U.S. FDAs eSTAR standardizes submissions and edits and provides step-by-step guidance, the EU lacks comparable infrastructure; for example, EUDAMED is still not required. (Epic Systems)

For example, when a NIS 2 entity offers services to a DORA financial entity and suffers an incident, the supplier may be legally required to report under NIS 2 but contractually prevented if the financial entity chooses not to report under DORA. (Anitec-Assinform)

Epic Systems: Highlights the EU's lack of standardized digital tooling for regulatory submissions, hindering automation and machine-readable workflows. Emphasizes the need for infrastructure comparable to U.S. eSTAR to support unified reporting.

Whereas the U.S. FDAs eSTAR standardizes submissions and edits and provides step-by-step guidance, the EU lacks comparable infrastructure; for example, EUDAMED is still not required.

Technology Industries of Finland: Advocates born-digital legislation with machine-readable formats, common standards, and open APIs. Aims to enable automated reporting, real-time compliance checks, and cross-EU interoperability.

Develop machine-readable regulations with open APIs to enable real-time compliance checks and automated reporting and to streamline interactions between businesses and regulatory authorities.

Intesi Group: Calls for a unified single reporting window with harmonised profiles and machine-readable incident payloads, plus automated routing and threaded updates. Proposes reusing conformity assessments to avoid redundant audits across regimes.

We also support the establishment of a single reporting window (API) with harmonised profiles for eIDAS, NIS2, and GDPR, automated routing to competent recipients, machine-readable attachments (IOCs, indicators), and threaded updates for the same incident within the respective legal deadlines.

ENGIE: Supports harmonised APIs integrated into operational systems to automate reporting and improve comparability. Stresses that digital measures can drastically reduce complexity and foster consistency.

Such measures would drastically reduce reporting complexity, enable automation (e.g. integrate reporting APIs in their SIEM systems), improve data comparability and foster regulatory consistency.

Infosys Limited: Promotes a common taxonomy and machine-readable JSON schema accepted across major regulations, with API-based uploads and automated evidence reuse. Seeks consolidation that lowers compliance costs and accelerates processing via interoperability.

We ask the Commission to (i) consider a common taxonomy and machine-readable JSON schema that is accepted across AI Act, CRA, NIS2, GDPR and data to flow automatically when required between regulators; (ii) mandate API-based conformity documentation uploads and (iii) allow automated evidence re-use across incidents and assessments.

ING Group: Recommends centralising incident reporting via a single EU channel with an API to integrate directly with internal systems. Aims to eliminate manual, error-prone workflows and standardise submissions.

Ideally, this single EU entity would provide an API, so reporting institutions can establish a link directly with their internal incident reporting systems.

Anitec-Assinform: Urges harmonised cybersecurity incident reporting with aligned thresholds and timelines, using machine-readable formats, APIs, and automation. Also calls for coordinated disclosures and mechanisms to resolve cross-regulatory conflicts.

The EU should maximize opportunities for machine-readable formats (e.g., OSCAL), standardized data formats and use of APIs, to allow for process automation and usage of AI where possible with current technology when setting down the requirements for cybersecurity reporting.

Alcon Laboratories Inc: Advocates end-to-end digitisation of conformity assessments with structured data exchange and AI-assisted checks. Suggests templates, pre-filled forms, and digital scheduling to streamline submissions.

Digitize conformity assessment workflows to enable structured data exchange, replacing traditional document-based submissions.

DigitalTrade4.EU: Proposes machine-readable Digital Product Passports to automate carbon reporting and interfaces that connect tax and customs data. Envisions real-time RegTech supervision through interoperable APIs.

Association des Constructeurs Européens de Motocycles: Supports a digitised regulatory portal and automation to simplify submissions and reduce burden. Emphasises standardized, machine-readable interactions with authorities.

International Information System Security Certification Consortium, Inc.: Highlights how APIs enable automated workflows and streamlined reporting. Encourages interoperable, machine-readable exchanges to improve incident management.

BDSI: Promotes automated mapping of company data to ESRS and VSME standards using machine-readable schemas. Seeks to simplify compliance through digital tooling.

CLOUD INFRASTRUCTURE SERVICES PROVIDERS IN EUROPE: Advocates an EU digital compliance registry with interoperable formats and APIs for cross-authority data sharing. Targets reduced duplication and seamless incident reporting.

Palo Alto Networks: Calls for standardized APIs to share real-time security telemetry across stakeholders. Aims to accelerate detection, response, and coordinated incident management.

SAP SE: Encourages AI-powered automation of reporting and machine-readable submissions via APIs. Focuses on reducing manual effort and improving auditability.

Wolt: Pushes for harmonised, API-driven incident reporting across EU regulations to cut administrative burden. Emphasises unified payloads and interoperable data flows.

CrowdStrike: Recommends allowing AI tools within reporting processes and structured data exchange. Seeks automation-friendly rules that enable machine-readable compliance.

1.6.8 Safe Harbors, Liability & Role Clarity

Stakeholders converge on the need for safe harbors and explicit liability protections to enable timely, candid reporting within EU cyber and product security frameworks. They urge no-liability assurances for good-faith notifications and controlled sharing of sensitive information, reinforced confidentiality of submissions, and clear delineation of what constitutes a reporting obligation versus other transparency duties. Given the heavy penalties for non-compliance under NIS2, predictable protections and role clarity are viewed as essential to avoid chilling effects and to build trust in unified reporting channels. Operational clarity is equally important: avoid mandating disclosure of previously unknown, unpatched vulnerabilities before fixes are available; grant vendors reasonable time to remediate; clarify that reporting obligations end when a product's support period concludes; and enable withdrawal or downgrading of misclassified or immaterial events. Clear assignment of responsibilities among manufacturers, deployers, and service providers, combined with liability shields and confidentiality, is expected to increase reporting quality and speed, thereby improving EU-wide situational awareness and response.

To foster this transparency, it is vital to integrate liability clauses within the reporting framework. (Trellix)

Introduce liability clauses in NIS2 and CRA, clarifying that notification shall not expose the notifying entity to liability for potential spill-over effects caused by the act of notification xxxviii. (Ibec)

Requiring manufacturers to report previously unknown, unpatched vulnerabilities to EU authorities before a patch is ready creates severe risks. (Workday)

Clarify that reporting obligations end once a product's support period concludes. (Verisure)

FERMA - Federation of European Risk Managers Associations: Warns that failure to meet cyber incident reporting obligations can carry severe fines under NIS2, underscoring liability exposure. Highlights the need for compliance clarity to mitigate penalty risk.

For example, non-compliance with NIS2 re- porting obligations may result in fines reaching up to €10 million or 2% of annual turnover for essential entities, and €7 million or 1.4% of turnover for important entities.

Workday: Argues against mandating disclosure of unpatched vulnerabilities before fixes are available due to security risk. Calls for allowing vendors time to develop and deploy patches before reporting.

Requiring manufacturers to report previously unknown, unpatched vulnerabilities to EU authorities before a patch is ready creates severe risks.

Verisure: Seeks clarity that reporting obligations cease when a product's support period ends. Addresses liability and responsibility boundaries over a product's lifecycle.

Clarify that reporting obligations end once a product's support period concludes.

Trellix: Advocates for embedding liability protections within reporting frameworks to provide legal certainty. Predicts this will incentivize faster, fuller reporting and improve collective response.

Incorporating liability protections into the reporting structure offers legal clarity and assurance for organisations.

Centre for Democracy and Technology Europe: Clarifies that requirements to publish copyright policies are not reporting obligations. Differentiates internal policy transparency from incident or model reporting duties.

This provision merely requires GPAI providers to establish and make public their internal policy approach to copyright compliance, rather than disclosing substantive information about the model, its training data, or its operations.

Ibec: Supports liability shields for entities that notify incidents to enable controlled information sharing. Proposes clauses ensuring notifications do not create legal exposure from spill-over effects.

Introduce liability clauses in NIS2 and CRA, clarifying that notification shall not expose the notifying entity to liability for potential spill-over effects caused by the act of notification xxxviii.

American Chamber of Commerce to the EU: Urges stronger confidentiality around notifications to protect reporting entities. Enhanced protections would reduce legal risk and encourage candid reporting.

BusinessEurope: Calls for assurances that entities incur no liability after fulfilling incident notification duties. This safe harbor would reduce disincentives to timely reporting.

IBM: Recommends liability protections for reporting and information sharing to foster cooperation. Clear safe harbors would encourage timely and accurate disclosures.

Confederation of Industry of the Czech Republic: Requests liability protections tied to notification to reduce legal risk. Seeks clear rules that reporting in good faith should not trigger penalties.

Confederation of Norwegian Enterprise (NHO): Asks to clarify that notifying authorities does not create post-notification liability. This would provide certainty and support prompt reporting.

ITI - Information Technology Industry Council: Advocates liability safe harbors to encourage incident reporting and information exchange. Legal clarity would improve participation and response timelines.

DOT Europe: Emphasizes clear accountability, rights of defense, and timely investigations in reporting processes. Role clarity helps balance transparency with fair treatment.

Association des Constructeurs Européens de Motocycles: Supports liability protection for notifications to avoid penalizing good-faith reporting. Safe harbors would encourage early engagement with authorities.

Google: Warns that forcing disclosure of unpatched vulnerabilities can elevate risk. Argues for reporting timelines that prioritize patch development and deployment.

secunet Security Networks AG: Endorses liability protections to encourage reporting without fear of legal repercussions. Safe harbors and clarity would bolster incident information flows.

European Association of Public Banks: Proposes withdrawal procedures for misclassified or immaterial events to avoid unnecessary obligations. Process clarity limits liability from over-reporting.

ACT | The App Association: Recommends safe harbor provisions to incentivize reporting by reducing legal exposure. Predicts improved transparency when notify-and-share is protected.

Cigref: Calls for clarified and aligned reporting responsibilities across actors. Clear role definitions reduce liability uncertainty and streamline incident handling.

Charter of Trust: Seeks clarified liability rules for reporting to remove barriers to disclosure. Legal certainty would support cooperative security practices.

SAP SE: Advocates liability protections to encourage vulnerability and incident disclosures. Assurances against legal risk would improve reporting quality and speed.

European Society of Radiology: Requests clearer deployer duties and reporting expectations in the regulatory framework. Role clarity helps ensure compliance without undue liability.

1.6.9 Miscellaneous

Under Unified Reporting & Incident Management, this Miscellaneous set highlights how fragmented, multi-layered regulatory regimes make reporting and remediation hard to navigate. Organisations face a patchwork of channels, formats, and timelines across EU and national instruments, alongside unclear expectations for conveying risk assessments and remediation to authorities. Persistent data hurdles—limited verification tools and scarce, hard-to-extract metrics—compound compliance workloads. Operational implications extend beyond internal processes: supply-chain relationships introduce additional reporting duties and vendor coordination, while insurers contend with frequent regulatory changes and specific laws that tie coverage to reporting obligations. Transparency and trust benefit from accessible outputs (e.g., dashboards and annual reports) to explain trends to policymakers and the public, even as stakeholders debate centralisation, language accessibility, and the strategic value of reporting. Across insights, priorities converge on clearer, simpler guidance, harmonised requirements, interoperable tooling, and machine-verifiable metrics—aimed at reducing friction, improving incident management, and enabling timely, consistent reporting across sectors and jurisdictions.

At the same time, we note that the current legislative framework remains, at times, challenging for organisations to navigate, given the variety of reporting channels, formats, and timelines across different regulatory instruments - spanning the European Digital Identity Framework, the General Data Protection Regulation, the Al Act, the NIS2 Directive, the Data Act, the Digital Operational Resilience Act, and more - at both EU and national levels. (Docusign)

there are concerns on how financial entities should convey remediation measures and risk assessments to competent authorities. (Assuralia)

In addition, the recent French LOPMI law8 imposes additional reporting obligations to law enforcement to maintain insurance coverage, adding further complexity to the compli- ance landscape. (FERMA - Federation of European Risk Managers Associations)

Furthermore, supply chain relationships introduce additional reporting obligations, requiring proactive communication with vendors across the supply chain. (European Cyber Security Organisation)

FERMA - Federation of European Risk Managers Associations: Highlights how frequent regulatory changes and new obligations to report incidents to law enforcement raise compliance complexity for insurers, affecting coverage terms and costs.

In addition, the recent French LOPMI law8 imposes additional reporting obligations to law enforcement to maintain insurance coverage, adding further complexity to the compli- ance landscape.

Assuralia: Calls for clear, simple guidance on how entities should communicate remediation measures and risk assessments to authorities, noting uncertainty about expectations.

There is no clear guidance of expectations.

Docusign: States the current reporting landscape is fragmented across multiple EU and national instruments with differing channels, formats, and timelines, making it hard for organizations to navigate.

At the same time, we note that the current legislative framework remains, at times, challenging for organisations to navigate, given the variety of reporting channels, formats, and timelines across different regulatory instruments - spanning the European Digital Identity Framework, the General Data Protection Regulation, the Al Act, the NIS2 Directive, the Data Act, the Digital Operational Resilience Act, and more - at both EU and national levels.

Adigital (Asociación Española de la Economía Digital): Points to practical hurdles in unified reporting: difficult data collection, lack of verification tools, and missing metrics that force costly internal processes.

Metrics required for compliance are not always readily available, forcing companies to carry out costly internal processes.

European Cyber Security Organisation: Emphasizes that supply chain relationships create extra reporting duties, necessitating proactive coordination with vendors.

Furthermore, supply chain relationships introduce additional reporting obligations, requiring proactive communication with vendors across the supply chain.

: Suggests using dashboards and annual reports to transparently present results and trend insights to policymakers and the public.

The results could be presented in dashboards and annual reports to explain trends to policy and public opinion.

Association des Constructeurs Européens de Motocycles: Recommends offering an English-language reporting option to reduce friction and support cross-border compliance.

Sdružení pro internetový rozvoj (SPIR): Argues that a transparency database would deliver minimal practical value for oversight.

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: Views reporting not only as a compliance task but as a strategic analysis tool to inform business decisions.

PensionsEurope: Opposes creating a centralized reporting hub, arguing existing regimes like DORA already provide sufficient structures.

Chamber of Commerce and Industry for Munich and Upper Bavaria: Proposes linking Digital Services Act complaint processes directly to specific user-generated content to improve incident handling.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Suggests incentivizing voluntary registration to encourage participation and improve reporting coverage without heavy mandates.

1.7 Privacy & Data Protection Modernization

The strongest throughline is a shift to a coherent, risk-based, and harmonized regime that rebalances away from blanket consent toward safeguarded legitimate interests, restores legal certainty across GDPR, ePrivacy, and adjacent laws, and enables responsible cross-border operations. Governance reforms seek predictable, proportionate enforcement: a procedural framework for cross-border cases, single reporting windows, greater reliance on codes and certifications, and advisory-first supervision to reduce needless DPIAs and delays. AI alignment prioritizes clear lawful bases, a safeguarded path for beneficial automated decisions, and practical guardrails—data minimization, early pseudonymisation/anonymisation, PETs, sandboxes, and transparent decision elements. Stakeholders ask for tighter, context-sensitive definitions and an actor-relative approach to de-identification and mixed datasets, aligned with sectoral rules (including biometrics). International transfers should be simpler and faster (streamlined BCRs, standardized instruments) with an explicit basis for intra-group special-category flows and fixes for extraterritorial gaps. Rights should remain effective yet scalable:

proportionate access handling, automation and signals (e.g., GPC), self-service dashboards, and paid equivalents that preserve free choice; clarify automated decision-making as a right with safeguards. Research and responsible data reuse need clearer recognition (algorithmic improvement, broader Article 89) and calibrated retention with oversight. Safety, security, and fraud prevention warrant proportionate processing, including flexible age verification, bounded by strict minimization, transparency, and due-process limits on third-party access. Cookies and tracking rules should cut banner fatigue through a GDPR-aligned, risk-based model that respects browser/OS preferences, exempts low-risk uses, and supports contextual ads. Additional updates span cybersecurity reporting, legal-basis clarity, and consumer transparency around location and profiling. Across categories, the common pattern is proportionality, harmonization, and predictability paired with practical user control. The goal is a modern framework that safeguards fundamental rights while enabling trustworthy innovation at EU scale.

1.7.1 Definitions, Scope & De-identification

Stakeholders advocate modernising GDPR's core definitions and scope to be clearer, narrower, and context-sensitive. They call for a more precise definition of personal data and practical guidance for mixed datasets and professional contexts (e.g., sole traders), to avoid overclassification. Several urge case-by-case, risk-based assessments that recognise when identification is not reasonably possible—such as technical telemetry or IP addresses used solely for cybersecurity—and for cross-regime alignment (e.g., biometric data across GDPR and the AI Act) and clarity on borderline inputs like prompts and AI training data. On de-identification, there is strong convergence on a relative, actor- and context-dependent standard: data should be considered anonymised when re-identification would require disproportionate effort, and pseudonymised data should be treated as non-personal for recipients who lack reasonable means or intent to re-identify. Stakeholders seek harmonised, practical criteria for anonymisation and pseudonymisation, clearer rules for mixed datasets, and actor-relative treatment of identifiers to enable low-risk reuse for research and innovation while safeguarding individuals. Some also propose scoping out processing whose purposes are unrelated to the data subject to reduce compliance burdens where personal linkages are not engaged.

> *A clearer definition of 'personal data' in Article 4(1) GDPR would help focus protection where it is truly needed and relieve companies whose aim is not to use personal data, but rather technical insights.* (Volkswagen Group)
>
> *Companies need reliable legal rules on when data is considered sufficiently anonymized and therefore no longer subject to the GDPR.* (German Insurance Association)
>
> *Some DPAs-such as Hamburg's-argue that once data is incorporated into an Al training dataset, it ceases to be personal data.* (Adigital (Asociación Española de la Economía Digital))
>
> *According to recent case law from the German Federal Court of Justice, documents or writings authored by the individual are considered personal data in their entirety, even if they are already known to the person.* (Verband kommunaler Unternehmen e.V.)
>
> **Verband kommunaler Unternehmen e.V.:** Critiques expansive case law that treats entire documents authored by an individual as personal data, questioning its practical value. Calls for a more balanced interpretation of what constitutes personal data.
>
> *According to recent case law from the German Federal Court of Justice, documents or writings authored by the individual are considered personal data in their entirety, even if they are already known to the person.*
>
> **Epic Systems:** Argues IP addresses used solely for cybersecurity are overclassified as personal data given minimal re-identification risk. Points to CJEU jurisprudence to scope them out where identification is not possible.
>
> *IP addresses are often treated as personal data despite minimal reidentification risk, especially when used solely for cybersecurity.*
>
> **ZVEI e.V.:** Calls for clear, harmonised rules for anonymisation and pseudonymisation. Endorses a relative approach where re-identification is only deemed possible if it is reasonably achievable without disproportionate effort.
>
> *ZVEI suggests, that anonymisation is based on a relative understanding, i.e. that anonymisation also exists if re-identification of the data subject is not completely excluded but is ruled out due to a disproportionately high effort.*

Technology Industries of Finland: Proposes scoping out processing unrelated to a data subject and treating such datasets as non-personal when actors lack means, interest, or intent to identify and safeguards prevent dissemination. Also suggests a quasi-controller category to better reflect actual roles.

This would allow processing as non-personal data if the processor has no means, interest, or intention to engage with the personal data aspect of the dataset and if the dissemination of the data is prevented through technical and organisational measures (e.g., industrial measurement data where the operator has no interest in possible traces of human activity).

: Advocates single controllership with most third parties acting strictly as processors on behalf of the consumer-facing business. Seeks clearer role delineation to reduce fragmentation.

With very rare exceptions, they should operate as data processors, working on behalf and only on behalf of the consumer-facing business who is then the single controller.

Volkswagen Group: Calls for clarifying GDPR material provisions, especially better anonymisation criteria and a sharper definition of personal data. Aims to focus protection where needed and relieve technical, non-personal insights.

A clearer definition of 'personal data' in Article 4(1) GDPR would help focus protection where it is truly needed and relieve companies whose aim is not to use personal data, but rather technical insights.

FEBIS: Highlights that professional activities of sole traders still fall under personal data, creating ambiguity at the personal–professional boundary. Warns this uncertainty hampers legitimate business data use.

Even when sole traders are clearly acting in a professional capacity-issuing invoices, registering with public authorities, or entering into commercial agreements, the data involved in these transactions is still personal data under GDPR.

Dun & Bradstreet: Seeks clearer distinction between personal and non-personal data, particularly for mixed datasets, to reduce legal ambiguity and compliance friction.

Clarification of the distinction between personal and non-personal data, particularly for mixed datasets, to reduce legal ambiguity.

German Insurance Association: Calls for reliable, practical, and harmonised criteria defining when data is sufficiently anonymised and thus outside the GDPR, aligning with other digital regulations.

Companies need reliable legal rules on when data is considered sufficiently anonymized and therefore no longer subject to the GDPR.

Airbus: Asserts pseudonymised data should not be treated as personal where recipients cannot reasonably re-identify individuals, to enable low-risk processing.

Clarify that pseudonymised data is not personal data when recipients cannot reasonably re-identify individuals.

Siinda: Urges differentiating sole traders' private versus professional capacities so that key professional data can be accessed and reused with proportionate GDPR obligations.

It would help to differentiate sole traders based on the capacity in which they interact : private capacity for personal use with full GDPR protection/ business capacity for professional use allowing access and re-use of key professional data items.

ENGIE: Requests clarity on when AI prompts constitute personal data and advocates a restrictive interpretation to avoid unnecessary GDPR burdens. Seeks coherent treatment between the AI Act and GDPR.

A restrictive interpretation would be preferred, limit unnecessary compliance obligations and reduce associated costs.

Ibec: Calls for clarifying limits on special category data and notes that pseudonymised data held by a third party may not always be personal. Aims to support research and fair, representative AI models.

The Advocate General (AG) of the Court of Justice of the European Union (CJEU) has opined that pseudonymised data in the hands of a third party may not always be considered "personal data" under the GDPR.

Finnish Food and Drink Industries´ Federation (ETL): Advocates limiting GDPR scope for temporary processing not linked to an identifiable individual and structuring pseudonymisation assessments. Suggests that removing identifiers should suffice so third-party data is no longer personal.

In the future, it should be sufficient to remove identifiers from datasets so that, for a third party, the data would no longer be considered personal data.

Adigital (Asociación Española de la Economía Digital): Notes positions that once data is incorporated into AI training datasets it may cease to be personal, urging clearer guidance for de-identified training data.

Some DPAs-such as Hamburg's-argue that once data is incorporated into an Al training dataset, it ceases to be personal data.

Panasonic Europe B.V.: Asks for actor-relative treatment of pseudonymised identifiers to streamline low-risk processing by regulated providers and trust services.

Clarify actorrelative treatment of pseudonymised identifiers to streamline lowrisk RP/QTSP processing.

ACEA (European Automobile Manufacturers' Association): Calls to align the definition of biometric data across the AI Act and GDPR to eliminate inconsistencies and ensure coherent scope.

The definition of biometric data in the AI Act is inconsistent with the definition established under the GDPR.

FEDIL, the Voice of the Luxembourg's Industry: Supports maintaining GDPR scope alongside clear safeguards, avoiding unnecessary expansion while preserving effective protection.

Insurance and Pension - Denmark: Stresses that strict limits on sensitive data hinder fairness assessments and seeks clearer pathways for compliant use under safeguards.

Under the GDPR, the use of sensitive data is strictly limited.

Business & Science Poland: Advocates narrowing the scope of special category data and exempting the use of public data where appropriate safeguards are applied.

carVertical: Urges easing GDPR constraints for VIN-related datasets, recognizing their often low identifiability and technical nature.

European Law Institute: Proposes exemptions for enterprise processing that does not identify individuals and for pseudonymised or anonymised data, alongside deregulating Article 9 where appropriate. Also suggests anti-discrimination extensions and exclusions for employee and billing-only data.

German Property Federation: Calls to deregulate anonymised data and clarify de-identification for energy-related datasets to enable lawful, low-risk use.

Bayerische Motoren Werke Aktiengesellschaft: Seeks alignment of biometric data definitions with the GDPR and clearer definitions of processing providers to resolve role ambiguities.

U.S. Chamber of Commerce: Calls to narrow GDPR’s application to remote or ancillary processing where identifiability and control are limited, refining scope.

FEDMA: Requests clear criteria to distinguish personal from non-personal data to ensure predictable compliance and data reuse.

Polish Confederation Lewiatan: Urges excluding or reclassifying entrepreneurs' professional data from GDPR to better reflect its business context.

Intesa Sanpaolo: Asks for clearer boundaries between personal and non-personal data to ease handling of mixed and technical datasets.

ITI - Information Technology Industry Council: Seeks clarity on third-party disclosure obligations and greater flexibility for pseudonymised data that is not reasonably re-identifiable.

ENCIRCLE Research Consortium: Calls for harmonised definitions of controller and processor roles to align legal responsibilities with practical realities.

Verband der Automobilindustrie e.V.: Requests a clearer, more targeted definition of personal data to focus protections and facilitate technical data processing.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Argues data that cannot reasonably be re-identified should be treated as non-personal, with clear, practicable criteria.

Google: Calls to clarify and narrow the scope of special category data to enable legitimate processing without undue burden.

Movement for an Open Web: Emphasises that identifiability should be assessed by reasonable means and context to avoid overclassification as personal data.

CLEPA: Proposes clearer role definitions and robust safeguards for de-identified data use within complex value chains.

Orgalim - Europe's Technology Industries: Advocates treating certain technical and pseudonymised datasets as non-personal under conditions that minimise re-identification risk.

Bayer AG: Supports farmer-controlled standards for secure anonymisation that clearly define when agricultural data falls outside GDPR.

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: Recommends allowing broader processing of pseudonymised data under safeguards where re-identification risk is negligible.

European Federation for Market Research Organisation (EFAMRO): Advocates case-by-case allocation of controller and processor roles and calls for harmonised pseudonymisation guidance with appropriate safeguards.

Insurance Europe: Endorses a relative anonymisation approach and clearer rules on when pseudonymised data falls outside the GDPR.

Audience Measurement Coalition (AMC): Seeks a definition that distinguishes audience measurement from analytics or targeting, narrowing obligations accordingly.

European Publishers Council: Urges clarity on the ePrivacy–GDPR overlap, trusted first-party distinctions, and a narrower ePrivacy scope to reduce unnecessary compliance.

SAP SE: Proposes broader lawful bases to process special category data under safeguards, easing constraints while maintaining protections.

Danish Industry: Recommends updating the personal data definition, enabling repurposing of de-identified and pseudonymised data, and exempting temporary processing unrelated to individuals. Suggests a new legal basis for using de-identified special category data.

DIGITALEUROPE: Argues pseudonymised data should not be personal where reasonable re-identification is ruled out and emphasises scalable use of de-identification as a key compliance tool.

AER - Association of European Radios: Supports permitting pseudonymised cross-device data use under strict safeguards, treating it as non-personal in certain contexts.

The European Crypto Initiative (EUCI): Calls for a technology-neutral, functional standard for anonymisation based on reasonable likelihood of re-identification.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Proposes safeguarded repositories and sandboxes to support anonymisation and responsible access without expanding personal data scope.

Esomar: Seeks clear allocation of GDPR roles in complex data chains and context-driven pseudonymisation guidance to manage risk.

Association Française des Entreprises Privées: Asks for clarification of core GDPR concepts, including the scope of personal data and thresholds for de-identification.

Cookie Information / Piwik PRO: Highlights the need to reconcile purpose limitation and data minimisation with workable de-identification to enable compliant analytics.

Confederation of Swedish Enterprise: Calls to clarify scope and de-identification to support innovation, ease constraints on special category data, and define when incidental intercom surveillance triggers GDPR obligations.

1.7.2 Regulatory Harmonization & Compliance Simplification

Stakeholders call for a risk-based, harmonized privacy and data protection framework that reduces fragmentation across the GDPR, ePrivacy, and sectoral rules (e.g., Data Act, AML, CRA, AI Act). They seek EU-level alignment and common standards to restore legal certainty for cross-border operations, streamline supervisory and incident reporting (e.g., via single reporting windows), and ensure consistent interpretation by regulators. Concrete simplifications include limiting notices to essential information, focusing record-keeping on high-risk processing, clarifying B2B vs B2C obligations, and aligning ePrivacy with the GDPR—without lowering the EU's high level of protection. Contributors emphasize that modernization should preserve fundamental rights while removing unnecessary burdens and conflicts, such as tensions between data-sharing mandates and GDPR, and uncertainties when data is both open and personal. Proposals range from targeted tweaks (e.g., Digital Omnibus clarifications) to bold reforms (e.g., repealing the ePrivacy Directive or expanding GDPR Article 9(2) for certain contractual health-data processing). The overarching goal is uniform implementation, reduced bureaucracy and legal uncertainty, and a framework that enables responsible innovation across the Single Market.

Furthermore, Connect Europe and the GSMA reiterate our full support for a considered simplification of the GDPR, which we believe would enhance legal certainty, reduce administrative burdens, and help to responsibly innovate without lowering the high level of data protection in the EU. (GSMA)

This fragmentation has created legal uncertainty and increased compliance burdens for cross-border business communications. (Mastercard Europe SA)

Telefónica calls for the complete repeal of the outdated ePrivacy Directive, which imposes disproportionate obligations solely on telecom operators. (Telefonica, S.A.)

According to the Data Act, Siemens would have to share this data with any external maintenance company, which leads to a dilemma: the data also contains information about which employee uses which room and when - personal data protected by the General Data Protection Regulation (GDPR). (SIEMENS AG)

Verband kommunaler Unternehmen e.V.: Advocates limiting data protection notices to essential information to reduce burden and enable uniform implementation across the EU.

The obligation to provide data protection notices should be limited to the most essential information, above all, to reduce the scope of content and promote uniform implementation in practice.

SIEMENS AG: Highlights conflicts between the Data Act data-sharing duties and GDPR protections and calls for harmonised rules to resolve compliance dilemmas.

According to the Data Act, Siemens would have to share this data with any external maintenance company, which leads to a dilemma: the data also contains information about which employee uses which room and when - personal data protected by the General Data Protection Regulation (GDPR).

ZVEI e.V.: Urges a clear distinction between B2C and B2B contexts and the removal of unnecessary bureaucracy in pure B2B processing.

Clear distinction between B2C and B2B - remove bureaucratic burdens in pure B2B business

Enel SpA: Supports streamlining personal data protection obligations across GDPR and related laws to reduce excessive regulatory burdens.

We appreciate the European Commission's initiative to streamline Personal Data Protection obligations through the Digital Omnibus package, and we welcome the effort to reduce the excessive regulatory burdens related to the General Data Protection Regulations (GDPR) and other related legislation (e.g. e-Privacy Directive).

Technology Industries of Finland: Calls for clear, harmonised rights for data holders to use data for diagnostics, R&D, quality and safety, reducing uncertainty and preserving innovation incentives.

Grant data holders rights to use data for diagnostics, R&D, quality and safety to preserve incentives for investment in data-driven innovation.

Volkswagen Group: Warns that unharmonised data legislation creates heavy compliance workload and diverts resources from innovation, underscoring the need for simplification and coherence.

The sheer volume of unharmonized data-related legislation has led to an unprecedented workload, consuming financial and human resources that could otherwise be invested in research, develop- ment, and innovation - all essential to maintaining global competitiveness.

France Digitale: Requests clarifications on how to treat datasets that are both open and personal to ensure consistent, harmonised compliance.

The Open Data Directive plays a central role here but still requires clarifications: when data is both open and personal, how should it be treated?

Unipol Assicurazioni S.p.A.: Proposes amending the GDPR to add a contractual necessity exemption for health data, promoting consistency and reducing fragmentation.

Hence, we call on the European Commission to take the opportunity of issuing a Digital Omnibus Package to promote greater consistency across the EU by amending Article 9(2) of the GDPR to introduce a new exemption for the processing of health data where it is necessary for the performance of a contract.

German Insurance Association: Seeks reductions in bureaucracy, legal uncertainty, and administrative burden under the GDPR to simplify compliance.

Reduce bureaucracy, legal uncertainty and administrative burden under the GDPR.

GSMA: Advocates a considered simplification of the GDPR to enhance legal certainty and reduce burdens while maintaining high protection standards.

Furthermore, Connect Europe and the GSMA reiterate our full support for a considered simplification of the GDPR, which we believe would enhance legal certainty, reduce administrative burdens, and help to responsibly innovate without lowering the high level of data protection in the EU.

Telefonica, S.A.: Calls for repealing the outdated ePrivacy Directive to eliminate disproportionate sector-specific obligations and improve harmonisation.

Telefónica calls for the complete repeal of the outdated ePrivacy Directive, which imposes disproportionate obligations solely on telecom operators.

Bitkom e.V.: Recommends a holistic reform of the ePrivacy Directive so it aligns with the broader data protection framework rather than focusing only on cookies.

The reform of the outdated ePrivacy Directive should take a holistic approach, addressing the entire directive - not just the cookie rule - as its isolated, sector-specific design no longer fits within today's broader data protection and digital legal framework.

Civil Liberties Union for Europe: Supports targeted, risk-based adjustments such as limiting records of processing to high-risk activities, simplifying compliance without weakening core principles.

We agree with the European Data Protection Board (EDPB) when it refers to potential "modifications to the GDPR to simplify and clarify the obligation to keep a record of processing are targeted and limited in nature and do not affect the core principles and other obligations under the GDPR" and their support to clarify in the recitals that a record of processing would only be mandatory for those processing activities "likely to result in a high risk".

Schibsted Media: Backs harmonisation and a risk-based approach aligning ePrivacy with the GDPR to simplify EU digital privacy rules.

We welcome the Commissions efforts to simplify and harmonise EU digital rules and support a risk-based approach that aligns the ePrivacy Directive with the GDPR.

Mastercard Europe SA: Notes that regulatory fragmentation increases legal uncertainty and compliance costs for cross-border communications and urges harmonisation.

This fragmentation has created legal uncertainty and increased compliance burdens for cross-border business communications.

Centre for Information Policy Leadership (CIPL): Identifies divergent interpretations and inconsistencies across GDPR and other laws, calling for coherent, harmonised guidance and transfer rules.

For example, there is a diverging interpretation of some GDPR concepts across regulators, undue complexity regarding international data transfers, and inconsistencies with other EU digital, sectoral, and national laws.

Leading Baltic tech and other businesses and professional associations listed in the submission: Emphasises that any harmonisation or simplification must preserve strong privacy and fundamental rights protections.

We strongly support the EU's commitment to protection of privacy and other fundamental rights and these core principles in no case should be undermined.

Sheridans, on behalf of Awin AG: Highlights regulatory confusion around programmatic advertising and seeks clearer, harmonised rules to reduce delays and contracting frictions.

Confusion with programmatic advertising is a constant challenge when developing new business and causes delays to contracting with advertisers and the launching of their campaigns.

LSEG: Urges resolving tensions between the GDPR and sectoral frameworks such as AML to provide consistent, simplified compliance expectations.

Simplification efforts should address growing tensions between GDPR and sectoral rules like the EU AML package.

The International Center for Law & Economics: Criticises the omission of GDPR reform from the consultation and calls for meaningful simplification of the privacy regime.

The consultation omits GDPR reform, despite the Commission's commitment to assess the digital acquis; this represents a missed opportunity for meaningful simplification.

Schneider Electric: Asks to streamline overlapping cybersecurity and personal data breach reporting requirements across existing and new regulations.

Streamlining cybersecurity and personal data breach reporting requirements (see section I. iii.), especially with new regulations like the CRA and the AI Act.

Meta Platforms Ireland Limited: Calls to modernise and harmonise the EU privacy regime to better enable responsible, innovation-driven activity.

Privacy & Data Protection - Reform the EU Data Protection and Privacy regime to create a modernised and innovation driven framework

Finnish Food and Drink Industries´ Federation (ETL): Urges revisiting the GDPR to ensure it facilitates data flows and utilisation rather than hindering them, while maintaining protection.

The GDPR should be revisited to ensure it does not hinder the smooth flow and utilization of data.

ING Group: Advocates relying on EU-level frameworks to avoid national divergence, clarifying data minimisation interactions, and harmonising supervisory reporting.

Data: Rely on EU-level frameworks like GDPR to avoid conflicting national rules, clarify how data minimisation interacts with other regulations, and harmonise supervisory reporting through a Single Reporting Window.

Anitec-Assinform: Calls for common GDPR compliance standards to ensure consistent, harmonised application across organisations.

We also call for ensuring common GDPR compliance standards across all organizations.

Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg: Notes that the GDPR and its interplay with other legal acts need clarification and improvement to reduce complexity.

The third point is the GDPR: The GDPR itself and its interaction with other legal acts still require improvement and clarification.

Doctrine: Warns against overly broad privacy claims blocking publication and calls for clearer, proportionate rules to harmonise practice with safeguards.

Third, administrations frequently invoke privacy as a reason to block publication, even when proportionate safeguards or anonymisation techniques exist.

American Chamber of Commerce to the EU: No specific information about regulatory harmonization or compliance simplification was provided in the available material.

1.7.3 Enforcement & Governance Modernization

Enforcement & Governance Modernization aims to make GDPR oversight more predictable, proportionate, and innovation-friendly while preserving strong protections. Stakeholders call out nonbinding and opaque guidance (including EDPB processes) and broad DPA discretion that fosters privacy absolutism and uncertainty, leading to defensive, redundant DPIAs and delayed technologies. They also flag impractical obligations (e.g., strict 72-hour incident reporting) and fragmented cross-border procedures, as well as ambiguity from nonbinding opinions in areas like cookies. Proposed governance upgrades include a distinct Procedural Regulation to harmonise cross-border enforcement without reopening the GDPR, predictable certifications through prior consultations, stronger use and promotion of Codes of Conduct and certification schemes, and streamlined supervisory reporting via a Single Reporting Window. To improve fairness and efficiency, stakeholders suggest pre-complaint notification mechanisms for early resolution, greater investigative transparency from DPAs (e.g., sharing complaint summaries), and an advisory-first approach that reduces fines by preventing ongoing non-compliance. Better coordination between the Commission and EDPB, clearer controller/processor roles, and main-establishment clarifications are also sought. To embed proportionality, proposals include making the GDPR's balancing of fundamental rights an explicit core principle and introducing multidisciplinary tribunals that can weigh privacy alongside innovation and economic goals. Pragmatic enforcement (e.g., CNIL's approach), PETs and centralized "set-and-forget" privacy signals, and alignment with cybersecurity aims are highlighted as practical pathways to reduce burdens while enhancing trust and consistency across the EU.

The GDPR Procedural Regulation is a separate piece of legislation designed to harmonise enforcement procedures for cross-border cases, maintaining the GDPR's core principles intact while addressing procedural shortcomings. (Technology Industries of Finland)

introduce transparency measures that the DPAs must adopt towards the data controllers and processors during the investigation process, for instance, when an investigation is initiated based on a complaint, the DPA should provide the data controller or processor with a summary of the complaint, including: the nature of the alleged violation, the categories of data involved, the relevant time frame, and access to the text of the complaint in anonymized form. (Enel SpA)

Ideally, abolish the reporting obligation entirely. (Verband kommunaler Unternehmen e.V.)

Current enforcement treats privacy as supreme over all other EU objectives, contradicting both the GDPR's own proportionality principles and broader EU economic goals. (The International Center for Law & Economics)

Verband kommunaler Unternehmen e.V.: Advocates scaling back breach notification duties—limiting or abolishing the 72-hour obligation and focusing on serious incidents—to reduce administrative burden and improve proportional enforcement.

Ideally, abolish the reporting obligation entirely.

Neogy.cz: Highlights that nonbinding DPA/EDPB opinions create legal uncertainty, calling for clearer, binding guidance and predictable enforcement.

According to the law firm Elegal (source), both the European Data Protection Board (EDPB) and ÚOOÚ opinions are not legally binding-the final interpretation lies with the courts.

Epic Systems: Warns that fear-driven, redundant DPIAs slow deployment of similar technologies, urging clearer, risk-based enforcement to avoid unnecessary re-evaluations.

Fear of GDPR penalties leads organizations to conduct redundant DPIAs and delay new technologies, even for similar data uses.

Enel SpA: Proposes a pre-complaint notification step and greater DPA investigation transparency to resolve issues early and reduce caseload while ensuring due process.

introduce a pre-complaint notification mechanism whereby data subjects, prior to lodging a formal complaint to the competent DPA, would be required to notify the data controller or processors of the alleged violation and allow a short period for a response or remediation.

Technology Industries of Finland: Calls for prior consultation to yield official certifications for predictable compliance and for keeping the Procedural Regulation separate to modernize enforcement without reopening the GDPR.

The prior consultation procedure with the supervisory authorities should lead to official certification confirming that the proposed activity meets data protection standards, when that is the case Authorities would be required to evaluate such consultations and issue certifications where appropriate based on the information provided.

: Argues that current application of GDPR and ePrivacy undermines competition and only benefits adtech intermediaries, urging modest enforcement reforms to boost privacy and EU media.

However, a modest revision of how the GDPR and ePri- vacy Directive are applied is sufficient to address the issue and deliver both a major win for privacy and a boost to European consumer-facing businesses, particularly the ad-supported media.

Video Games Europe: Supports targeted adjustments and harmonization of GDPR application via the Digital Omnibus to restore consistency and reduce business burdens.

While Video Games Europe does not support a full reopening of the GDPR, minimal adjustments in the context of the upcoming Digital Omnibus could bring some relief and clarity.

ING Romania: Urges EU-level harmonization and clarification (e.g., data minimization vis-a-vis other rules) and a Single Reporting Window to streamline supervisory reporting and enforcement.

Rely on EU-level frameworks like GDPR to avoid conflicting national rules, clarify how data minimisation interacts with other regulations, and harmonise supervisory reporting through a Single Reporting Window.

The International Center for Law & Economics: Critiques an enforcement framework that privileges privacy absolutism and uncertainty, proposing proportionality-centered governance such as independent, multidisciplinary tribunals.

The core problem is not the GDPR's text, but its enforcement structure, which fosters privacy absolutism by enabling data-protection authorities (DPAs) to act as both prosecutor and judge with near-limitless discretion.

Meta Platforms Ireland Limited: Advocates embedding fundamental-rights balancing at GDPR's core to guide proportionate enforcement that supports innovation and growth.

Move Recital 4 (balancing rights) into Article 1: Make the duty to balance fundamental rights arising from the Charter an explicit core principle in the GDPR.

egta - the international trade body of multiplatform TV and audio businesses: Seeks greater coherence in the EU privacy framework through improved coordination between the Commission and EDPB to ensure consistent enforcement.

Finally, in order to ensure legal certainty and good administration, a better and clearer coordination between the European Commission and the European Data Protection Board (EDPB) is crucial, as it would foster a consistent interpretation of the rules and enhance their proper enforcement across all Member States down the line.

Adigital (Asociación Española de la Economía Digital): Encourages active DPA promotion of Codes of Conduct and a collaborative, advisory-first approach to reduce fines and prevent persistent non-compliance.

Second, it proposes greater interaction between data protection agencies and private entities to avoid imposing fines through prior advisory on areas needing improvement, thereby preventing ongoing non-compliance and limiting the number of fines.

American Chamber of Commerce to the EU: Recommends expanding and clarifying main-establishment jurisdiction to strengthen the one-stop-shop and deliver more consistent cross-border enforcement.

European Law Institute: Calls to clarify controller-processor responsibilities and governance to improve accountability and facilitate effective, coordinated enforcement.

: Urges limiting joint controllership and reinforcing Article 26 arrangements to clarify roles, liability, and enforcement focus.

IBM: Supports harmonizing and extending the main-establishment concept to streamline cross-border supervision and modernize enforcement.

Verband der Automobilindustrie e.V.: Advocates streamlining GDPR rules and procedures and introducing a group privilege for intra-group data sharing to reduce enforcement friction.

TikTok Technology Ltd.: Proposes a structured assessment of GDPR's impacts to identify targeted enforcement and governance improvements.

eyeo GmbH: Calls for enforceable, centralized set-and-forget privacy signals to simplify compliance and enable consistent enforcement.

Google: Promotes recognition of privacy-enhancing technologies in enforcement to mitigate risks and reduce the need for intrusive corrective measures.

Movement for an Open Web: Highlights opaque EDPB processes and expansive interpretations, urging more transparent governance and narrower, predictable enforcement.

Orgalim - Europe's Technology Industries: Recommends streamlining codes of conduct and accelerating DPA certifications to deliver legal certainty and uniform enforcement.

Renault Group: Supports ex-ante impact assessments of new measures to calibrate proportional enforcement and reduce unintended burdens.

Global Data Alliance: Urges greater use of underutilized GDPR tools (codes, certifications, BCRs) to provide predictable compliance pathways and harmonized enforcement.

Audience Measurement Coalition (AMC): Advocates audited, transparent audience measurement under strict non-profiling controls, aligning enforcement with proportional, purpose-limited practices.

Alliance Digitale: Proposes minimal guarantees by large controllers to underpin a compliant ad ecosystem and enable targeted, risk-based enforcement.

Österreichische Notariatskammer: Welcomes secure digital identification services as governance infrastructure that supports compliant processing and facilitates efficient enforcement.

: Calls to clarify accountability for consent/banner providers to focus enforcement on responsible actors and improve real-world compliance.

DIGITALEUROPE: Supports enabling ongoing personal data monitoring with clear safeguards to align enforcement with operational needs and accountability.

AI Accountability Lab (AIAL), Trinity College Dublin: Recommends reducing administrative burdens and simplifying enforcement mechanisms to improve compliance without stifling innovation.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Proposes a presumption of compliance for controllers meeting defined criteria to reduce uncertainty and streamline enforcement.

CrowdStrike: Urges enforcement that recognizes the complementarity of data protection and cybersecurity, enabling effective threat defense within GDPR.

European Games Developer Federation (EGDF): Calls for harmonized GDPR enforcement across Member States to reduce fragmentation and support innovation in the games sector.

Confederation of Swedish Enterprise: Seeks streamlined delineation of GDPR roles and better authority coordination to modernize governance and ensure consistent enforcement.

1.7.4 International Transfers & Extraterritoriality

Stakeholders call for streamlined, harmonized, and predictable GDPR mechanisms for international data transfers. Binding Corporate Rules (BCRs) are viewed as too slow and burdensome; there are calls to accelerate approvals and confine requirements to the essentials of Article 47, alongside greater consistency across supervisory authorities and standardization of contractual instruments and intra-group frameworks. A recurring pain point is intra-group processing of special-category data: legitimate interests cannot serve as a basis and consent is often impractical and trust-eroding, prompting proposals for an explicit GDPR legal basis for such intra-group flows. Contributors also flag gaps affecting entities caught by GDPR's extraterritorial reach under Article 3(2), urging simplified accountability and transfer frameworks that close these mechanism shortfalls while maintaining high protection standards.

Above all, the lengthy approval process makes BCRs increasingly unattractive in practice as a tool for data transfers to third countries within corporate groups. (German Insurance Association)

Scale back BCR requirements to what is strictly required by Article 47 GDPR. (German Insurance Association)

Obtaining consent from all customers is im- practical and would also unnecessarily strain customer relations: frequent consent requests feel disruptive, and rode trust-especially without clear benefit. (German Insurance Association)

Article 6(1)(f) GDPR cannot justify processing sensitive data and therefore cannot serve as a legal basis in such cases. (German Insurance Association)

German Insurance Association: Argues that Binding Corporate Rules for intra-group third-country transfers are hampered by lengthy approvals and excessive requirements, urging acceleration and limiting obligations to Article 47 GDPR. Calls for a specific GDPR legal basis for intra-group processing of special-category data, noting consent is impractical and legitimate interests cannot support such processing.

Above all, the lengthy approval process makes BCRs increasingly unattractive in practice as a tool for data transfers to third countries within corporate groups.

American Chamber of Commerce to the EU: Calls to simplify and harmonize GDPR accountability and international transfer mechanisms to lower compliance burdens and increase legal certainty for cross-border operations.

German Property Federation: Advocates standardized data processing agreements and consistent intra-group transfer rules to support predictable, efficient international data flows within corporate groups.

Johnson & Johnson: Urges EU-wide harmonization and clearer guidance on data transfer requirements to reduce fragmentation and enable compliant global data movements.

Danish Industry: Highlights gaps in available transfer tools for entities subject to GDPR under Article 3(2) and seeks tailored solutions or clarifications to enable lawful international transfers.

1.7.5 Risk-Based Processing & Legitimate Interests

Stakeholders call for a shift from prohibition or consent-centric rules toward a genuinely risk-based, proportionate model that relies more confidently on legitimate interests with appropriate safeguards, transparency, and a right to object. They seek clearer, authoritative guidance on when legitimate interest can be used—especially for AML/sanctions screening, security, product development, and AI training—alongside support for intra-group data transfers where data subjects' overriding interests are respected. They highlight that current practice often treats processing as inherently risky and provides little relief for low-risk use cases, making the balancing test particularly challenging for SMEs and compounding legal complexity when GDPR intersects with the AI Act. Proposed adjustments include recognizing legitimate interest for advertising and AI training, streamlining B2B information duties, and embedding proportionality to preserve free movement of data while safeguarding fundamental rights.

Move from a prohibition-based to a risk-based approach. (ZVEI e.V.)

It is important to note that the legitimacy of these purposes is not in question, provided that the processing is proportionate and subject to appropriate safeguards. (CNIL (French Data Protection Authority))

It proposes the simplification across all industries, not just SMEs, and recognizing AI training as a legitimate interest under GDPR, with safeguards such as pseudonymization & transparency. (Telefonica, S.A.)

When authorities interpret "necessity" to exclude economic or business necessities, such as revenue generation, they effectively undermine sustainable business models upon which European consumers may rely. (The International Center for Law & Economics)

Verband kommunaler Unternehmen e.V.: Supports intra-group personal data transfers for internal administration under legitimate interests, subject to an overriding data-subject interests test.

Controllers that are part of a corporate group or a group of entities assigned to a central body shall be permitted to transfer personal data within the group, particularly for internal administrative purposes, including the processing of personal data of customers and employees, unless the legitimate interests of the data subjects override this.

ZVEI e.V.: Urges a shift from prohibition-centric rules to a risk-based model that calibrates obligations to actual privacy risks.

Move from a prohibition-based to a risk-based approach.

CNIL (French Data Protection Authority): Affirms that certain purposes can rely on legitimate interests if processing is proportionate and protected by appropriate safeguards.

It is important to note that the legitimacy of these purposes is not in question, provided that the processing is proportionate and subject to appropriate safeguards.

Technology Industries of Finland: Highlights that conducting the legitimate interests balancing test is especially challenging for SMEs and calls for clearer, simpler guidance.

The balance test required to rely on legitimate interest poses significant challenges for SMEs.

Volkswagen Group: Calls to review and adapt data protection rules with stronger emphasis on risk-based proportionality to enable data flows while protecting fundamental rights.

To ensure the free movement of data while safeguarding fundamental rights, data protection rules should be critically reviewed and adapted with greater emphasis on the risk-based and proportionality principles embedded in the GDPR.

EMMA-ENPA: Advocates permitting processing for advertising on the basis of legitimate interest combined with transparency and a right to object.

Moreover, and as a real tool to simplify rules for European digital industries, the Commission should consider allowing data processing, including for advertising purposes, on the basis of legitimate interest, coupled with an obligation to inform and a right to object.

FEBIS: Seeks recognition of legitimate interest for business information providers to access and reuse public sector data for credit, fraud prevention, KYC, KYB, and AML.

The need to better streamline EU regulations and national implementation applying to access and re-use of public sector data by BIPs with a spotlight on the recognition of the legitimate interest of BIPs to access public sector data, (both PSI and non-PSI) for purposes of credit scoring, fight against fraud, KYC and KYB and AML.

Dun & Bradstreet: Emphasizes the importance of legitimate interest as a lawful basis for processing in business contexts under GDPR Article 6(1)(f).

In this context, we wish to highlight the importance of recognising legitimate interest as a lawful basis for data processing under Article 6(1)(f) of the General Data Protection Regulation (GDPR).

German Insurance Association: Proposes risk-proportionate transparency obligations by exempting B2B partners and their employees from GDPR Articles 13 and 14 to reduce unnecessary burden.

To avoid unnecessary bureaucratic burden and overwhelming data subjects with information, the disclosures required under Articles 13 and 14 GDPR should not apply in the B2B context to business partners and their employees.

GSMA: Notes overlapping GDPR and AI Act requirements create legal complexity, suggesting more coherent, risk-based alignment.

The concurrent application of the GDPR and the AI Act raises substantial legal complexities and hurdles that we believe could be better addressed.

Telefonica, S.A.: Recommends cross-industry simplification and recognizing AI training as a legitimate interest with safeguards like pseudonymization and transparency.

It proposes the simplification across all industries, not just SMEs, and recognizing AI training as a legitimate interest under GDPR, with safeguards such as pseudonymization & transparency.

Airbus: Calls to reinforce legitimate interest as a basis for processing in product development, AI model building, and security.

Reinforce the use of 'legitimate interest' as a ground to process personal data for key use cases such as product development - including Al models - and security.

Centre for Information Policy Leadership (CIPL): Argues that overreliance on consent burdens individuals and weakens privacy, endorsing more appropriate bases such as legitimate interests.

Similarly, CIPL's work on appropriate legal bases for data processing demonstrates that the continued preference of consent, often required across multiple digital laws, has created an unsustainable model that puts an undue burden on the individual and ultimately weakens privacy protections.

Leading Baltic tech and other businesses and professional associations listed in the submission: Criticizes approaches that presume data processing is inherently risky, urging a more balanced risk-based framework that enables innovation.

It leads regulators to treat data processing as inherently risky, resulting in an overly restrictive approach that hinders innovation and lawful data use.

LSEG: Requests authoritative guidance on when legitimate interest can be used, particularly for AML, sanctions, and risk screening.

Without authoritative interpretation from EU institutions data protection authorities, organisations face uncertainty about when and how legitimate interest can be relied upon, particularly in the context of AML, sanctions, and risk screening.

The International Center for Law & Economics: Warns that excluding economic necessities from the necessity test undermines viable business models and calls for pragmatic interpretation.

When authorities interpret "necessity" to exclude economic or business necessities, such as revenue generation, they effectively undermine sustainable business models upon which European consumers may rely.

Meta Platforms Ireland Limited: Asserts that rapid data-driven innovation exposes gaps in current rules, supporting modernization grounded in risk-based principles.

However, rapid technological change and the rise of data-driven innovation have exposed significant shortcomings in this regulatory framework.

FiCom ry: Observes that GDPR's risk-based approach often fails to reduce obligations in low-risk cases, calling for more proportionate treatment.

At the moment, the risk-based approach in the GDPR does not substantially decrease regulatory requirements even in low-risk cases.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Stresses the need for effective, practicable data protection to support digitalization, implying a balanced, risk-based approach.

Effective and practicable data protection is an important requirement for a functioning digitalisation.

1.7.6 Consent, Cookies & ePrivacy Modernization

There is broad agreement that EU rules on cookies and similar tracking set under ePrivacy are outdated, fragmented, and overly consent-centric, resulting in banner fatigue, poor user experience, and compliance burdens. Stakeholders urge simplification and coherence with GDPR (including one-stop-shop oversight), clearer allocation of roles between frameworks, and modernization that respects browser/OS-level preference signals while prohibiting invasive cross-site tracking. The aim is a clear, practical, and future-proof regime that preserves privacy, trust, and business sustainability without duplicative obligations. A risk-based model is preferred: reserve consent for higher-risk purposes and create targeted exemptions for low-risk or essential uses such as first-party analytics, security/integrity telemetry, fraud prevention, simple audience measurement, and certain B2B marketing with straightforward opt-out. Calls include reducing purpose granularity, recognizing contextual advertising as privacy-preserving, treating analytical cookies like technical ones under defined conditions, and enabling legitimate-interest or opt-out pathways where appropriate—thereby cutting consent prompts while maintaining transparency and user control.

EU's rules on cookies and other tracking technologies laid down by the ePrivacy Directive should be simplified. (Amazon)

The DSV therefore welcomes the Commission's plans to modernise outdated cookie and tracking rules, thus simplifying consent processes. (German Social Insurance European Representation)

Remove Article 5(3) cookie provisions and rely on the GDPR's more flexible framework, eliminating duplicative requirements and the overly restrictive binary-consent model that lacks "legitimate interest" provisions. (The International Center for Law & Economics)

Modernise ePrivacy to end banner fatigue with a narrow consentfree basis for firstparty measurement using privacyenhancing techniques and for strictly necessary security/integrity telemetry, with an explicit ban on crosssite tracking and recognition of verifiable browser/OS preference signals. (Panasonic Europe B.V.)

Neogy.cz: Proposes shifting cookie and tracking preference decisions from individual websites to browser or device-level settings to reduce banner fatigue and centralize user control.

We recommend that the decision about cookie and tracking preferences be moved from individual websites to the users browser or device settings.

: Calls to eliminate cookie consent banners to improve the browsing experience.

Stop this cookie bars!

Kaspersky Labs Limited: Argues the current consent framework has become a box-ticking exercise with little user benefit and high business friction, urging meaningful reform.

The current framework, while well-intentioned, has evolved into a compliance exercise that offers limited benefits to users and imposes significant friction on businesses.

CNIL (French Data Protection Authority): Supports retaining the ePrivacy structure while adding targeted, legitimate exemptions rather than overhauling the framework.

We consider that future regulatory developments should primarily focus on the integration of new, targeted and legitimate exemptions for which we put forward concrete proposals, rather than on modifying the fundamental structure of the ePrivacy framework

Enel SpA: Advocates a GDPR exemption whitelisting processing of personal communications data for technical purposes and simple statistics without consent.

It could be appropriate to make an exemption in the GDPR, whitelisting the processing and storage of personal communications data for technical purposes and for simple statistics.

Technology Industries of Finland: States the ePrivacy Directive is outdated and that efforts to replace it failed, underscoring the need for modernization.

The existing ePrivacy Directive is outdated and the attempt to replace it with an ePrivacy regulation failed.

PHOENIX group: Says EU cookie consent mechanisms are overly complex and harm patient experience, calling for simplification.

Current cookie consent mechanisms in the EU are overly complex and lead to a suboptimal patient experience.

: Warns that excessive consent granularity undermines simplicity and usability, advocating streamlined choices.

Experience shows that granularity is the enemy of simplicity.

Encode Europe: Encourages support for contextual advertising as a privacy-friendlier, resource-efficient option that can still deliver performance.

Fifthly, for the upcoming Digital Fitness Check of Consumer Laws, we would welcome recommendations in the field of contextual advertising, which reduces pressure on data centers & computing power, improves privacy and research shows it leads to higher conversion for commercial parties.

Volkswagen Group: Criticizes consent-only interpretations that have distorted ePrivacy, creating inconsistencies with GDPR and hindering the IoT economy.

This has resulted in absolutist interpretations which de facto has transformed the ePD regime in a "con- sent-only" regime incoherent with other laws including the GDPR and the Data Act and incompatible with activities that are inherent to how the Internet works and how the Internet of Things economy can be developed.

eco - Verband der Internetwirtschaft e.V.: Opposes new or tighter rules and instead seeks clarification on the use of technical cookies.

This stated, eco does not see the necessity to establish new or tighter regulation and instead vows for a clarification on the deployment of technical cookies.

EMMA-ENPA: Proposes simplifying consent by limiting purposes requiring consent, reducing granularity, and streamlining information.

Nonetheless, simplification could to some degree be achieved by limiting the purposes for which consent is required, the level of granularity and the information to display.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Endorses consent exemptions for low-risk uses like analytics and fraud detection when they pose no risk to data subjects.

Moreover, when data uses do not pose a risk to data subjects, like analytics or detecting and combatting fraud, such uses could be conducted without consent.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Requests clearer guidance on how ePrivacy rules interact with other legal frameworks, particularly for AI use cases.

Clarify the interaction with ePrivacy.

Government Office of the Czech Republic: Notes that cookie and tracking rules protecting terminal equipment are outdated and need modernization.

The use of cookies and other tracking technologies is governed by outdated rules that regulate the protection of users' terminal equipment and access to, as well as the collection of, data from such devices.

Telefonica, S.A.: Calls for elaborating ePrivacy Article 5 to introduce specific processing exemptions.

Secondly, Article 5.1 and 5.2 provisions should be further elaborated to allow specific exemptions that permit its processing.

World Federation of Advertisers: Urges targeted consent exemptions for low-risk marketing and a risk-based, principles-driven approach consistent with the GDPR.

The Digital Omnibus offers an important opportunity to introduce targeted consent exemptions for low-risk but essential marketing functionalities and to embed a more risk-based, principles-driven approach to consent and data processing consistent with the GDPR.

Amazon: Supports simplifying EU rules on cookies and other tracking technologies under the ePrivacy Directive.

EU's rules on cookies and other tracking technologies laid down by the ePrivacy Directive should be simplified.

German Social Insurance European Representation: Welcomes modernization of outdated cookie and tracking rules to simplify consent processes.

The DSV therefore welcomes the Commission's plans to modernise outdated cookie and tracking rules, thus simplifying consent processes.

Seznam.cz, a.s.: Argues first-party analytical cookies should be treated like technical cookies and not require consent under clear conditions.

We believe that, under clearly defined conditions, analytical cookies should be treated in the same way as technical cookies and not require user consent.

Schibsted Media: Asserts overlapping cookie and tracking rules are not fit for purpose and require reform.

The existing overlapping framework and in particular the rules governing the use of cookies and similar technologies, are not fit for purpose.

Mastercard Europe SA: Calls for a harmonized, practical framework with straightforward B2B opt-out, proportionate consent requirements, and coverage of emerging channels.

Any future legislative initiative aimed at harmonizing these rules should ensure a clear and practical framework, including a straightforward opt- out mechanism for B2B marketing, proportionate consent requirements, and coverage of emerging communication channels not explicitly addressed under the current Directive.

BEUC - The European Consumer Organisation: Supports reducing consent prompts via targeted exceptions for low-risk purposes like first-party analytics while safeguarding privacy.

This is done while also aiming to reduce the number of consent requests encountered by users through the inclusion of new targeted exceptions for purposes that should not pose privacy risks (e.g. first party web analytics).

Leading Baltic tech and other businesses and professional associations listed in the submission: Challenges extending marketing restrictions to B2B communications, arguing they pose minimal data protection risks.

The current outdated ePrivacy version extends marketing restrictions to business-to- business (B2B) communications, which do not pose data protection risks.

Sheridans, on behalf of Awin AG: States cookies are necessary for advertisement performance measurement and should be accommodated accordingly.

In order to measure how an advertisement has performed, it is necessary to use cookies:

European Tech Alliance: Highlights complexity from dual GDPR and ePrivacy regimes and national transposition, calling for better alignment.

The data protection and privacy regulatory framework is based on two separate legal instruments that both regulate the use of data from different perspectives: (1) the GDPR regulating the processing of personal data, directly applicable in national laws and (2) the e-Privacy Directive regulating the placing and reading of information (cookies) on a user's device that is transposed in 27 different national laws.

Ibec: Recommends integrating cookie rules into GDPR and aligning oversight with the one-stop-shop model.

ePR rules on cookies should be integrated to GDPR and align with the one stop shop approach to oversight.

The International Center for Law & Economics: Recommends removing ePrivacy's cookie provisions and relying on GDPR's flexible bases, including legitimate interests.

Remove Article 5(3) cookie provisions and rely on the GDPR's more flexible framework, eliminating duplicative requirements and the overly restrictive binary-consent model that lacks "legitimate interest" provisions.

ISP Alliance a.s.: Advocates returning to an opt-out or more flexible model to simplify compliance, especially for small sites.

We believe that a return to an opt-out system (or at least a more flexible system) would represent a significant simplification, especially for small website operators.

AIM - European Brands Association: Supports a risk-based approach and opposes generic browser-level consent that could undermine consumer choice and publishers.

A risk-based approach to consumer consent, rejecting rigid or browser-level consent mechanisms that are overly generic, ineffective, and risk undermining consumer choice and responsible publishers.

Meta Platforms Ireland Limited: Warns that over-reliance on consent fuels fatigue and operational uncertainty, hindering IoT, safety uses, and PETs.

A major source of complexity is the ePD's over-reliance on consent, leading to a proliferation of consent requests, user fatigue, and operational uncertainty that hinders the development of the Internet of Things ("loT") and the Data Act's goals, prevents safety and integrity data uses and PETs, and creates distrust in the technology.

: Expresses user frustration with frequent, granular cookie choices and the time burden they impose.

I am very harassed and I have no time or taste to explore individual cookies.

egta - the international trade body of multiplatform TV and audio businesses: Calls for reforms that maintain proportionality and coherence while ensuring future-proof, trust-enhancing solutions.

This exercise however must ensure that the proportionality and coherence of existing legislations are maintained, while providing for future-proof solutions guaranteeing business sustainability, privacy and user trust.

Vodafone Group: Proposes recasting limited ePrivacy provisions into other laws and repealing the ePrivacy Directive.

Recast limited ePrivacy provisions into relevant legislation and repeal the ePrivacy Directive.

Panasonic Europe B.V.: Suggests ending banner fatigue via narrow consent-free bases for first-party measurement and security telemetry, banning cross-site tracking, and honoring preference signals.

Modernise ePrivacy to end banner fatigue with a narrow consentfree basis for firstparty measurement using privacyenhancing techniques and for strictly necessary security/integrity telemetry, with an explicit ban on crosssite tracking and recognition of verifiable browser/OS preference signals.

FiCom ry: Urges repeal of the outdated ePrivacy Directive due to regulatory challenges.

The EU should repeal the ePrivacy Directive, which is outdated and creates regulatory challenges

: Complains about intrusive consent windows that obstruct access to content, urging simplification.

Currently, when visiting any compliant website that wishes to collect my personal data, instead of getting to the desired content as easily as possible, I always need to go through the consent windows, which is super annoying.

: Notes overlapping domestic and foreign privacy regimes increase compliance costs for African businesses, highlighting the need for coherence.

African business/corporates face the cost of navigating overlapping domestic and foreign compliance regimes, including EU standards such as GDPR.

Union of Entreprenuers and Employers: Supports no-consent for security or technical cookies and recognizes contextual ads and anonymized analytics as low risk with transparency and opt-out.

Cookies essential for security or technical functionality should not require consent, and contextual advertising or anonymised analytics could be recognised as low-risk practices when transparency and opt-out options are available.

Anitec-Assinform: Advocates repealing ePrivacy or, if focusing on cookies, simplifying rules and reducing consent triggers.

Notwithstanding the general request to repeal the ePrivacy Directive, should the Commission confirm its focus on cookies only, we maintain that EU's rules on cookies and other tracking technologies laid down by the ePrivacy Directive should be simplified, including reducing cases where consent must be obtained.

European AI Forum: Seeks clarification on the interaction between ePrivacy and adjacent frameworks.

Clarify the interaction with ePrivacy.

WKÖ - Austrian Federal Economic Chamber: Warns that without explicit simplification, such as legitimate interest for analytics or broader technical grounds, new rules are not sensible.

If no explicit simplification of the current provisions is planned, such as an extension of the legitimate interest to include (third-party) analysis options or the expansion of the permitted grounds for technically necessary technology, we believe that new regulations on this issue are not sensible.

: Advocates shifting cookie consent handling to browsers for centralized control.

I would shift the responsibility for cookie handling and accepting to browsers.

ACEA (European Automobile Manufacturers' Association): Argues institutional reform is needed to balance privacy protections with Europe’s digital economy.

Only through such institutional reform can the regulation of the privacy of electronic communication strike the right balance between protecting individuals' rights and enabling Europe's digital economy to flourish.

: Suggests browser-level options letting users easily choose whether to receive targeted advertising.

Put options in browsers: do you want targeted advertising or not.

1.7.7 Data Subject Rights & User Control

Modernization of data subject rights focuses on making rights effective for individuals while practical and scalable for controllers. Stakeholders highlight that access (especially under GDPR Article 15) can be highly resource-intensive, advocating measures like narrowing requests, two-step responses for large datasets, clearer guidance on abusive or excessive demands, and proportionate limits where trade or business secrets or disaster-recovery backups are implicated. Transparency remains essential but should be applied in ways that are pragmatic and genuinely informative rather than burdensome or performative. User control is strengthened through automation and improved UX. Proposals include adopting the Global Privacy Control to automate rights like opt-outs at scale, enabling privacy dashboards and other self-service tools, and ensuring full transparency, choice, and control in advertising and consent flows. Models that offer an equivalent paid alternative to tracking or personalized ads are promoted alongside robust transparency, ensuring users face no undue pressure and that consent is freely given, specific, informed, and unambiguous. Several contributors urge a shift from procedural compliance to enforceable user rights in AI contexts, and call to clarify GDPR Article 22 as a right rather than a blanket prohibition, enabling beneficial automation (e.g., claims processing) without undermining individual protections. Broader harmonization and simplification of rights, coupled with safeguards against vexatious use and impractical “open data only” approaches, are seen as necessary to balance innovation with meaningful privacy controls.

WFA believes that consumers should have full transparency, choice, and control over what data they share and how it is used, particularly in digital advertising. (World Federation of Advertisers)

Editing the draft standard Global Privacy Control which defines the technical signal that browsers can use to automate the exercise of user rights in ways that simplify compliance while maintaining publishers access to advertising revenue. ()

The paid alternative is genuinely equivalent to the free service, except for the absence of personalized advertising or tracking, and is offered at a reasonable price. (Seznam.cz, a.s.)

Particularly problematic is the EDPB's demand that data from backup systems must also be made accessible. (German Insurance Association)

Verband kommunaler Unternehmen e.V.: Advocates narrowing and prioritizing data access requests, allowing controllers to ask subjects to specify scope and excluding requests pursuing non-protective objectives, while safeguarding trade and business secrets.

b) providing the information would reveal a trade or business secret of the controller or a third party to the data subject and the interest in maintaining confidentiality outweighs the data subject's interest in the information."

: Promotes Global Privacy Control to automate the exercise of user rights, reduce compliance costs, and improve user experience while supporting publishers.

Developing and deploying the Global Privacy Control (GPC) as a technical system to reduce compliance costs, improve user experience, and improve the business position of media publishers with respect to tech monopolies and advertising intermediaries.

Volkswagen Group: Calls for more practical, less resource-intensive handling of GDPR data subject rights, noting Article 15 access requests often impose disproportionate effort with limited benefit.

Responding to access requests- especially under Article 15 - is often highly resource-intensive and can result in disproportionate effort, with limited benefit for the individual.

FEBIS: Warns that an open-data-only approach may reduce transparency in practice and urges transparency that is practical, scalable, and effective.

While transparency remains essential, it must be applied in a way that is practical, scalable, and effective.

Unipol Assicurazioni S.p.A.: Urges the AI Act to pivot from procedural provider obligations to empowering users with concrete, enforceable rights such as explanation, contestation, and opt-out.

In light of the above, we urge that any AI Act review shift its focus from purely procedural obligations on providers - which act as a de fact barrier to innovation - to empowering users with concrete, enforceable rights.

German Insurance Association: Opposes requirements to provide access to backup systems, advocates a clarified two-step approach for large datasets and limits on vexatious requests, and seeks a rights-focused interpretation of Article 22 to enable automation.

Particularly problematic is the EDPB's demand that data from backup systems must also be made accessible.

World Federation of Advertisers: Supports full user transparency, choice, and control over data in advertising, committing to ethical use that respects user preferences throughout the lifecycle.

WFA believes that consumers should have full transparency, choice, and control over what data they share and how it is used, particularly in digital advertising.

Seznam.cz, a.s.: Endorses a consent-or-pay model with a genuinely equivalent paid alternative at a reasonable price, no undue pressure, and robust transparency ensuring valid, informed consent.

The paid alternative is genuinely equivalent to the free service, except for the absence of personalized advertising or tracking, and is offered at a reasonable price.

Leading Baltic tech and other businesses and professional associations listed in the submission: Argues for expanding exceptions to data subject rights to restore balance, reduce unnecessary administrative burdens, and refocus resources on meaningful protection and innovation.

This undermines the balance between individual rights and interest of data controllers, creating unnecessary administrative burdens and diverting resources from innovation and genuine data protection efforts.

Meta Platforms Ireland Limited: Calls for clear guidance to prevent abuse of data subject rights by privacy profiteers and representative organizations, and for scalable tools like dashboards and automation to manage rights at scale.

The current approach also fails to provide clear, practical guidance on what constitutes "manifestly unfounded or excessive" data subject requests, leading to abuse of data subject rights by privacy profiteers and increased administrative burden.

Protector PriVit S.R.L.: Questions the need for open clauses and overlapping exceptions, advocating simplification, harmonization, and analysis of rejection cases to streamline GDPR data subject rights.

Do we need separate exceptions per right, on top of the ones that allow rejection of rights when identity cannot be established [Art. 12(2) GDPR] or when the request is manifestly unfounded/excessive [Art. 12(5) GDPR]?

iProov Ltd: Highlights tensions between current practices and the GDPR mandate to provide data subject rights free of charge, indicating a need for clearer alignment and guidance.

European Law Institute: Examines data subject rights and remedies through the lens of the EU Charter of Fundamental Rights, emphasizing effective redress mechanisms.

DigitalTrade4.EU: Advocates minimal, user-controlled data verification approaches that uphold privacy while enabling trustworthy interactions.

Telekom Austria AG: Calls to reassess and streamline burdensome data subject rights obligations to ensure proportionality and operational feasibility.

SIA Tet: Supports privacy-preserving opt-out mechanisms that reduce tracking and empower user control over personal data.

Healthtech Finland: Urges maintaining high standards for digital rights, transparency, and user control in sensitive healthtech contexts.

U.S. Chamber of Commerce: Seeks clearer scope definitions, reasonable timelines, and practical guidance for data subject access requests to improve compliance.

Polish Confederation Lewiatan: Requests precise criteria and guidance for identifying manifestly unfounded or excessive data subject requests, protecting organizations from abuse.

Salesforce, Inc.: Proposes limiting vexatious or tactical DSARs in employment contexts and streamlining employer handling to focus on relevant data.

Verband der Automobilindustrie e.V.: Calls to extend Article 14(5) exemptions to Article 13, streamline data subject rights obligations, and clarify the right to copy to avoid exposing trade secrets.

Association des Constructeurs Européens de Motocycles: Recommends extending notice exemptions with appropriate safeguards to balance transparency and practicality for users and controllers.

Advertising Information Group: Promotes enhanced transparency and accessible choices to strengthen user control over data in advertising contexts.

eyeo GmbH: Advocates clear opt-out options accompanied by strong transparency so users can effectively control tracking and data use.

: Suggests revising or removing the GDPR's right to object phrasing to reduce ambiguity and improve consistency among data subject rights.

Independent Retail Europe: Seeks clarification of the scope of Article 15 access to ensure proportional, meaningful disclosure rather than exhaustive, burdensome detail.

Broadcom: Supports limiting DSAR misuse in employment disputes and focusing disclosures on relevant, proportional personal data.

Seznam.cz, a.s.: Calls for heightened privacy protections for vulnerable groups and clearer transparency about data processing choices to enable informed control.

Insurance Europe: Urges clarification that Article 22 is a data subject right rather than a general prohibition, enabling fair automation with safeguards.

European Entrepreneurs CEA-PME: Supports voluntary digital ID schemes with offline alternatives to preserve user choice and control.

European Savings and Retail Banking Group: Highlights implementation challenges for permission dashboards and managing consent at scale, calling for practical solutions.

Danish Industry: Advocates reform of Articles 13–14 and 14(5)(b) and streamlining of access rights to reduce burdens while maintaining transparency and user control.

Euroconsumers: Demands robust transparency and opt-out safeguards to protect consumer privacy and strengthen user control.

Dutch Startup Association: Promotes improved consent UX and clear transparency to avoid dark patterns and ensure informed user choices.

Cookie Information / Piwik PRO: Urges recognition and honoring of Global Privacy Control signals as universal opt-outs to automate user rights.

Too Good To Go: Suggests relaxing DSAR requirements to avoid disproportionate burdens on smaller services while preserving core protections.

APPLiA (Home Appliance Europe): Recommends limiting access requests, protecting trade secrets, and extending protective exceptions to balance user rights with business needs.

VAUNET - German Association of Private Media: Proposes a de minimis threshold for GDPR rights requests to filter trivial or abusive submissions and focus resources on significant cases.

DER MITTELSTANDSVERBUND - ZGV e.V.: Encourages standardized labels and digital disclosures to improve user understanding and control over how data is collected and used.

1.7.8 Public Interest, Research & Retention Limits

This category centers on updating EU privacy rules to accommodate public-interest research and responsible data reuse while maintaining strong safeguards. Stakeholders seek alignment across the AI Act, GDPR, and the ePrivacy Directive to enable lawful secondary use of personal (including special category) data for AI training, testing, bias correction, and safety/fairness monitoring. They advocate recognizing algorithmic improvement as a legitimate purpose (GDPR Art. 6; Art. 9(2)(j)), broadening and clarifying the Article 89 research framework (and extending research privileges to industry, pre-commercial, and collaborative work), and ensuring consistent interpretations with safeguards such as pseudonymisation, purpose limitation, access controls, and ethical oversight. They also highlight audience measurement and market research as activities serving the public interest, and warn that current GDPR practice can slow data-driven growth and innovation. On retention limits, views diverge. Some call for targeted, evidence-based, and proportionate retention regimes with clear necessity standards, limited purposes (e.g., quality control and ongoing fairness/safety monitoring), time bounds, and oversight—citing court pushback against blanket mandates and the risk that indiscriminate retention is both unlawful and ineffective. Others support extended retention for security-related public interests or propose refining the framework via sectoral instruments, provided it complies with EU jurisprudence. Overall, the emphasis is on calibrated retention that enables research and safety objectives without eroding fundamental rights.

The interplay between the AI Act, the GDPR, and the ePrivacy Directive creates uncertainty for companies seeking to use data responsibly to train, test and improve AI systems. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Recognise bias correction and algorithmic improvement as legitimate processing purposes under GDPR Article 6 and Article 9 (2 lit. g.j), provided appropriate safeguards (e.g. pseudonymisation,

purpose limitation, access controls1) are implemented. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Modernise ePrivacy provisions to permit low-risk data collection (e.g. telemetry, performative analytics) without explicit consent, where such processing is necessary to ensure security, accuracy or fairness of AI systems. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

All academic, pre-commercial and collaborative Al experimentation should remain outside the Al Act's scope until systems are deployed commercially. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Calls for aligning GDPR, ePrivacy, and the AI Act to enable responsible data reuse for research, bias correction, and long-term monitoring with strong safeguards, and for broadening research exemptions. Emphasizes clarifying lawful repurposing and modernizing consent rules to support innovation while maintaining protections.

The current legal norms restrict their ability to reuse data for essential quality control and fairness checks, while demanding deletion of datasets that could be necessary for long-term monitoring.

Business & Science Poland: Urges balancing privacy with other fundamental rights to allow proportionate data use for research and innovation in the public interest. Seeks calibrated rules that permit limited data reuse and retention where justified and safeguarded.

DigitalTrade4.EU: Supports enhancing data retention frameworks via EUTIR to provide clearer, harmonized rules for lawful retention. Emphasizes proportionality and safeguards to protect privacy while enabling legitimate uses.

ENCIRCLE Research Consortium: Requests clearer standards for applying the research exemption and the necessity test under GDPR. Aims to enable necessary processing and retention for legitimate research with appropriate safeguards.

DOT Europe: Asks to reconsider data retention proposals to ensure they are targeted, proportionate, and legally robust. Warns against broad mandates that overreach or lack clear necessity.

Verband der Automobilindustrie e.V.: Advocates expanding GDPR Article 89(2) research exceptions so industrial R&D can reuse and retain data under safeguards. Seeks clearer allowances for public-interest and scientific research in industry settings.

Confederation of European Security Services (CoESS): Supports extended data retention periods to enable effective security services and public safety operations. Emphasizes oversight and safeguards to balance privacy with safety needs.

Association des Constructeurs Européens de Motocycles: Calls to broaden GDPR research exemptions and derogations, enabling responsible data reuse and retention for both academic and industrial research. Seeks harmonized safeguards to ensure compliance and trust.

Google: Advocates expanding exemptions to process special-category data for research and public-interest purposes with strong safeguards. Supports necessary retention to ensure research validity and safety outcomes.

European Federation for Market Research Organisation (EFAMRO): Supports a broad interpretation of Article 89 and explicit recognition of research and audience measurement exemptions. Seeks practical rules for necessary data reuse and retention with privacy protections.

Audience Measurement Coalition (AMC): Argues audience measurement should qualify under public-interest or research grounds, permitting necessary processing and limited retention. Calls for clear legal bases to reduce uncertainty for measurement activities.

SAP SE: Proposes extending research privileges beyond academia to include industry-led research and innovation. Seeks explicit allowances for data reuse and retention under safeguards to support development and testing.

Danish Industry: Warns that GDPR constraints slow data-driven growth and restrict innovation. Calls for modernization that enables proportionate data reuse and retention for research while maintaining protections.

Esomar: Seeks a broader, clearer Article 89 framework to reduce uncertainty and enable compliant research uses and retention across the EU. Emphasizes harmonization and robust safeguards.

BUGLAS e.V.: Opposes blanket data retention as ineffective, high-risk, and repeatedly invalidated by courts. Supports targeted, evidence-based, and proportionate approaches instead of mass retention mandates.

1.7.9 Safety, Fraud & Government Access Controls

This category captures a broad consensus to modernise EU privacy rules so that proportionate, clearly-scoped processing for safety, security, and fraud/theft prevention is enabled while preserving strong privacy guarantees. Stakeholders ask to recognise operational and legal necessity (e.g., essential security functions, identity verification, theft prevention), allow legitimate interests or public-interest grounds for low-risk fraud/AML use cases, and permit automated and communications data processing to protect users (including children) from harms like harassment and grooming. They also call for flexible, risk-based age verification and for GDPR/ePrivacy to accommodate secure monitoring and incident prevention without turning safety into surveillance. At the same time, contributors urge firm limits and safeguards on public- or third-party access: proportionality, minimisation, confidentiality, transparency, and due process should govern requests; blanket or overly broad mandates (e.g., indiscriminate traveller data uploads or publishing workers' home contact details) should be curtailed. Narrow emergency carve-outs (such as caller-ID overrides for eCall) are acceptable, but routine access must be bounded, auditable, and context-sensitive, with special vigilance in illiberal environments. The throughline is a calibrated balance: maintain the ability to process data to keep services and people safe, while tightening controls against unnecessary disclosure and governmental overreach.

However, from the perspective of the data controller, some processing involving access to information stored in the user's terminal are essential to ensure both the security and the proper functioning of the service. (CNIL (French Data Protection Authority))

Therefore, in the context of a simplification exercise, the processing of communications data according to the ePD must continue to be allowed to ensure not just the security of the service, but also the safety of its users. (Video Games Europe)

We also welcome the proposed exceptions to the presentation of calling and connected line identification envisaged in Article 13 (e.g. when overriding the elimination of calling line identification is necessary to allow emergency services, such as eCall, to carry out their tasks). (BEUC - The European Consumer Organisation)

Disclosing this data to all potential customers does not add any value and creates a safety risk. (Bolt)

CNIL (French Data Protection Authority): CNIL highlights the difficulty of reconciling strict ePrivacy consent rules with essential anti-fraud and theft-prevention measures, noting some terminal data access is indispensable for security and compliance. It recognizes that such processing can be operationally and legally necessary to fulfill service and safety obligations.

Importantly, these processing activities may also be strictly necessary from an operational or even legal standpoint - for example, vehicle theft can directly jeopardise the ability of a service provider to deliver its services and identity verification measures may be required by law.

Video Games Europe: Video Games Europe urges maintaining ePrivacy allowances for automated processing of communications to protect users—especially children—from harassment, grooming, and other harms. It stresses that processing should support not just service security but the broader safety of users.

While the confidentiality rules should be modernised and adapted to the current environment, allowing for automated processing of communications for goals that benefit users, for video game companies, it

is of utmost importance not to be restricted in their ability to protect users, especially children, from harassment, bullying, grooming, hate speech and cheating.

BEUC - The European Consumer Organisation: BEUC supports targeted exceptions to caller ID presentation to enable emergency services like eCall to perform their tasks. Such limited carve-outs are seen as necessary for public safety without undermining privacy more broadly.

We also welcome the proposed exceptions to the presentation of calling and connected line identification envisaged in Article 13 (e.g. when overriding the elimination of calling line identification is necessary to allow emergency services, such as eCall, to carry out their tasks).

Bolt: Bolt argues that mandating disclosure of drivers' personal contact details to all customers is disproportionate, adds no value, and creates safety risks. It contends platforms can trace providers when necessary without broadly exposing personal data.

Disclosing this data to all potential customers does not add any value and creates a safety risk.

Adigital (Asociación Española de la Economía Digital): Adigital flags a Spanish decree requiring tourism providers to share all travelers' personal data with the government even without an investigation, calling it disproportionate and potentially unlawful under EU privacy rules. The measure also creates legal uncertainty for businesses.

Since December 2024, a Royal Decree in Spain obliges tourism service providers to share detailed personal data of all travellers with the government, even when no investigation is ongoing.

ENSHPO - The European Network of Safety and Health Professional Organizations: ENSHPO calls for clearly distinguishing genuine safety objectives from surveillance in AI deployments. This separation is needed to protect rights while ensuring effective safety practices.

Elia Group: Elia Group advocates adapting GDPR interpretations to enable secure monitoring and necessary data sharing for critical infrastructure. It seeks a framework that supports safety and reliability while maintaining strong privacy safeguards.

ASNEF: ASNEF requests clarity that fraud prevention and anti-money laundering processing can rely on public interest grounds. Clear legal bases would improve certainty and enforcement effectiveness.

Confederation of European Security Services (CoESS): CoESS recommends evaluating GDPR to ensure security service providers can support public security with proportionate data use. It emphasizes balancing safety needs with robust data protection safeguards.

Association des Constructeurs Européens de Motocycles: ACEM urges restricting disclosure of sensitive rider and vehicle information to prevent misuse while meeting safety needs. It seeks proportionate rules that protect privacy alongside security objectives.

Google: Google supports permitting automated processing for security and fraud prevention as a legitimate basis. This would protect users and services without imposing undue consent friction.

Movement for an Open Web: Movement for an Open Web proposes allowing legitimate interests for low-risk fraud prevention. This approach would reduce burdens while still protecting users from abuse.

The Center for Countering Digital Hate: The Center for Countering Digital Hate highlights parental oversight features as important safety tools, exemplified by platforms like Discord. It favors privacy rules that enable protective controls for families.

Orgalim - Europe's Technology Industries: Orgalim calls to limit public-sector data requests to what is strictly necessary and subject them to strong confidentiality. This protects users' personal data and companies' sensitive information while allowing justified access.

Meetic Group, a Match Group Company: Meetic urges clarifying that privacy rules should enable safety-by-design, including flexible, proportionate multi-level age verification. This protects minors effectively without excessive data collection.

Alliance Digitale: Alliance Digitale recommends stronger procedural safeguards and confidentiality for government access to data. It emphasizes due process, minimization, and protection of sensitive information.

DIGITALEUROPE: DIGITALEUROPE supports recognizing fraud prevention and security as legitimate interests under EU law. This would enable protective processing with proportionate safeguards and reduce reliance on consent for critical safety functions.

Mistral AI: Mistral AI calls for narrowly scoped, safeguarded information request regimes with transparency and oversight. Such limits protect user privacy and sensitive data while accommodating legitimate access needs.

European Games Developer Federation (EGDF): EGDF asks that data processing for user safety and content moderation in games remain permitted to tackle harms like harassment and grooming. It stresses maintaining capacities to keep online communities safe.

BUGLAS e.V.: BUGLAS urges scrutiny of surveillance and data-access cooperation in illiberal contexts. It calls for robust safeguards before enabling cross-border access to users' data.

Adyen: Adyen seeks clearer, harmonized rules for lawful fraud prevention data processing and sharing in payments. It asks for guidance on legal bases, retention, and cooperation with partners and authorities to combat fraud effectively.

1.7.10 AI Alignment & Privacy-Preserving Technologies

AI Alignment & Privacy-Preserving Technologies within Privacy & Data Protection Modernization centers on enabling AI training, testing, and beneficial automated decisions while upholding strong privacy protections under the GDPR. Stakeholders seek clearer lawful bases beyond consent (including adjustments to Article 9 for AI training, embedding proportionality in Article 24, and revising Article 22 to permit beneficial ADM with safeguards) and legal coherence between the GDPR, the AI Act, and sectoral rules. Operational alignment relies on concrete guardrails: EU-wide guidance on data quality and minimisation, early pseudonymisation/anonymisation, exclusion of sensitive sources, transparency to data subjects, and risk-based evaluations—especially to prevent leakage of sensitive information in rare disease contexts. Proposals endorse responsible data reuse for safety improvements and compliance, the use of synthetic or anonymised data, and sandbox flexibility, recognizing that consent is often suboptimal for fraud prevention and health scenarios. Innovative governance ideas (e.g., pointer-based retention) and clearer communication of decision elements to individuals aim to protect privacy while enabling trustworthy, competitive AI development, including for SMEs.

Such processing of personal data for the training of AI systems and models would include clear guardrails, such as the exclusion of sensitive data sources, limitations of data categories, early pseudonymisation or anonymisation, transparency towards data subjects, and a risk-based evaluation of relevant safeguards. (Telefonica, S.A.)

We underline the importance of introducing EU-wide common guidelines on Data Quality and Data Minimisation for artificial intelligence (AI) systems, in order to ensure the responsible, proportionate and transparent use of data. (GSMA)

XX) The processing of personal data, including special categories of personal data, in the form of pseudonymised data sets is necessary to ensure compliance of high-risk artificial intelligence systems with Union harmonisation legislation, in particular with regard to health and safety considerations, which are public interests of the Union. ()

Our proposal is for such STF to enjoy pointer-based retention. (Infosys Limited)

FERMA - Federation of European Risk Managers Associations: Advocates embedding the proportionality principle more clearly in GDPR accountability rules to ensure risk-based controls for AI processing, supporting privacy-preserving alignment.

Embed proportionality principle more clearly in Article 24.

DigiFinland: Calls to amend GDPR Article 9 to explicitly allow personal data processing for AI training with robust safeguards against leakage, particularly for sensitive and rare disease data.

Consider amending Article 9 of the GDPR to explicitly allow the processing of personal data for AI training and development, while ensuring robust safeguards against the leakage of sensitive information, especially in rare disease contexts.

Enel SpA: Requests clearer definitions of key decision elements communicated to affected individuals in AI-driven outcomes to strengthen transparency and privacy rights.

Clarify the meaning of main elements of the decision for affected individuals.

Technology Industries of Finland: Supports lawful reuse of personal data for AI testing under safeguards to improve models, correct bias, and foster innovation, especially for SMEs.

Permit lawful re-use of personal data for AI testing under safeguards to improve AI systems, correct bias and foster innovation, especially for SMEs with limited resources.

Unipol Assicurazioni S.p.A.: Argues that reliance on explicit consent hinders training fraud-detection AI on large historical datasets containing health data, urging alternative lawful bases with safeguards.

For instance, the reliance on explicit consent makes it operationally unfeasible to train fraud-detection AI models on large, historical datasets of claims, which often contain health data.

German Insurance Association: Emphasizes developing AI using synthetic or anonymised data as a privacy-preserving approach that reduces reliance on identifiable personal data.

AI models, IT applications, products, systems, and analytical tools can often be developed using synthetic or anonymised data.

GSMA: Urges EU-wide guidelines on data quality and minimisation for AI to ensure responsible, proportionate and transparent data use.

We underline the importance of introducing EU-wide common guidelines on Data Quality and Data Minimisation for artificial intelligence (AI) systems, in order to ensure the responsible, proportionate and transparent use of data.

Telefonica, S.A.: Proposes clear guardrails for AI training, including excluding sensitive sources, limiting data categories, early pseudonymisation or anonymisation, transparency, and risk-based safeguards.

Such processing of personal data for the training of AI systems and models would include clear guardrails, such as the exclusion of sensitive data sources, limitations of data categories, early pseudonymisation or anonymisation, transparency towards data subjects, and a risk-based evaluation of relevant safeguards.

Bitkom e.V.: Advocates for inclusive AI sandboxes under safeguards so beneficial applications are not arbitrarily excluded, supporting privacy-aligned innovation.

This would ensure that useful and beneficial AI applications are not arbitrarily excluded from sandbox environments.

Mastercard Europe SA: Notes that consent is not an optimal lawful basis for AI-based fraud prevention and calls for more suitable bases with safeguards.

In the case of using AI for fraud prevention, consent is not optimal.

Centre for Information Policy Leadership (CIPL): Calls to revise automated decision-making rules to permit beneficial automated decisions under strong safeguards, aligning privacy with utility.

Revise Automated Decision-Making (ADM) rules (Article 22) to permit beneficial automated decisions under strong safeguards.

Infosys Limited: Recommends pointer-based retention for AI training artefacts to minimize data replication and enhance privacy-by-design in workflows.

Our proposal is for such STF to enjoy pointer-based retention.

Ibec: Stresses regulatory coherence so new laws work with existing rules to support innovation and EU competitiveness in privacy-preserving AI.

The interplay between any proposed new laws and existing rules must work with, not against, innovation and the goal of EU competitiveness.

Adigital (Asociación Española de la Economía Digital): Requests legal clarity and consistency on how GDPR interacts with other regulations to reduce uncertainty for compliant, privacy-preserving AI.

Provide legal clarity and consistency in how the GDPR interacts with other regulations-both at the EU level and between Member States.

FiCom ry: Highlights that access to data is essential for AI development and alignment, calling for mechanisms that balance innovation with privacy safeguards.

Data is the engine of Al development.

European AI Forum: Advocates responsible data reuse by allowing repurposing of personal data for AI training and testing when improving safety or compliance, under safeguards.

Enable responsible data reuse by clarifying that personal data collected for one purpose may be lawfully repurposed for AI training and testing when this serves compliance with the AI Act or demonstrable safety improvements.

: States that processing pseudonymised personal and special-category data is necessary to ensure compliance and health and safety of high-risk AI systems, serving the public interest.

XX) The processing of personal data, including special categories of personal data, in the form of pseudonymised data sets is necessary to ensure compliance of high-risk artificial intelligence systems with Union harmonisation legislation, in particular with regard to health and safety considerations, which are public interests of the Union.

1.7.11 Miscellaneous

This Miscellaneous subcategory under Privacy & Data Protection Modernization gathers diverse stakeholder views on updating EU data rules. Contributors welcome a stronger legislative focus on cookies and other tracking technologies, cybersecurity incident reporting, and targeted adjustments to the AI Act to ensure rules apply optimally. They also point to the need for clarity on GDPR legal bases (including legal obligation), discuss targeted amendments despite existing CJEU guidance, and advocate both for promoting responsible data use and, in some domains, deregulatory moves such as easing tenant data disclosure. Several note a fundamental shift in data processing practices that modernization efforts must address. On consumer-facing practices, the set highlights how location history is leveraged to personalize recommendations, predict traffic for commutes, and deliver advertising both on and off platform—illustrating the trade-offs between utility and privacy. Transparency-first digital tools are presented as a way to build citizen trust, while other contributions urge stricter limits on profiling and the reuse of data for advertising. Overall, the thread is pragmatic modernization: refining the interplay between privacy, AI, and cybersecurity frameworks to enhance trust and legal certainty without stifling practical, responsible data use.

We very much welcome the fact that the European Commission is focusing its measures on data legislation, including rules on cookies and other tracking technologies, cybersecurity incident reporting, and targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules. (Kaspersky Labs Limited)

According to the information provided by Google, Location History "helps you get better results and recommendations on Google products. (BEUC - The European Consumer Organisation)

This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google." (BEUC - The European Consumer Organisation)

For example, you can see recommendations based on places you've visited with signed-in devices, or traffic predictions for your daily commute." (BEUC - The European Consumer Organisation)

Kaspersky Labs Limited: Kaspersky welcomes the European Commission's focus on modernizing data legislation, covering cookies and tracking, cybersecurity incident reporting, and calibrated AI Act adjustments to improve rule application.

We very much welcome the fact that the European Commission is focusing its measures on data legislation, including rules on cookies and other tracking technologies, cybersecurity incident reporting, and targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules.

BEUC - The European Consumer Organisation: BEUC highlights how Google's Location History fuels extensive personalization across services and targeted advertising based on places visited and commuting patterns.

This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google."

: It argues that prioritizing transparency in the use of digital tools, rather than scrutiny, is key to building citizens' trust.

It increases citizens' trust because digital tools are not used primarily for scrutiny, but first for transparency.

European Law Institute: The European Law Institute calls for a fundamental shift in approaches to data processing under modernization initiatives.

German Property Federation: The German Property Federation supports deregulating tenant data disclosure to simplify processes and reduce compliance burdens.

Bundesverband Großhandel, Außenhandel, Dienstleistungen e.V.: The association promotes responsible data use that enables innovation while safeguarding privacy.

Audience Measurement Coalition (AMC): AMC contends that audience measurement can be grounded in GDPR's legal obligation basis to ensure lawful processing and compliance.

Danish Industry: Danish Industry urges targeted amendments to the GDPR despite existing CJEU guidance, aiming for clearer, more practical rules.

Cookie Information / Piwik PRO: Cookie Information/Piwik PRO advocates prohibiting profiling and the reuse of personal data for advertising to strengthen privacy protections.

1.8 Cybersecurity & Certification Alignment

The most compelling theme is EU-wide harmonization and mutual recognition that replaces fragmented, duplicative audits with proportionate, risk-based assurance—aligning NIS2, CRA, DORA, eIDAS, RED, and the AI Act so compliance effort improves security outcomes. Streamlining calls include consistent transposition and enforcement, retiring overlapping provisions, centralized reporting, and sector-aligned certification that reuses evidence. International standards and MRAs (ISO/IEC, NIST, 62443, GSMA/3GPP) should underpin presumption of conformity, supported by unified guidance and auditor accreditation. Conformity assessment needs coherent accreditation, capacity building for Notified Bodies, shared supervisory results (e.g., DORA JET), and practical bridges like CSA schemes and common specifications. Clear scope and guidance—covering CRA coverage, "substantial modification," CE marking for software, modular hardware/software certification, proportionality, and sector carve-outs—reduce interpretation risk. Outcome-focused assurance prioritizes self-assessment, voluntary certification, compensating controls, TLPT, and CTI. Vulnerability management should adopt KEV, CVSS/NVD alignment, and calibrated disclosure to avoid new risks. Supply-chain assurance emphasizes minimal interoperable SBOMs, chain-of-custody transparency, standard clauses, and SME relief. Lifecycle-aware regimes favor rolling validity, decoupled updates, predictable paths, and durable credentials. Digital identity and trust services need QSCD continuity, automated proofing benchmarks, modular compliance, and global interoperability. Technical baselines should clarify encryption and incident severity while keeping outcome-based flexibility. Secure-by-design AI warrants pragmatic certification, ethical interoperability, and proportionate oversight. Collaboration, intelligence sharing, managed services, and careful public data collection bolster operational resilience. Across sub-categories, consolidation, international alignment, and risk-

proportionate, lifecycle-aware obligations dominate—aiming to cut redundancy while preserving high assurance and agility.

1.8.1 Regulatory Harmonization & Streamlining

Regulatory Harmonization & Streamlining (under Cybersecurity & Certification Alignment) centers on reducing fragmentation and overlap across EU cybersecurity laws and schemes so compliance effort reinforces—rather than distracts from—security outcomes. Stakeholders call for consistent transposition and enforcement of NIS2, a coherent horizontal framework across instruments like the CRA, RED, Machinery Regulation, CE marking and harmonized standards, and limits on the complexity of certification and conformity processes. The goal is predictable, proportionate requirements that cut redundant bureaucracy and free resources for real cyber defense without weakening effectiveness. Concrete streamlining proposals include repealing or deferring overlapping provisions (e.g., retiring RED cybersecurity requirements once CRA is in force), building on established NIS2/CER processes for reporting, certification and risk management, centralizing incident reporting, and aligning terminology and definitions across texts. Sector-specific alignment is also sought—harmonized vehicle cybersecurity certification (UN R155), reuse of existing evidence (e.g., smart payment cards), reassessment of additional voluntary schemes, and clearer CE-marking harmonization. Some positions are more radical (e.g., withdrawing the EU Cybersecurity Act), reflecting strong pressure for consolidation while keeping resilience front and center.

> *Avoid redundancies in European cybersecurity legislation* (ZVEI e.V.)
>
> *A coherent, horizontal approach will ensure predictable, proportionate requirements that reinforce-not dilute-Europe's digital resilience.* (Verisure)
>
> *German industry urges the European Commission to withdraw the EU CSA completely.* (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)
>
> *Harmonise overlapping cybersecurity requirements, exempt financial services from CRA, and centralise incident reporting through a single EU channel.* (ING Romania)
>
> **FERMA - Federation of European Risk Managers Associations:** Advocates consistent national transposition of NIS2 to avoid a patchwork of obligations and ease compliance and enforcement.
>
> *A better governance will also mean to ensure that EU directives (particularly NIS2) are transposed into national laws consistently to avoid creating a patchwork of obligations that complicate compliance and enforcement between member states.*
>
> **SIEMENS AG:** States that CRA requirements sufficiently cover cybersecurity aspects of the Machinery Regulation, helping avoid duplication.
>
> *Compliance with the CRA requirements reasonably cover the cybersecurity-related aspects of the MR.*
>
> **ZVEI e.V.:** Calls to eliminate redundancies across EU cybersecurity legislation to streamline compliance.
>
> *Avoid redundancies in European cybersecurity legislation*
>
> **LightingEurope:** Supports repealing RED cybersecurity requirements once the CRA is in force to prevent overlap and simplify obligations.
>
> *Our association supports the European Commission's approach to repeal the RED cybersecurity requirements once the CRA is in force.*
>
> **Workday:** Warns that proliferating EU cybersecurity rules create complexity and overlapping requirements that divert resources from security; urges alignment and simplification.
>
> *The proliferation of cybersecurity regulations in the EU has led to significant complexity and overlapping requirements, often diverting resources away from security enhancements to compliance.*
>
> **Volkswagen Group:** Recommends limiting the complexity of cybersecurity regulation, certification schemes, and harmonized standards to what is strictly necessary.
>
> *2) Furthermore, the complexity of cyberse- curity-related regulation, certification schemes, and harmonized European standards (hENs) must be limited to what is strictly necessary.*

European Energy Information Sharing and Analysis Centre: Urges building on established NIS2 and CER processes for reporting, certification, and risk management to ensure harmonized practices.

Build upon established NIS2 and CER processes for reporting, certification, and risk management.

GSMA: Proposes delaying enforcement or introducing a grace period for the RED Delegated Regulation to smooth transition and reduce compliance strain.

The enforcement of the RED Delegated Regulation should be delayed, or a grace period should be introduced.

ING Romania: Advocates harmonizing overlapping requirements, exempting financial services from CRA, and centralizing incident reporting via a single EU channel.

Harmonise overlapping cybersecurity requirements, exempt financial services from CRA, and centralise incident reporting through a single EU channel.

Bitkom e.V.: Identifies considerable potential for harmonization in CE marking requirements to ensure consistency.

For instance, there is considerable potential for harmonization when it comes to CE marking requirements.

Verisure: Supports a coherent, horizontal regulatory approach to deliver predictable, proportionate requirements that strengthen digital resilience.

A coherent, horizontal approach will ensure predictable, proportionate requirements that reinforce-not dilute-Europe's digital resilience.

Trellix: Backs simplification that removes redundant bureaucracy while maintaining security effectiveness.

We agree with the Commission that simplification efforts must not compromise security effectiveness; rather, they should eliminate redundant bureaucracy that diverts resources from actual cyber defence.

Mastercard Europe SA: Seeks to avoid duplication under CRA by confirming smart payment card compliance using existing evidence.

In regard to CRA, we would like to avoid duplication and confirm compliance with the rules using the existing evidence for Smart Payment Cards.

European Express Association (EEA): Endorses NIS2 and promotes a smooth, harmonized rollout across the Union to protect businesses and supply chains.

We support NIS2 as vital for protecting European businesses and supply chains; we are promoting a smooth and harmonized roll-out of NIS2 across the Union.

Schneider Electric: Calls for reassessing the need for additional voluntary certification schemes amid growing cybersecurity requirements, within a simplification context.

With the growing number of cybersecurity requirements in the EU, the need for additional voluntary certification schemes, in a context of simplification, should be thoroughly reassessed.

Finnish Food and Drink Industries´ Federation (ETL): Urges aligning terminology and definitions across NIS2 and other cybersecurity regulations to improve clarity and application.

Terminology and definitions in NIS2 and other cybersecurity regulations should be aligned to make regulation clearer and easier to apply.

Adigital (Asociación Española de la Economía Digital): Highlights burdens from Codes of Conduct and certification due to extra documentation and guidance, indicating the need for streamlining.

Difficulties for all types of companies in complying with the mechanisms of Codes of Conduct and certification, as they require additional documentation and interpretive guidance, leading to greater workloads and higher compliance costs.

Vodafone Group: Views the Digital Omnibus as an opportunity to tackle longstanding cybersecurity regulatory challenges through simplification and alignment.

In regard to cybersecurity regulation the Digital Omnibus presents a critical opportunity to address longstanding challenges.

WKÖ - Austrian Federal Economic Chamber: Supports EU efforts to streamline, simplify, and make cybersecurity legislation more user-friendly.

We support the Commission's initiative, which aims, among other things, to streamline, simplify, and make EU cybersecurity legislation more user-friendly.

ACEA (European Automobile Manufacturers' Association): Calls for harmonising vehicle cybersecurity certification procedures under UN R155, aligning enforcement and establishing common certification.

Finally, we urge for harmonisation of vehicle cybersecurity certification procedures under UNECE Regulation No. 155 (UN R155), harmonising enforcement practices among Member States, and establishing common certification.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Calls for the withdrawal of the EU Cybersecurity Act, signaling a need to rethink certification and regulatory frameworks.

German industry urges the European Commission to withdraw the EU CSA completely.

1.8.2 International Standards & Mutual Recognition

This category promotes aligning EU cybersecurity and AI compliance with internationally recognized standards and certification schemes to reduce trade barriers, audit redundancy, and costs. It recommends using ISO/IEC 2700x, ISA/IEC 62443, NIST Cybersecurity Framework, ISO/IEC 42001, GSMA/3GPP NESAS, and harmonized European standards (e.g., RED EN series) as foundations for presumption of conformity across NIS2, CRA, DORA, GDPR, and the AI Act, while streamlining EU harmonized standards and leveraging established vertical norms. Voluntary, flexible, internationally aligned certification is favored to reflect sector diversity. A core theme is mutual recognition and equivalence: pan-European audits, EU-wide recognition of certifications and assessments, auditor accreditation frameworks, and international MRAs to avoid duplicative work. Stakeholders call for unified guidance (e.g., ENISA and the AI Office), alignment of NIS2 with ISO 27001 to minimize redundant audits, and acceptance of foreign certifications in specific domains, addressing fragmentation among Member States and enabling scalable, efficient compliance.

Promote the adoption and mutual recognition of international standards and certification schemes. (Vodafone Group)

Broadly adopted international cybersecurity standards and frameworks such as the ISO/IEC 2700X series, ISA/IEC 62443, and the NIST Cybersecurity Framework should be recognised and leveraged as foundational tools for demonstrating compliance with European regulations like the NIS2 directive, the CRA, the Data Act, and the GDPR, provided they align with European requirements. (Schneider Electric)

Germany is the only country mandating EU-certified ICT products/services under the Cybersecurity Act, according to recent benchmarking by Cullen International. (Vodafone Group)

Stop thinking that businesses need such regulations to protect themselves from cybercriminals, there are already international standards and best practices that deal with these aspects. ()

SIEMENS AG: Advocates leveraging harmonized European and international standards as the basis for conformity and reducing trade barriers, and urges CRA work to build on proven RED standards.

We advise also making use of international standards as these enable international alignment and reduce trade barriers.

Enel SpA: Calls for voluntary, flexible certification schemes aligned internationally to reflect energy sector diversity and reduce burdens.

Promotion of flexible, voluntary, and internationally aligned certification schemes that reflect the diverse needs of energy sector stakeholders.

Volkswagen Group: Urges reducing the number of harmonized European standards for CRA and using established sector-specific standards to avoid duplication.

Instead, established and existing standards from vertical, indus- try-related regulation shall be considered.

France Digitale: Recommends aligning NIS2 implementation with ISO 27001 to streamline audits and cut compliance costs.

For instance, the implementation of NIS2 should be aligned with ISO 27001, a widely recognised and globally adopted security standard, to reduce redundancy between audits and certifications, and thus lower compliance costs.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Seeks EU-wide mutual recognition of AI certifications and coordinated guidance to minimize duplication and scale across the single market.

Ensure that Al certifications, assessments or approvals obtained in one Member State are automatically recognised across the EU to reduce duplication and support market scalability.

GSMA: Proposes mutual recognition and standardized audit approaches, and acceptance of ISO-based certifications to meet EU requirements efficiently.

To avoid duplication, pan- European audits and international certifications, mutual recognition, harmonised and standardised audit approaches, and an EU framework for auditor approval, should reduce compliance burdens.

Amazon: Supports additional mutual recognition so a single NIS2 compliance assessment applies across Member States and comparable regimes.

These should provide that for organisations that are assessed by their responsible authority as being compliant with their obligations under NIS2, this assessment would be valid for other EU Member States' authorities also, including for comparable horizontal or sectoral regulatory regimes.

Association française de normalisation (AFNOR): Argues that international standards provide a credible foundation, with ISO/IEC 42001 serving to demonstrate AI Act compliance.

For instance, the ISO/IEC 42001 standard establishes requirements for AI management systems and could serve as a solid foundation for demonstrating compliance with key AI Act obligations, including those relating to governance, risk management, and transparency.

Trellix: Advocates mechanisms for mutual recognition and equivalence across regimes to eliminate duplicative compliance work.

Promoting compliance efficiency: Establishing mechanisms for the mutual recognition of compliance efforts to eliminate duplicative work.

European Tech Alliance: Warns of conflicts between NIS2 and GDPR and calls for alignment to avoid redundant or blocked incident reporting.

There are concerns about potential conflicts between NIS-2 requirements and GDPR obligations.

Ibec: Urges incentives for industry participation in developing harmonized EU certification schemes and codes to aid compliance.

Industry should be incentivised to develop/participate in the development of certification schemes and codesvii to aid compliance.

Schneider Electric: Encourages recognition of widely adopted international cybersecurity standards as foundational tools for demonstrating EU regulatory compliance.

Broadly adopted international cybersecurity standards and frameworks such as the ISO/IEC 2700X series, ISA/IEC 62443, and the NIST Cybersecurity Framework should be recognised and leveraged as foundational tools for demonstrating compliance with European regulations like the NIS2 directive, the CRA, the Data Act, and the GDPR, provided they align with European requirements.

: Contends that existing international standards and best practices already address cybersecurity protection needs, reducing the need for new prescriptive rules.

Stop thinking that businesses need such regulations to protect themselves from cybercriminals, there are already international standards and best practices that deal with these aspects.

Vodafone Group: Calls for EU-wide adoption and mutual recognition of international standards and certification schemes such as ISO/IEC 27001 and NESAS, noting current fragmentation.

Promote the adoption and mutual recognition of international standards and certification schemes.

European AI Forum: Advocates automatic EU-wide recognition of AI certifications and compliance verifications to reduce duplication and support scalability.

Ensure that compliance verifications or certifications approved by one competent authority are recognised EU-wide.

Alcon Laboratories Inc: Requests mutual reliance arrangements to recognize foreign certifications for certain device categories.

Recognize foreign certifications (e.g., FDA, MHLW) for certain device categories under mutual reliance agreements

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Proposes a common EU mechanism to demonstrate compliance against identified international cybersecurity standards to lower implementation costs.

For demonstrating compliance with cybersecurity risk-management measures, German industry urges the European Commission and Member States to establish a common mechanism via which companies can demonstrate the responsible national authorities across the EU that they fulfil the European requirements against one or more clearly identified international cyber security standard (like the ISO270xx family).

Business & Science Poland: Encourages recognition of industry certification programs and global frameworks, preferring international standards over EU-only approaches to bridge compliance gaps.

Gen Digital: Urges EU acceptance and recognition of global cybersecurity standards to streamline compliance.

DigitalTrade4.EU: Supports union-wide mutual recognition via mutual recognition agreements to reduce duplicative assessments.

Cisco: Recommends mutual recognition of audits and certifications to cut audit burdens and accelerate compliance.

Japan Business Council in Europe (JBCE): Calls for recognizing UNECE UN R155 as satisfying RED cybersecurity expectations to avoid overlap.

BusinessEurope: Advocates integrating the Cybersecurity Act framework, recognizing voluntary certificates, and avoiding mandatory duplicative schemes.

IBM: Supports mutual recognition to streamline audits and alignment of EU certification with global standards.

Confederation of Norwegian Enterprise (NHO): Calls for streamlined CRA compliance with recognition mechanisms to minimize duplicative testing and documentation.

Ecommerce Europe: Urges alignment with international standards and recognition of foreign certifications to facilitate cross-border compliance.

ITI - Information Technology Industry Council: Promotes mutual recognition and reciprocity across jurisdictions to avoid duplicative certification.

Salesforce, Inc.: Supports recognition of international standards as adequate evidence of compliance with EU cybersecurity obligations.

DOT Europe: Calls for alignment with international standards and frameworks to ensure interoperable and efficient compliance.

Association des Constructeurs Européens de Motocycles: Requests limiting overlapping requirements and allowing UNECE alternatives to meet EU obligations efficiently.

Comitato Elettrotecnico Italiano - CEI: Encourages collaboration between ESOs and ENISA to align standards and guidance for coherent certification.

Centre for Cybersecurity Belgium: Supports mutual recognition mechanisms and favors CRA as the primary vehicle over RED for consistent cybersecurity requirements.

Forvis Mazars: Advocates streamlined certification processes and mutual recognition to reduce compliance overheads.

NCC Group: Proposes mutual recognition of accredited cybersecurity laboratories to avoid repeated testing across markets.

Business Software Alliance: Calls for mutual recognition of audits and alignment with international standards to lower costs and improve consistency.

Connect Europe: Urges harmonized standards and recognition of audits to reduce fragmentation and duplication.

Charter of Trust: Promotes global recognition via MRAs and integrated cross-regime assessments to simplify compliance.

Siemens Healthineers AG: Calls for mutual recognition of NIS2 audits to avoid duplication across Member States.

Computer & Communications Industry Association (CCIA Europe): Advocates alignment with international standards and mutual recognition to prevent fragmentation and reduce burdens.

Palo Alto Networks: Supports mutual recognition and integration of international standards into EU frameworks to streamline compliance.

European Savings and Retail Banking Group: Encourages voluntary European standards from ESOs to underpin consistent cybersecurity compliance.

SAP SE: Urges recognition of international standards and competent bodies to facilitate efficient compliance across jurisdictions.

Data & Technology for Compliance Alliance: Promotes alignment with international standards to enable interoperable compliance and reduce redundancy.

Eurosmart: Suggests linking compliance obligations to adoption of recognized standards to provide clear, efficient pathways.

Dedalus S.p.A.: Calls for ENISA guidance aligned with international standards to ensure coherent, cross-border cybersecurity compliance.

DIGITALEUROPE: Advocates mutual recognition of NIS2 audits and cybersecurity certifications, leveraging the NLF and standards while clarifying that international standards alone may not guarantee compliance.

AMETIC: Seeks mutual recognition across EU and international frameworks to minimize duplicative compliance.

OpenAI: Encourages industry-led convergence on standards and mutual recognition to keep pace with innovation while ensuring security.

Confederation of Swedish Enterprise: Supports global mutual recognition of certifications to facilitate international market access and reduce costs.

1.8.3 Conformity Assessment, Accreditation & Oversight

This category captures efforts to align cybersecurity conformity assessment, accreditation, and oversight across EU instruments to reduce duplication and improve comparability. Stakeholders call for centralized, harmonized approaches spanning NIS2, DORA, CRA, and the ECCF, mutual recognition and consolidation of national and sectoral schemes, and structural alignment with ISO. Recognition of CSA schemes (e.g., EUCC) as compliance pathways under the CRA and the use of common specifications where harmonized standards are not yet available are seen as practical bridges, alongside clearer scope definitions and maintenance procedures for certification schemes. A strong emphasis is placed on accreditation quality and supervisory coherence: uniformly assessing Notified Bodies, expanding NB capacity, and safeguarding their independence through economic measures. Oversight efficiency should improve by sharing supervisory audit results (e.g., ESAs' JET under DORA) to avoid duplicative audits, even as some sectors still require institutions to conduct their own assessments despite certifications. With ongoing standardization delays, these measures aim to balance efficiency with high protection levels, ensuring consistent assurance and trust in the European regulatory ecosystem.

In parallel, FERMA recommends introducing a centralized conformity assessment framework to address inconsistent requirements under NIS2, DORA, and CRA. (FERMA - Federation of European Risk Managers Associations)

Ensuring a uniform assessment of Notified Bodies by Member States' Competent Authorities is essential to maintain consistency, credibility, and trust in the European regulatory system. (TEAM-NB)

Consequently, even with recognised certifications, financial institutions are still required to con- duct their own audits. (German Insurance Association)

In practice, however, internal estimates from CEN-CENELEC's JTC21 - the group responsible for drafting these standards - suggest that the first standards may not be ready before mid-2026, and full availability may not be achieved before end of 2026. (Bitkom e.V.)

DATEV eG: Calls to avoid duplicate national certification structures within the ECCF and to harmonise schemes aligned with ISO to ensure comparability and consistency.

Within the EU Cybersecurity Certification Framework (ECCF), duplicate certification structures at national level (e.g. C5 and EUCS) should be avoided.

FERMA - Federation of European Risk Managers Associations: Recommends a centralized conformity assessment framework to resolve inconsistencies across NIS2, DORA, and CRA, creating cross-regulatory alignment and reduced burdens.

In parallel, FERMA recommends introducing a centralized conformity assessment framework to address inconsistent requirements under NIS2, DORA, and CRA.

TIC Council: Urges recognition of Cybersecurity Act schemes (e.g., EUCC) as valid pathways to CRA compliance, giving industry flexible, efficient conformity options.

Through secondary legislation, recognise Cybersecurity Act (CSA) schemes such as EUCC as a pathway to compliance under the CRA for important and critical products.

ZVEI e.V.: Advocates using common specifications where harmonised standards are not yet available and underscores that standards play a central role in conformity, not just implementation.

Use common specifications when harmonised standards are not yet available.

Enel SpA: Calls for clarifying the ECCF's risk scope and formalising maintenance procedures for certification schemes to ensure continuity and relevance over time.

Formalisation of procedures for the maintenance phase of certification schemes, ensuring continuity and relevance over time.

German Insurance Association: Supports allowing access to ESAs' Joint Examination Team audit results to reduce duplicative audits and notes current rules still force institutions to conduct their own audits despite certifications.

This could potentially eliminate the need for duplicative audits by each institution of the same service provider.

Bitkom e.V.: Warns that key standards may not be available until mid-to-late 2026, risking delays for conformity assessment and certification timelines.

In practice, however, internal estimates from CEN-CENELEC's JTC21 - the group responsible for drafting these standards - suggest that the first standards may not be ready before mid-2026, and full availability may not be achieved before end of 2026.

TEAM-NB: Calls for uniform, harmonized assessments of Notified Bodies across Member States, adequate NB capacity, and economic safeguards to uphold impartiality and high protection standards.

Ensuring a uniform assessment of Notified Bodies by Member States' Competent Authorities is essential to maintain consistency, credibility, and trust in the European regulatory system.

Alcon Laboratories Inc: Urges expanding Notified Body capacity and improving transparency in designation and scope to ensure timely, credible conformity assessments.

Expand Notified Body capacity and improve transparency in designation and scope

WKÖ - Austrian Federal Economic Chamber: Supports harmonising and mutually recognising existing certification and assessment schemes to reduce effort, while viewing voluntary schemes as only moderately useful.

In the interests of harmonizing existing European cybersecurity legislation, we recommend further consolidating and mutually recognizing existing national and sectoral certification and assessment schemes.

American Chamber of Commerce to the EU: Supports establishing centralized conformity assessments to streamline oversight and coherence across cybersecurity-related regulations.

Business & Science Poland: Highlights manufacturers' challenges navigating overlapping certification requirements and calls for clearer, streamlined conformity pathways.

Telekom Austria AG: Seeks to minimise overlapping security assessments and duplicative CE-related conformity steps, and asks that group-wide audits be recognised for NIS2 compliance.

BusinessEurope: Advocates automatic compliance pathways under the RED delegated act to align assessments and reduce administrative burden.

European Signature Dialog: Encourages enabling automated verification in conformity processes and rejecting hybrid mandates that complicate oversight.

Intesa Sanpaolo: Emphasises neutrality and independence in certification bodies to bolster trust, credibility, and effective oversight.

European Justice Forum: Argues that compliance with recognised standards and certifications should rebut presumptions of defect, strengthening legal certainty.

Ireland - Department of Enterprise, Tourism and Employment: Recommends linking enforcement with strengthened, harmonised certification mechanisms to ensure consistent oversight and compliance.

ITI - Information Technology Industry Council: Urges limiting mandatory third-party assessments under the RED in favour of risk-based self-assessment where appropriate.

Association of Netherlands Municipalities: Promotes adoption of sectoral codes of conduct and certification schemes to support consistent compliance among municipalities.

Federation of European Securities Exchanges: Recommends relying on accredited audits and certifications to harmonise oversight across the financial sector and reduce duplication.

SGI Europe: Supports voluntary codes of conduct and certification schemes as pragmatic tools to improve compliance without excessive burdens.

Bocconi University: Proposes a unified, modular conformity assessment framework to align requirements across sectors and improve efficiency and scalability.

Orgalim - Europe's Technology Industries: Calls to allow Module A self-assessment where suitable and to keep CSA schemes voluntary to avoid unnecessary burdens.

Cigref: Advocates centralized, harmonised conformity assessments to streamline compliance across multiple overlapping regulations.

Insurance Europe: Encourages leveraging ESAs audits and recognised certifications to minimise duplication, and calls for strong stakeholder participation in certification governance.

Siemens Healthineers AG: Warns that Notified Body capacity is insufficient for upcoming requirements, risking bottlenecks, and calls for capacity-building measures.

Palo Alto Networks: Supports voluntary, standards-based certification and self-assessment options to maintain agility while ensuring security assurance.

Danish Industry: Calls for reassessing the scope of mandatory third-party conformity assessments and adopting proportionate, risk-based approaches.

Zentralverband Deutsches Baugewerbe: Asks to waive certification in low-risk scenarios and accept self-declarations to streamline conformity and reduce burdens on SMEs.

DIGITALEUROPE: Highlights a mismatch between conformity assessment demand and available capacity, urging planning, phasing, and reliance on international standards to mitigate.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Notes shortcomings of certification in practice and advocates flexible, iterative approaches and oversight to handle evolving risks.

APPLiA (Home Appliance Europe): Promotes industry-led, voluntary, standards-based certification schemes to ensure practicality, scalability, and alignment with innovation.

1.8.4 Risk-Based, Outcome-Focused Assurance

Risk-Based, Outcome-Focused Assurance centers on proportional, flexible cybersecurity obligations and certification that align with real-world risks and measurable security outcomes. Stakeholders advocate default self-assessment with voluntary, limited certification, recognition of proportionate voluntary schemes, and harmonised risk-based regulation that privileges effectiveness over box-checking. Assurance should be threat-led (including flexible TLPT), informed by shared risk models and cyber threat intelligence (CTI), supported by a standardized audit chain and risk evaluation, and coordinated with DORA oversight where alternatives are warranted. Sector voices—from rail to energy and software—also call for coherence with the CRA and for EUTIR to strengthen resilience and preparedness. Operationally, this means enabling compensating controls when certification is impractical, including permitting alternative mitigations for complex extensions (e.g., restricting use to trusted environments, limiting exposure, or applying safeguards), and allowing use of uncertified products with risk-based mitigation. Obligations and assurance are tailored to context and risk, with transparent communication of residual risks and documented exemptions, maintaining a

technical, risk-based, outcome-focused certification posture that delivers tangible security improvements without unnecessary burden.

> *For project extensions that face interoperability or technical compatibility challenges, railway suppliers seek permission to use alternative mitigation measures, such as restricting use to trusted environments, limiting system exposure, or applying safeguards.* (ALSTOM)
>
> *These risks should be clearly communicated to customers, and a corresponding exemption should be included in the CRA.* (ALSTOM)

ALSTOM: They urge regulators to allow risk-based alternative mitigations for project extensions facing interoperability or compatibility constraints, with transparent risk communication and appropriate CRA exemptions. This prioritizes outcomes by enabling practical safeguards when full compliance is infeasible.

> *For project extensions that face interoperability or technical compatibility challenges, railway suppliers seek permission to use alternative mitigation measures, such as restricting use to trusted environments, limiting system exposure, or applying safeguards.*

DigitalTrade4.EU: Advocates an EUTIR framework to bolster resilience and preparedness, aligning assurance with real-world risk and response capabilities. The emphasis is on outcomes that improve defensive readiness rather than prescriptive certification.

EVOLIS: Calls for a holistic cybersecurity approach that aligns assurance to risk across systems and lifecycle. The focus is on coherent, outcome-oriented measures rather than one-size-fits-all requirements.

Federation of Austrian Industries: Supports proportionate, voluntary recognition of certifications to align obligations with product risk. This approach aims for outcome-focused assurance while minimizing unnecessary compliance burdens.

Mafex – Spanish Railway Association: Backs coherent, tailored CRA rules calibrated to sector and product risk. The goal is pragmatic, outcome-driven assurance that fits railway-specific contexts.

Outpacr / VAICE: Proposes standardized audit chains and consistent risk evaluation to ensure comparable, risk-based assurance across the supply chain. Standardization targets outcomes like traceability and measurable security improvements.

Comitato Elettrotecnico Italiano - CEI: Encourages shared risk models and cyber threat intelligence to drive consistent, risk-based evaluations. This supports outcome-focused assurance grounded in common understanding of threats and impacts.

Google: Recommends keeping certification voluntary and scoped to higher risks to maintain agility and focus on meaningful outcomes. Mandatory, broad certification is discouraged in favor of proportionate assurance.

Business Software Alliance: Favors default self-assessment complemented by optional certification, expanding voluntary pathways. This enables risk-proportional, outcome-oriented assurance without excessive overhead.

Connect Europe: Endorses risk-based, threat-led testing to validate security against realistic adversaries. The approach measures outcomes by demonstrating resilience under plausible attack scenarios.

Palo Alto Networks: Advocates maintaining a technical, risk-based, outcome-focused certification regime. Assurance should prioritize practical security results over procedural compliance.

Eurosmart: Promotes harmonized, risk-based regulation and allows use of uncertified products when mitigations reduce risk sufficiently. The emphasis is on measured outcomes enabled by compensating controls.

ECIS, European Committee for Interoperable Systems: Supports flexible alternatives under DORA oversight and adaptable TLPT methodologies to achieve effective, risk-based assurance. Flexibility is used to optimize real security outcomes.

WindEurope: Calls for cybersecurity obligations and certification proportionate to risk. The objective is outcome-focused assurance that strengthens the sector without unnecessary burdens.

1.8.5 Scope, Sectoral Schemes & Guidance

Stakeholders call for clear, consistently applied scope definitions and guidance across EU cybersecurity laws (CRA, NIS2, DORA, RED, AI Act). They seek Commission guidance and ENISA-led mapping to international standards to avoid fragmented interpretations, enable predictable compliance, and support a unified yet flexible certification framework. Key asks include clarifying CRA coverage, the notion of "substantial modification," CE marking for software/app-store distribution, and modular hardware/software certification; aligning sectoral and international standards; and keeping certification voluntary or proportionate, with geographic and product-boundary limits where appropriate (e.g., excluding stand-alone AI software that does not control hardware or network-critical functions). Sectoral schemes and proportionality feature prominently: telecom operators note ambiguity for ECN use cases under the AI Act; automotive and industrial stakeholders urge limiting CRA obligations to essential Annex I requirements for internal-use products; video-gaming raises the impracticality of decade-long update duties; logistics propose carving intra-group ICT units out of NIS2 with responsibility assigned to regulated consuming entities; and multiple actors request EU-wide criteria for NIS2 training. Several submissions advocate coherence safeguards (ENISA's technical neutrality, interoperability derogations, RED DA adjustments for B2B) and alignment among CRA, NIS2, and DORA to reduce overlap and ensure market-facing, proportionate enforcement.

> *In this vein, we would like to take the opportunity to highlight that the scope of the Cyber Resilience Act (CRA) is not clearly defined, as is the issue of the notion of 'substantial modification', and recall that the Commission is empowered to provide guidance under Article 26(2)a) and d) of the CRA.* (Video Games Europe)

> *ENISA must be empowered to conduct a comprehensive coherence and simplification analysis and a mapping exercise to EU requirements with international standards, making compliance predictable and consistent.* (Telefonica, S.A.)

> *Where services that would otherwise fall under NIS2 are provided exclusively intra-group, the providing entity should be out of scope of NIS2 and of Implementing Regulation (EU) 2024/2690; the regulatory obligations should instead attach to the in-scope operating entities that consume those services, managed through their supply-chain controls and consolidated accountability.* (European Express Association (EEA))

> *Exclude stand-alone software Al applications from CRA obligations unless they control hardware or network-critical functions.* (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Video Games Europe: Calls for clearer CRA scope, definitions of substantial modification, and practical guidance on CE marking for app store–distributed software, noting that long update obligations are unsuitable for consoles.

> *In this vein, we would like to take the opportunity to highlight that the scope of the Cyber Resilience Act (CRA) is not clearly defined, as is the issue of the notion of 'substantial modification', and recall that the Commission is empowered to provide guidance under Article 26(2)a) and d) of the CRA.*

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Recommends excluding stand-alone AI software from CRA obligations unless it governs hardware or network-critical functions, to right-size scope.

> *Exclude stand-alone software Al applications from CRA obligations unless they control hardware or network-critical functions.*

Telefonica, S.A.: Urges a unified, internationally aligned certification framework and coherent standards, with clear Commission guidance to avoid fragmented interpretations, especially for telecom AI use.

To ensure consistent and effective implementation, it is crucial that the European Commission provides clear and detailed guidance.

European Express Association (EEA): Advocates carving out intra-group ICT service units from NIS2 and the implementing regulation, shifting accountability to in-scope operating entities through supply chain controls.

Where services that would otherwise fall under NIS2 are provided exclusively intra-group, the providing entity should be out of scope of NIS2 and of Implementing Regulation (EU) 2024/2690; the regulatory obligations should instead attach to the in-scope operating entities that consume those services, managed through their supply-chain controls and consolidated accountability.

WKÖ - Austrian Federal Economic Chamber: Stresses maintaining technical neutrality in EU cybersecurity work and respecting operators' long-term provider choices made under the 5G toolbox context.

However, this task must always be implemented under the condition that ENISA's technically neutral work is not jeopardized or instrumentalized.

ACEA (European Automobile Manufacturers' Association): Supports limiting CRA obligations for certain automotive internal-use products to Annex I essential cybersecurity requirements, avoiding disproportionate burdens from additional conformity elements.

Alternatively, if a full exclusion is not adopted, the CRA's application to such products should be limited to the essential cybersecurity requirements outlined in Annex I.

American Chamber of Commerce to the EU: Calls to simplify and narrow the CRA's scope to reduce unnecessary overlap and compliance complexity across sectors.

CECE - Committee for European Construction Equipment: Notes that CRA compliance already addresses certain essential health and safety requirements for machinery, and urges coordination to prevent duplication.

Fédération des Industries Ferroviaires: Requests targeted CRA derogations where interoperability obligations or product extensions would otherwise be hindered, aligning sector rules with cybersecurity duties.

Business & Science Poland: Highlights mismatches between hardware and software certification approaches and seeks clarity on certification of pre-installed applications. Proposes separating hardware and software certification paths.

Elia Group: Seeks guidance to ensure cybersecurity compliance for decentralized energy assets and consistent application of cross-regime requirements.

Bayerische Motoren Werke Aktiengesellschaft: Asks for clear, harmonized criteria for NIS2-related cybersecurity training to ensure consistent application across operations.

VDMA - Advancing Europe´s machinery industry: Points to uncertainty in NIS2 entity classifications and requests clearer guidance to determine obligations consistently.

Japan Business Council in Europe (JBCE): Calls for clarity on CRA product classifications and the treatment of substantial modifications to ensure predictable compliance.

Federation of Austrian Industries: Urges exemptions for affiliates providing intra-group services under NIS2 Article 22(5), aligning obligations with the regulated operating entities.

Confederation of Norwegian Enterprise (NHO): Supports group-level exemptions for internal ICT providers and streamlining NIS2 obligations to minimize duplication and ambiguity.

Intesa Sanpaolo: Requests clearer scoping and alignment between DORA, CRA, and NIS2 to delineate responsibilities and avoid overlap for financial institutions and their providers.

Outpacr / VAICE: Urges recognition of real-time industrial systems and allowances for self-assessments where appropriate, with guidance tuned to operational constraints.

MedTech Europe: Advocates keeping cybersecurity certification voluntary and aligned with international standards in the medical technology sector.

ITI - Information Technology Industry Council: Seeks clarity on NIS2 and CRA scope boundaries and proposes geographic limits to CRA obligations, while ensuring cybersecurity-only components are not misclassified as safety elements.

Federation of European Securities Exchanges: Encourages allowing ICT providers to deliver security training under clear criteria, aligning sectoral responsibilities with practical expertise.

Verband der Automobilindustrie e.V.: Requests EU-wide, harmonized criteria for NIS2-related training in the automotive sector to ensure consistent compliance.

Association des Constructeurs Européens de Motocycles: Calls for EU-wide, harmonized NIS2 training criteria for motorcycle manufacturers to support uniform implementation.

Comitato Elettrotecnico Italiano - CEI: Endorses the EUCC cybersecurity certification scheme provided integration safeguards prevent duplication and ensure alignment with existing standards.

CLEPA: Asks for clear boundaries and guidance between CRA and NIS2 scopes to avoid double regulation and conflicting duties in the automotive supply chain.

Broadcom: Supports aligning NIS2 and DORA requirements through ENISA's mapping and seeks clarity on processing obligations to reduce fragmentation.

Orgalim - Europe's Technology Industries: Urges harmonized classification rules for NIS2 providers to ensure consistent treatment across Member States and sectors.

Connect Europe: Calls for clearer allocation of responsibilities, calibrated scope, and moderated audit requirements under DORA to avoid disproportionate burdens.

Cigref: Requests guidance on when CE marking suffices for demonstrating cybersecurity conformity and how it interacts with other sectoral schemes.

Global Data Alliance: Supports voluntary, standards-based cybersecurity certifications with international alignment to facilitate cross-border compliance.

Palo Alto Networks: Proposes establishing a European Cyber Readiness Framework to align sectoral expectations, streamline assessments, and raise baseline security.

SAP SE: Seeks clarity on CRA scope for remote digital product services and related exclusions to ensure predictable obligations for enterprise software.

Danish Industry: Recommends withdrawing the RED delegated act for B2B contexts and clarifying definitions of critical products to focus obligations where risk is highest.

WindEurope: Calls for guidance ensuring sectoral schemes adequately cover critical infrastructure cybersecurity needs in the wind energy ecosystem.

Schaeffler AG: Proposes limiting CRA scope to products with bidirectional data exchange to better target cybersecurity obligations.

1.8.6 Technical Baselines & Cryptography

Technical Baselines & Cryptography (within Cybersecurity & Certification Alignment) focuses on turning high-level regulatory cybersecurity mandates into concrete, measurable technical baselines and robust cryptographic practices. Stakeholders highlight that requirements like an "adequate level of cybersecurity" lack defined

baselines, generating costly uncertainty and making it hard to prove compliance. This gap is exacerbated by limited guidance on incident severity classification and response timelines, which undermines consistent certification and audit readiness. To close these gaps, the emphasis is on harmonizing standards (e.g., ISO/IEC, including 18031 for cryptographic random number generation) under the CRA and privileging outcome-based requirements over prescriptive controls. Priorities include maintaining strong encryption, clarifying "no data in clear" transfer expectations, and avoiding overly explicit references to particular encryption mechanisms to preserve flexibility and future-proofing.

> *The AIA requires providers to ensure an "adequate level of cybersecurity," yet it does not define any specific technical baseline for compliance.* (Meta Platforms Ireland Limited)
>
> *As a result, organisations face open-ended expenditures with no clear path to measurable compliance certainty.* (Meta Platforms Ireland Limited)
>
> *Furthermore, standards organizations such as ISO/IEC currently offer no guidance regarding incident severity or response deadlines.* (Meta Platforms Ireland Limited)
>
> **Meta Platforms Ireland Limited:** The document flags that the AIA's lack of defined technical cybersecurity baselines creates compliance uncertainty and costs, and calls for measurable baselines and clearer incident severity and response expectations.
>
> *The AIA requires providers to ensure an "adequate level of cybersecurity," yet it does not define any specific technical baseline for compliance.*
>
> **Intesa Sanpaolo:** The document urges removing explicit references to encryption to avoid prescriptive requirements and preserve flexibility in meeting cybersecurity objectives.
>
> **Salesforce, Inc.:** The document seeks clarification that data should never be transmitted in the clear, establishing an explicit baseline for protected data transfer.
>
> **Orgalim - Europe's Technology Industries:** The document supports using harmonised standards, notably ISO/IEC 18031, within the CRA to align cryptographic technical baselines across industry.
>
> **AMETIC:** The document advocates maintaining strong encryption standards as a core element of cybersecurity baselines.

1.8.7 Secure-by-Design & AI Assurance

This category emphasizes making AI secure-by-design across the lifecycle and aligning cybersecurity and assurance regimes. Stakeholders call for embedding security principles into AI systems and data platforms to strengthen critical infrastructure resilience, encouraging voluntary secure development practices, and harmonizing "secure AI by design" approaches. They also highlight the need for user-friendly cybersecurity, accountability and escalation consistent with the Cyber Resilience Act, AI-enabled defenses and information sharing, harmonized AI/data standards, and clearer AI Act provisions for cybersecurity use cases. Assurance and certification challenges—especially for stochastic AI models—are flagged, urging pragmatic, risk-based certification pathways. Certification alignment extends beyond technical controls to governance compatibility. Proposals include ethical interoperability so that systems built under African principles (e.g., Ubuntu ethics, community data stewardship) can be recognized within simplified EU certification paths. To balance assurance with security and IP protection, several stakeholders oppose routine regulatory access to source code, arguing for proportionate oversight mechanisms that reduce breach risk while still enabling accountability.

> *The implementation of the Al Act and updates to data governance rules should embed security-by-design principles, ensuring that AI tools and data platforms strengthen, rather than weaken, critical infrastructure resilience.* (European Energy Information Sharing and Analysis Centre)
>
> *The Omnibus should therefore encourage voluntary secure software development practices.* (Video Games Europe)
>
> *The Omnibus should encourage the creation of ethical interoperability frameworks, ensuring that AI systems developed under African governance principles (e.g., Ubuntu ethics, community data stewardship) are recognised as legitimate within simplified EU certification paths.* ()
>
> *Authorities requesting source code access may not have the technical means and sufficient resources to avoid data breaches and have the code accessed by malicious actors.* (Technology Industries of Finland)

Technology Industries of Finland: Argues against granting market surveillance authorities access to AI source code, warning it increases exposure and exceeds authorities' capabilities. Urges removal of such provisions to protect security, IP, and system integrity.

Art. 74(13) and Art 92(3): Delete the possibility for market surveillance authorities to access the source code of an AI system or a GPAI model.

European Energy Information Sharing and Analysis Centre: Urges the AI Act and data governance updates to embed security-by-design so AI and data platforms bolster critical infrastructure resilience. Emphasizes integrating cybersecurity from the outset.

The implementation of the Al Act and updates to data governance rules should embed security-by-design principles, ensuring that AI tools and data platforms strengthen, rather than weaken, critical infrastructure resilience.

Video Games Europe: Recommends promoting voluntary secure software development practices within the sector to mitigate risks and build trust. Positions secure-by-design as a driver of player safety and sustainable growth.

The Omnibus should therefore encourage voluntary secure software development practices.

: Calls for ethical interoperability frameworks so AI built under African governance principles can be recognized within streamlined EU certification. Links culturally grounded ethics to practical assurance and certification alignment.

The Omnibus should encourage the creation of ethical interoperability frameworks, ensuring that AI systems developed under African governance principles (e.g., Ubuntu ethics, community data stewardship) are recognised as legitimate within simplified EU certification paths.

Healthtech Finland: Highlights the difficulty of certifying stochastic AI models under traditional assurance regimes. Calls for adaptable, risk-appropriate certification approaches to reflect probabilistic behavior.

ENCIRCLE Research Consortium: Advocates for user-friendly cybersecurity measures that make secure-by-design practical for end users. Stresses ease-of-use as key to effective assurance and adoption.

Connect Europe: Supports harmonized AI data standards and certification to enable interoperability and consistent assurance across the EU. Aims to reduce fragmentation and simplify compliance.

OpenSSF: Backs clearer accountability and escalation mechanisms under the Cyber Resilience Act to strengthen software supply chain assurance. Seeks enforceable, transparent responsibilities aligned with secure-by-design.

Palo Alto Networks: Promotes harmonized secure-by-design requirements for AI and increased use of AI-enabled defenses and information sharing. Seeks coordinated guardrails that enhance security outcomes and assurance.

CrowdStrike: Requests clarification of AI Act provisions for cybersecurity to ensure defenders can innovate while meeting compliance. Emphasizes predictable, security-supportive obligations.

1.8.8 Supply Chain Security & SBOM Assurance

Supply Chain Security & SBOM Assurance focuses on end-to-end, risk-based control of third-party software and ICT vendors under evolving EU obligations (e.g., CRA). Insights underscore the difficulty of achieving full compliance across multi-tier value chains—especially in sectors integrating legacy and COTS components—where organizations must document their own and partners' processes, align policies, and maintain traceability. To reduce burdens (notably for SMEs), stakeholders call for clear third-party classification/management methods, voluntary harmonised assessment templates, and standard contractual clauses, complemented by limits on ICT subcontracting to shrink the attack and compliance surface. For SBOM assurance, the corpus advocates a minimal, interoperable SBOM profile and chain-of-custody transparency so component provenance, vulnerabilities, and updates can be tracked consistently across suppliers. Coupled with legal clarity and

flexibility (aligned with ENISA recommendations), these measures aim to standardize evidence, enable proportionate supplier attestations, speed vendor onboarding, and strengthen certification alignment—improving resilience while curbing delays, costs, and administrative overhead.

> *In the railway sector, where systems are developed through the integration of multiple products and often include legacy and COTS (Commercial Off-The-Shelf) components, achieving and maintaining full compliance with the CRA across the entire supply chain represents a major challenge.* (ANIE Federazione - ANIE ASSIFER)
>
> *Voluntary, harmonised templates should be developed for assessing cybersecurity in the supply chain to make the process more efficient and less burdensome, especially for SMEs.* (Finnish Food and Drink Industries´ Federation (ETL))
>
> *This web of obligations directly affects vendor contracting, leading to delays, increased costs, and higher administrative burdens, even in relatively simple business arrangements.* (Adigital (Asociación Española de la Economía Digital))
>
> *It is proposed to grant legal clarity and flexibility for suppliers to define their own compliance standards within the supply chain, following the ENISA recommendation model.* (Adigital (Asociación Española de la Economía Digital))

ANIE Federazione - ANIE ASSIFER: The CRA's expanded manufacturer responsibilities collide with the railway sector's multi-vendor, legacy/COTS-heavy systems, making end-to-end supply chain compliance and assurance difficult to achieve and maintain.

> *In the railway sector, where systems are developed through the integration of multiple products and often include legacy and COTS (Commercial Off-The-Shelf) components, achieving and maintaining full compliance with the CRA across the entire supply chain represents a major challenge.*

Finnish Food and Drink Industries´ Federation (ETL): Calls for voluntary, harmonised supplier cybersecurity assessment templates to streamline due diligence across the chain and reduce burdens, particularly for SMEs.

> *Voluntary, harmonised templates should be developed for assessing cybersecurity in the supply chain to make the process more efficient and less burdensome, especially for SMEs.*

Adigital (Asociación Española de la Economía Digital): Urges clear methodologies to classify and manage third parties and greater legal flexibility so suppliers can meet requirements in scalable ways, reducing documentation burdens, delays, and costs in fragmented supply chains.

> *It is proposed to grant legal clarity and flexibility for suppliers to define their own compliance standards within the supply chain, following the ENISA recommendation model.*

DigitalTrade4.EU: Promotes transparent compliance via an auditable chain-of-custody across the supply ecosystem, enabling verifiable, end-to-end assurance of components and processes.

Mafex – Spanish Railway Association: Highlights traceability and CRA compliance challenges in complex, multi-tier railway supply chains, where integrating legacy and COTS components impedes end-to-end assurance.

Inter IKEA Group: Advocates standardized contractual clauses to embed cybersecurity and assurance obligations in supplier agreements, improving consistency and oversight across the chain.

ENCIRCLE Research Consortium: Recommends a minimal, standard SBOM profile to ensure practical, interoperable component transparency and vulnerability management across suppliers.

Federation of European Securities Exchanges: Supports simplifying and limiting ICT subcontracting chains to preserve oversight of third parties and reduce compounded supply chain cyber risk.

Charter of Trust: Calls to strengthen supply chain security with common requirements and vendor assurance practices to mitigate systemic vulnerabilities across ecosystems.

1.8.9 Digital Identity & Trust Services (eIDAS/QSCD)

This category centers on aligning and modernizing EU digital identity and trust services under eIDAS, with a strong focus on QSCD lifecycle management, continuity, and long-term verifiability. Providers highlight the operational risks of the current five-year QSCD certification cap and biennial assessments, advocating a risk-based grace and assisted-migration clause to avoid cliff-edge disruptions. They also call for formal recognition of preservation services (LTA/LTV policies, periodic trusted timestamping), modular compliance for Wallet Providers leveraging existing QTSP certifications, standardized and prompt revocation processes, and clearer guidance on responsibilities where PSD2 SCA intersects with eIDAS SUA. A key theme is enabling secure, fully automated identity proofing for qualified certificates and EUDI Wallet onboarding, with outcome-focused rules and public benchmarks for biometric accuracy, PAD/IAD anti-spoofing, liveness, document checks, and deepfake defenses—rather than mandating hybrid approaches that can raise rejection rates. At the same time, stakeholders warn of testing bottlenecks and prohibitive costs given the limited number of accredited labs, urging pragmatic timelines and capacity building. They also seek reviews of standards that hinder automation or create market risks (such as the QSCD five-year limit) and clarity on the financial framework for "free-of-charge" wallet services. To prevent regulatory isolation and reduce fragmentation, the EU is urged to align CEN/CENELEC specifications with international standards (ISO, ITU-T, FIDO, W3C) and broader frameworks (OECD, G7), using European refinements rather than replacements and promoting mutual recognition. This approach supports global interoperability, compliance certainty, and access to innovative solutions while maintaining high assurance.

> *Article 30's five-year certification limit for qualified electronic signature devices, with biennial vulnerability assessments, makes QTSPs heavily reliant on manufacturers.* (Intesi Group)
>
> *Prioritise alignment with international standards (ISO, ITU-T, FIDO, W3C) in developing technical specifications.* (Amazon)
>
> *Costs for these tests alone are already quoted in the hundreds of thousands of euros, creating significant barriers not only for small providers but even for established ones.* (Entrust SAS)
>
> *If SCA is executed through a wallet outside the bank's domain, this creates uncertainty about the extent of PSP liability.* (ING Group)
>
> **Intesi Group:** Calls for a grace-and-assisted-migration clause to avoid service disruptions when QSCD certifications lapse due to manufacturers and to explicitly allow secure, fully automated identity proofing. Also urges formal recognition of preservation services and review of burdensome standards like the five-year QSCD limit and wallet funding clarity.
>
> *One possibility is to introduce a grace and assisted-migration clause: where a QSCD certification lapses for reasons attributable to the manufacturer, QTSPs should be allowed to continue controlled operation based on a documented risk assessment and targeted vulnerability testing, preventing cliff-edge service disruptions for citizens and businesses.*
>
> **Amazon:** Advocates aligning EU technical standards with international frameworks to avoid regulatory isolation and fragmentation. Urges using European refinements to ISO, ITU-T, FIDO, and W3C with mutual recognition to ensure interoperability and lower compliance costs.
>
> *Embracing international standards and mutual recognition will position the EU as a leader in global digital identity interoperability while maintaining high security standards and reducing unnecessary barriers for all providers.*
>
> **Evotrust:** Proposes a grace clause to maintain QSCD operations during manufacturer-driven certification lapses and explicitly permits fully automated identity proofing for qualified certificates and EUDI Wallet onboarding. Recommends outcome-based technical criteria and reviewing standards that hinder automation.
>
> *While its rejection is positive, EU regulations should explicitly permit fully unattended identity proofing for qualified certificates and EUDI Wallet onboarding to ensure legal clarity.*
>
> **Namirial Spa:** Recommends a modular compliance approach so Wallet Providers can leverage existing QTSP certifications instead of duplicative audits. Supports secure, fully automated remote onboarding aligned to ETSI EN 119 461 without unnecessary extra requirements.
>
> *Apply a modular compliance model under eIDAS 2, allowing Wallet Providers to demonstrate conformity through existing QTSP certifications (QES, QEAA, QeRDS) without duplicative audits.*

ING Group: Seeks clarity on the relationship between PSD2 Strong Customer Authentication and eIDAS Signature or Seal User Authentication responsibilities. Emphasizes that wallets should enable, not implement, SCA and calls for clear liability guidance when SCA is executed via wallets.

Clear guidance is needed on how PSD2 SCA relates to elDAS SUA.

Entrust SAS: Supports stronger assurance under eIDAS but warns that current biometric testing timelines, limited accredited labs, and high costs risk creating compliance bottlenecks. Also calls for standardized, prompt revocation processes to prevent misuse when roles or operations change.

However, the way testing requirements are currently structured risks creating serious compliance bottlenecks.

iProov Ltd: Argues that mandatory hybrid biometric and manual verification raises false rejection rates and user drop-off compared to state-of-the-art automated approaches. Encourages flexibility to adopt high-security automated liveness and anti-spoofing methods.

DigitalTrade4.EU: Promotes immutable, verifiable records under eIDAS to ensure legal proof and trust in cross-border trade processes. Suggests strengthening authenticity and integrity for trade documents via recognized trust services.

European Signature Dialog: Advocates default use of qualified trust services to enhance security and resilience. Seeks simplification of processes across the EU by leveraging standardized trust services.

European Signature Dialog: Calls for alignment and standardization of assurance levels, including recognition of Level of Assurance Substantial across schemes. Aims to improve cross-border interoperability and reduce duplicative compliance.

Deutscher Steuerberaterverband e.V. (DStV): Emphasizes the need for secure wallet-to-wallet communication channels aligned with eIDAS. Highlights interoperability and data protection for sensitive professional exchanges.

ASNEF: Notes increasing identity theft and fraud risks, urging stronger digital identity controls under eIDAS. Supports measures that balance security with user-friendly onboarding.

Business Software Alliance: Urges streamlining and harmonizing QTSP accreditation to accelerate adoption of trust services. Seeks reduced administrative burdens while maintaining high security and compliance.

D-Trust: Critiques the five-year QSCD certification cap and advocates robust LTV and LTA mechanisms to ensure long-term verifiability. Calls for preservation-oriented guidance to maintain probative value over time.

InfoCert: Supports secure automated identity proofing and periodic benchmarks while reviewing standards that impede automation. Urges anchoring long-term verifiability and revisiting the disruptive five-year QSCD limit.

Trans Sped: Proposes a grace period for QSCD certification lapses, explicit permission for unattended identity proofing, and simpler long-term signature preservation. Aims to prevent service disruption and maintain probative value.

Eurosmart: Warns that five-year certification caps create lifecycle strain for identity card QSCDs and issuance programs. Calls for more flexible certification or renewal approaches to maintain continuity.

Global Legal Entity Identifier Foundation (GLEIF): Promotes vLEI as a trust service component to digitally verify legal entities and representatives' authority. Enhances organizational identity assurance and authorization in digital transactions.

: Advocates a risk-based approach to QSCD certification and continuity instead of rigid binary rules, acknowledging higher operational risks and costs for remote QSCDs. Suggests easing initial certification barriers while ensuring security outcomes.

Capgemini Deutschland GmbH: Requests clear guidance on verifying Wallet Unit Attestations to support trust and interoperability. Seeks precise roles, procedures, and evidence requirements for attestation verification.

1.8.10 Lifecycle Certification & Update Management

This category advocates lifecycle-aware certification regimes that minimize disruptive re-certifications and enable safe, predictable security updates without compromising system availability. Stakeholders highlight burdens and risks in current safety certification, redundancy in update requirements, and the need to permit temporary functionality restrictions to mitigate threats during patching while maintaining operational resilience. Recommended reforms include replacing mandatory recertification with rolling validity backed by continuous oversight, decoupling hardware and software certification to permit independent upgrades, and deferring CRA assessments until system integration. Proportionate obligations calibrated to a product's digital lifetime, EU-wide certification for privacy-enhancing technologies that ensures lifetime protection, and explicit support for long-lived credentials (e.g., ID cards) address longevity and maintenance realities. To deliver these outcomes, organizations call for reorganized safety engineering principles and processes, predictable update pathways, and recognition of supply-chain erosion that can limit certification maintenance. The goal is cybersecurity and safety alignment that sustains compliance, reduces cost, and preserves availability across the full lifecycle.

Re-certification processes, which are time-consuming and resource intensive. (ANIE Federazione - ANIE ASSIFER)

Compromise of system availability during update cycles. (ANIE Federazione - ANIE ASSIFER)

Reorganization of safety engineering principles and processes. (ANIE Federazione - ANIE ASSIFER)

elimination of the mandatory recertification requirement and adoption of a rolling validity model that recognizes the rigor and continuity of existing oversight. (Alcon Laboratories Inc)

ANIE Federazione - ANIE ASSIFER: They emphasize that safety re-certification is resource-intensive and that update cycles can disrupt availability. They call for lifecycle-aligned engineering and streamlined processes.

Re-certification processes, which are time-consuming and resource intensive.

Alcon Laboratories Inc: Proposes replacing mandatory recertification with a rolling validity model to cut costs and administrative burden while maintaining safety and compliance.

elimination of the mandatory recertification requirement and adoption of a rolling validity model that recognizes the rigor and continuity of existing oversight.

Business & Science Poland: Advocates a lifecycle-oriented approach to CRA compliance, aligning certification and update obligations to product stages and long-term support.

PII Guard: Supports an EU-wide certification framework for privacy-enhancing technologies that ensures consistent, lifetime protection and maintainable updates across the lifecycle.

Telekom Austria AG: Argues that overlapping security update requirements are redundant and should be streamlined to simplify lifecycle update management.

EHIMA: Calls for predictable, safe software update pathways that preserve compliance without triggering undue recertification, enabling long-term maintenance.

Confederation of Norwegian Enterprise (NHO): Promotes proportionate CRA obligations tied to realistic digital lifetimes, balancing certification and update responsibilities over a product's lifecycle.

Google: Recommends decoupling hardware and software certification so software can be updated rapidly without full device recertification, improving lifecycle agility.

Orgalim - Europe's Technology Industries: Supports allowing temporary functionality restrictions during security updates to protect users while maintaining compliance and service continuity.

Eurosmart: Suggests deferring CRA conformity assessments for components until system integration to avoid repeated certifications over the lifecycle.

: Warns that long-lived ID cards and component erosion or supply constraints conflict with fixed certification and support caps, requiring lifecycle-appropriate maintenance policies.

1.8.11 Vulnerability Disclosure & Management

The insights emphasize a coordinated, risk-based approach to vulnerability disclosure and management that aligns EU practices with established global standards. Stakeholders support building and prioritizing a public catalog of Known Exploited Vulnerabilities (KEV) and methodological alignment of the EU Vulnerability Database with the US NVD, including adoption of CVSS, to enable consistent scoring, triage, and remediation across jurisdictions. They also call for harmonization and an EU-wide unified coordinated vulnerability disclosure (CVD) policy to streamline processes and reduce fragmentation across regulations. A recurring theme is calibrating the scope, audience, and timing of disclosures to avoid increasing risk. Industry urges limiting public disclosure—especially in critical infrastructure—favoring targeted notifications to users/customers, secure follow-up communication, and flexibility in support periods. Several contributions caution that mandatory reporting of actively exploited vulnerabilities before patches are available could undermine security, and note that vulnerabilities are inherent and dynamically managed in operational environments; therefore, compliance obligations should focus on robust vulnerability handling rather than expansive transparency that may compromise confidentiality.

Instead of collecting zero-day data, the Commission (via ENISA) should focus on establishing and maintaining a public catalog of Known Exploited Vulnerabilities (KEV). (Workday)

Furthermore, Trellix is pleased with the development of the EU Vulnerability Database (EU-VD) and strongly supports ongoing efforts to align its methodology with the US National Vulnerability Database (NVD). (Trellix)

Similarly, the requirement to report actively exploited vulnerabilities within the CRA effectively means reporting a vulnerability before the vendor has the chance to deploy patches and customers can implement them. (Emerson Electric Co.)

In situations where such vulnerabilities could be used for the provision of core services/ functions of critical national infrastructure or sensitive government structures, we believe that it should be clarified that the obligation to notify should occur after the patch has been deployed to prevent the unnecessary expansion of the attack of these essential service entities. (Emerson Electric Co.)

Workday: Advocates focusing EU efforts on a public Known Exploited Vulnerabilities catalog rather than zero-day collection to prioritize remediation of actively exploited threats.

Instead of collecting zero-day data, the Commission (via ENISA) should focus on establishing and maintaining a public catalog of Known Exploited Vulnerabilities (KEV).

Trellix: Supports aligning the EU Vulnerability Database with the US NVD and adopting CVSS to ensure consistent, cross-jurisdiction vulnerability assessment.

Furthermore, Trellix is pleased with the development of the EU Vulnerability Database (EU-VD) and strongly supports ongoing efforts to align its methodology with the US National Vulnerability Database (NVD).

Emerson Electric Co.: Urges limiting disclosure of sensitive system details and delaying notification of actively exploited vulnerabilities until patches are deployed, especially for critical infrastructure.

In situations where such vulnerabilities could be used for the provision of core services/ functions of critical national infrastructure or sensitive government structures, we believe that it should be clarified that the obligation to notify should occur after the patch has been deployed to prevent the unnecessary expansion of the attack of these essential service entities.

WKÖ - Austrian Federal Economic Chamber: Notes that vulnerabilities are ubiquitous and that operators continuously discover and remediate them, maintaining secure, high-quality services.

Network security is a dynamic field in which new vulnerabilities must be continuously discovered and remediated, which is something that Austrian communications network operators are doing, as

demonstrated by the secure and continuous provision of services and thus the high quality of service our companies have demonstrated for years.

UNIFE: Recommends restricting public disclosure of fixed vulnerabilities in the railway sector, favoring targeted notification to users in justified cases.

It should thus be clarified that targeted information to the customer/ user specifically is sufficient in duly justified cases like critical infrastructure sectors etc.

American Chamber of Commerce to the EU: Opposes mandates to disclose zero-day vulnerabilities.

Swedtrain - the Swedish Railway Industry Association: Advocates limiting the scope of vulnerability disclosure in the rail industry to reduce security risks.

Fédération des Industries Ferroviaires: Calls for limiting the scope of vulnerability disclosure to protect operational security in rail systems.

CECIMO - European Association of Manufacturing Technologies: Supports secure, structured follow-up communication with stakeholders after vulnerability identification and remediation.

CLEPA: Prefers flexible support periods for vulnerability management to balance product lifecycles, risk, and resource constraints.

Eurosmart: Calls for harmonized vulnerability management requirements across EU regulations to ensure consistency and reduce fragmentation.

DIGITALEUROPE: Proposes an EU-wide coordinated vulnerability disclosure policy and limiting compliance obligations to vulnerability handling activities.

1.8.12 Miscellaneous

This Miscellaneous category under Cybersecurity & Certification Alignment highlights cross-sector efforts to strengthen operational resilience through collaboration, shared intelligence, and regulatory compliance. It emphasizes operational support and intelligence-sharing mechanisms (EE-ISAC), public-private partnerships to spread threat intelligence and best-practice guidance, especially for SMEs, and rapid alignment with EU rules like DORA in the financial sector to raise baseline cybersecurity. It also focuses on safeguards for responsible public data collection: continuous monitoring of domain health during collection, rate limiting to avoid DoS/DDoS impacts, and strict scoping to publicly accessible internet data that excludes restricted login areas. Complementary themes include maintaining data security obligations, promoting managed cybersecurity services to help organizations meet requirements, and mobilizing startup ecosystems to support EU cybersecurity objectives, pointing to an ecosystem approach that blends compliance, shared capabilities, and service-based support.

EE-ISAC stands ready to support the Commission and its stakeholders with operational expertise, intelligence-sharing experience, and practical insights from the energy sector. (European Energy Information Sharing and Analysis Centre)

The Digital Operational Resilience Act (DORA) ensures a high level of cybersecurity, and the financial sector has made great efforts to implement its requirements in a very short time. (German Insurance Association)

Domain health monitoring entails continuous monitoring of website responsiveness during collection to prevent degradation of services of the target internet location. (Alliance for Responsible Data Collection)

Multiple methods of rate limitation are available to protect the domain health of internet locations and help prevent DDoS/DoS (Distributed Denial of Service/Denial of Service) attacks. (Alliance for Responsible Data Collection)

European Energy Information Sharing and Analysis Centre: EE-ISAC commits operational expertise and intelligence-sharing to bolster cybersecurity coordination for EU energy stakeholders. It offers practical sector insights to support effective resilience efforts.

EE-ISAC stands ready to support the Commission and its stakeholders with operational expertise, intelligence-sharing experience, and practical insights from the energy sector.

German Insurance Association: DORA establishes a high level of cybersecurity in the financial sector, with rapid industry efforts to implement its requirements. It underscores strong regulatory-driven alignment on operational resilience.

The Digital Operational Resilience Act (DORA) ensures a high level of cybersecurity, and the financial sector has made great efforts to implement its requirements in a very short time.

Airbus: Airbus advocates creating public-private partnerships to enable threat intelligence and best-practice sharing, prioritizing support for SMEs. This approach aims to strengthen collective cybersecurity capabilities.

Establish Public-Private Partnerships to facilitate threat intelligence and best :unselected: practice sharing, especially for SMEs.

Alliance for Responsible Data Collection: The Alliance sets standards for responsible public internet data collection that protect domain health, including continuous monitoring and rate limiting to prevent service degradation and DDoS/DoS. It excludes data behind restricted logins to safeguard security.

Data collection under these standards is limited to public internet data.

European Law Institute: The European Law Institute stresses maintaining data security obligations to ensure compliance and resilience. It highlights the importance of clear duties within cybersecurity governance frameworks.

Eurochambres: Eurochambres promotes access to managed cybersecurity services to help businesses strengthen protection and meet compliance demands. This supports broader alignment with resilience and certification objectives.

Dutch Startup Association: The Dutch Startup Association supports EU cybersecurity objectives, encouraging startup engagement and alignment with European resilience goals. It signals commitment to advancing a secure and innovative digital ecosystem.

1.9 Proportionate AI Governance Simplification

Anchor obligations in demonstrable risk and control: focus duties on AI systems and actors with direct, verifiable impacts on safety or fundamental rights, and avoid blanket high-risk labels. Scope by sector and context (e.g., B2B vs B2C), exempt internal/intra-group tooling, and reserve onerous requirements for large-scale societal risk. Tighten role allocation so responsibilities track who can mitigate harm, with clear boundaries for substantial modification and safety-critical components. For foundation models, keep obligations targeted to systemic risk, update thresholds pragmatically, avoid shifting liability to fine-tuners/deployers, and provide practical codes, decision trees, and machine-readable disclosures. Transparency should be proportionate: tiered signals, narrow deepfake duties, machine-readable provenance, and agent self-identification—without exposing IP or causing label fatigue. Streamline compliance by eliminating non-high-risk registration, using standardized templates, modularizing rights impact assessments, limiting routine reporting, and avoiding technically infeasible audits. Operationalize proportionate rules through principles-based law, harmonized standards over common specifications, sector-specific clarifications, and sandboxes that confer presumption of conformity; lightweight licensing can add guardrails. Preserve research and open-source flexibility, keeping non-commercial developers out of scope and shifting accountability to commercial deployers. Maintain robust rights safeguards, clarify biometrics/emotion uses, and separate safety from security to avoid duplicating NIS2/CRA/DORA. Ensure adaptive, capability-based oversight with feasibility derogations and globally consistent updates, align with existing regimes, clarify territorial/IP interfaces, and provide SME-oriented tools and pathways. Strategic simplification (including targeted reforms and pauses) supports competitiveness without diluting protections. Common threads: risk-tiered, context-aware obligations; clarity of roles; interoperability with existing laws; and practical infrastructure (standards, sandboxes, templates) that prevents compliance drift while preserving innovation and rights.

1.9.1 Roles, Definitions and Proportionate Liability

This category emphasizes clear allocation of roles along the AI value chain and proportionate liability. Stakeholders call for unambiguous delineation of responsibilities between providers, deployers, and downstream

actors—particularly in dual-role scenarios—so obligations track actual control and information access. They stress that deployers often rely on upstream compliance and certification, making transparency and accountability from providers essential. Concepts that trigger role shifts and liability—such as substantial modification and change management—need tight, predictable boundaries to avoid uncertainty and duplicated duties. Contributors also seek precise, practical definitions to right-size regulation. They urge refining the AI definition to cover systems with genuine cognitive or autonomous capabilities, excluding basic automation and traditional statistical models; clarifying when an AI model is a product; and resolving ambiguities like "safety component." On liability, they argue for relying on existing horizontal frameworks (e.g., product liability) and avoiding overlapping regimes (including reconsidering a separate AI Liability Directive), ensuring compliant systems are not penalized and that transparency duties remain context-sensitive. The goal is predictable, non-duplicative obligations aligned to risk and actor capability.

> *The roles and responsibilities among providers, deployers, and downstream providers within extensive supply chains require clarification.* (Finnish Food and Drink Industries´ Federation (ETL))
>
> *Refine the definition of AI to ensure the scope only includes systems with actual cognitive or autonomous capabilities, not basic automation or rule-based systems.* (UNIFE)
>
> *Art. 82: Delete Art. 82 on compliant AI systems which present a risk, as compliance with the AI Act should be sufficient for an AI system to be allowed on the market.* (Technology Industries of Finland)
>
> *We take the view that our responsibilities must be met, but we cannot do so without relying upon the compliance and certification of AI upstream providers, over which we have limited control and transparency.* (Infosys Limited)
>
> **FERMA - Federation of European Risk Managers Associations:** Recommends withdrawing the AI Liability Directive to avoid overlapping and conflicting obligations on developers and users, ensuring a proportionate liability framework.
>
> *Consider retracting the Al Liability Directive proposal to eliminate overlapping and potentially conflicting obligations on AI developers and users.*
>
> **SIEMENS AG:** Argues that existing horizontal liability regimes already address AI risks and that new, duplicative digital acts are unnecessary.
>
> *where there is already a (general) act or legislative framework covering the targeted risks, no new digital acts are needed (e.g. Product Liability Act already covers AI liability risks)*
>
> **ZVEI e.V.:** Advocates adapting existing frameworks instead of creating a new AI Liability Directive to keep liability proportionate and clear.
>
> *No need for an AI Liability Directive existing frameworks can be adapted instead of creating new ones.*
>
> **Technology Industries of Finland:** Calls for deleting Article 82 so that compliant AI systems are not subject to additional restrictions beyond AI Act compliance, maintaining proportionate treatment.
>
> *Art. 82: Delete Art. 82 on compliant AI systems which present a risk, as compliance with the AI Act should be sufficient for an AI system to be allowed on the market.*
>
> **Unipol Assicurazioni S.p.A.:** Contends actuarial risk assessment should not be classified as profiling that triggers high-risk obligations, aligning scope with established insurance practices.
>
> *Precisely, actuarial risk assessment should not be classified as "profiling" under Article 6(3) of the AI Act, and therefore should not automatically be subject to high-risk AI system requirements.*
>
> **Eurofinas:** Urges proportionality by excluding long-standing, transparent statistical methods from the AI Act's scope.
>
> *Proportionality in the Al Act, ensuring that long-established and transparent statistical techniques, such as logistic regression and generalised linear models, remain clearly outside its scope.*
>
> **German Insurance Association:** Seeks reaffirmation that traditional statistical models are outside the AI definition and scope, clarifying liability boundaries.

In view of the recent uncertainties expressed by some member state authorities, it is necessary to reaffirm the exclusion of traditional statistical models (such as linear or logistic regression methods) from the AI definition and, therefore, from the scope of the Al Act.

Airbus: Requests clearer definition of safety components to ensure consistent high-risk classification and predictable responsibilities across sectors.

The ambiguous definition of a 'safety component' requires immediate clarification to ensure a consistent and predictable classification of sectoral high-risk AI systems across the Union.

World Federation of Advertisers: Advocates a proportionate and flexible approach to transparency obligations in advertising and marketing.

Advertising and marketing therefore warrant a proportionate and flexible interpretation of the AI Act's transparency rules in this regard.

Bitkom e.V.: Highlights uncertainty over when an AI model qualifies as a product for liability purposes, especially if it is not an AI system.

When is an AI model considered a product, especially if it is not an AI system?

ENGIE: Warns that the framework risks overburdening deployers and should better incentivize providers' compliance through clearer role-based responsibilities.

Concerning the AI Act, while ENGIE values its contribution to the safe deployment of AI, the current framework risks overburdening deployers/users of AI models and systems instead of incentivising providers to ensure compliance.

Leading Baltic tech and other businesses and professional associations listed in the submission: Notes that dual provider/deployer roles create ambiguity and duplication, underscoring the need for clearer role delineation.

Such dual-role situations create ambiguity and potential duplication.

Infosys Limited: Emphasizes reliance on upstream provider compliance and certification, calling for proportionate allocation of responsibilities across the supply chain.

We take the view that our responsibilities must be met, but we cannot do so without relying upon the compliance and certification of AI upstream providers, over which we have limited control and transparency.

Meta Platforms Ireland Limited: Flags unclear rules on modification and change management that affect which party holds compliance responsibilities over time.

Finally, the AIA's provisions on modification and change management are unclear.

Finnish Food and Drink Industries´ Federation (ETL): Calls for clearer allocation of roles and responsibilities among providers, deployers, and downstream actors in complex supply chains.

The roles and responsibilities among providers, deployers, and downstream providers within extensive supply chains require clarification.

Vodafone Group: Reports ambiguity about which party is responsible for specific compliance duties, indicating the need for clearer role definitions.

This can create ambiguity in terms of regulatory compliance responsibilities, as at times it can be unclear which party is responsible for which aspects of compliance.

Entrust SAS: Urges a tightly bounded definition of substantial modification to prevent unintended shifts in liability between providers and deployers.

The concept of substantial modification should be clearly and carefully bounded.

European Advertising Standards Alliance (EASA): Proposes limiting the relevant high-risk classification to law-enforcement bodies to ensure proportionate scope and avoid overreach to self-regulatory organisations.

About Annex III point 8(a): the high-risk Al system defined under this point should only cover law-enforcement bodies, not self-regulatory organisations

UNIFE: Seeks a refined AI definition that covers truly cognitive or autonomous systems, excluding basic automation or rule-based tools to keep obligations proportionate.

Refine the definition of AI to ensure the scope only includes systems with actual cognitive or autonomous capabilities, not basic automation or rule-based systems.

1.9.2 Risk-Tiered Scope and Exemptions

This category advocates proportionate, risk-tiered scoping so that obligations fall primarily on AI systems with clear, direct impacts on safety or fundamental rights, rather than sweeping in heterogeneous tools under blanket rules. Stakeholders call for nuanced classifications that avoid automatic high-risk labeling, with distinctions by sector and context (e.g., B2B vs B2C, public-interest uses vs commercial profiling) and explicit recognition of low-risk domains (such as video games). They urge reclassifying or exempting internal and intra-group systems used solely for business processes, warning that disproportionate frameworks would stifle beneficial innovation and harm SME competitiveness. Implementation proposals emphasize pragmatic thresholds and precise harm focus: assess risk at the appropriate level (prioritizing system-level impact while identifying safety-critical components), refine Annex III to target concrete rights and safety risks (e.g., limit emotion recognition to contexts with discrimination risks), and apply proportionate treatment to specific safeguards-oriented uses (such as biometrics for fraud prevention). Several submissions also recommend reserving the most onerous duties for actors or contexts with large-scale societal risk (e.g., VLOPs or platforms doing large-scale moderation) and focusing obligations on direct, causally linked harms rather than indirect or consequential damages.

Narrow definition of high-risk AI to systems directly impacting safety. (Enel SpA)

The need to change the AI Act by reclassifying certain AI systems from the high-risk category to categories with fewer regulatory requirements, for example systems that are used exclusively in internal business processes. (FiCom ry)

Limit this requirement to Very Large Online Platforms (VLOPs) or platforms that perform large-scale algorithmic moderation in-house. (Bolt)

Amend Annex III of the AI Act to limit high-risk classification of emotion recognition systems to systems that may lead to discrimination or rights infringement (ACEA (European Automobile Manufacturers' Association))

SIEMENS AG: Advocates differentiating obligations by application context, clearly separating B2B from B2C requirements to reflect differing risk profiles.

Overall, make a clear distinction for the requirements of B2B applications versus B2C applications.

Enel SpA: Urges narrowing the high-risk definition to AI systems that directly affect safety, ensuring proportionate scope.

Narrow definition of high-risk AI to systems directly impacting safety.

Dun & Bradstreet: Calls for nuanced, context-sensitive high-risk classification so tools aren't automatically designated high-risk.

It is therefore essential that forthcoming guidance on high-risk classification under the AI Act does not automatically categorise such tools as high-risk without a nuanced assessment of their context and risk profile.

Unipol Assicurazioni S.p.A.: Supports narrowing high-risk classifications and tailoring requirements to ensure proportionality, with alignment to sector realities such as GDPR adaptations.

This includes narrowing the AI Act's high-risk classification and requirements to ensure proportionality and adapting GDPR's provisions to better align with sectoral realities.

Video Games Europe: Argues for proportionate implementation recognizing that video games generally pose low risk.

For the implementation of the Al Act, a proportionate application is needed, taking into account the low risk of video games

Telefonica, S.A.: Urges focusing obligations and liability on direct harms rather than indirect or consequential damages to maintain proportionality.

Indirect or consequential damages, i.e., those that do not result directly from failure or malfunction of a product.

World Federation of Advertisers: Proposes using explicit factors to determine what qualifies as low-risk AI when assessing obligations.

When assessing what qualifies as low risk, consideration should be given to factors such as:

Amazon: Supports practical, proportionate solutions that reduce burdens across company sizes while sustaining EU competitiveness.

Our proposals below focus on practical solutions that would benefit the entire EU digital environment, from large enterprises to SMEs, while ensuring Europe remains competitive in the global digital economy.

German Social Insurance European Representation: Recommends distinguishing public-interest AI in the public sector from commercial profiling to avoid stifling innovation and to calibrate obligations.

In addition, a clear distinction should be made between public-interest AI interventions in the public sector and commercial profiling in order not to hamper innovation.

Bolt: Suggests limiting certain requirements to VLOPs or platforms conducting large-scale in-house algorithmic moderation, reflecting a tiered scope.

Limit this requirement to Very Large Online Platforms (VLOPs) or platforms that perform large-scale algorithmic moderation in-house.

Leading Baltic tech and other businesses and professional associations listed in the submission: Warns the AI Act's scope is overly broad and treats very different risk profiles similarly, urging more differentiated compliance.

The current Al Act casts too wide a net, treating vastly different Al systems - from low- risk productivity tools to critical infrastructure applications - under similar compliance expectations.

Ibec: Endorses a risk-based approach and coherent, timely implementation to right-size obligations.

Ensure: · A risk-based approach; and · Timely and coherent implementation of EU policy objectivesxxvii

Schneider Electric: Advocates assessing risk at the system level rather than solely at component level to achieve proportionate classification and controls.

It is also essential that risks are assessed at system level, and not only at component level.

Meta Platforms Ireland Limited: Cautions that a disproportionate high-risk framework could chill beneficial AI, calling for a more targeted scope.

At the same time, the AIA's disproportionate high-risk framework could further restrict the development and deployment of beneficial AI technologies.

Polish Chamber of Insurance (PIU): Calls for a more proportionate approach by narrowing prohibitions that could unduly affect the insurance sector.

PIU advocates for a more proportionate approach in the AI Act by narrowing the scope of prohibitions, especially in areas that may unduly impact the insurance sector.

Finnish Food and Drink Industries´ Federation (ETL): Seeks clarifications to ensure rules enable European companies to benefit from AI, implying proportionate scope.

The AI Act should be clarified to ensure that European companies can benefit from AI.

Entrust SAS: Urges proportionality and clarity, particularly so biometric systems used for fraud prevention are not overclassified.

Ensuring proportionality and clarity in the Al Act, especially in the treatment of biometric systems used for fraud prevention.

FiCom ry: Proposes reclassifying some AI from high-risk to lower categories, such as systems used solely for internal business processes.

The need to change the AI Act by reclassifying certain AI systems from the high-risk category to categories with fewer regulatory requirements, for example systems that are used exclusively in internal business processes.

Anitec-Assinform: Supports limiting high-risk labeling in ECN infrastructure to components with direct safety functions, avoiding blanket designation.

The AI Act rightly avoids labeling all ECN infrastructure as high-risk, focusing only on components with direct safety functions.

ACEA (European Automobile Manufacturers' Association): Recommends limiting high-risk status for emotion recognition to uses that risk discrimination or rights infringements.

Amend Annex III of the AI Act to limit high-risk classification of emotion recognition systems to systems that may lead to discrimination or rights infringement

UNIFE: Argues the high-risk definition should reflect actual risks to safety and fundamental rights rather than technical complexity or deployment context alone.

In this context, the definition of "high-risk" Al should be refined to reflect the actual risk posed to fundamental rights and safety, rather than relying solely on technical complexity or deployment context.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Suggests exemptions or lighter requirements for intra-group services to avoid unnecessary administrative and financial burdens.

Requiring compliance with the AI Act for intra-group services imposes unnecessary administrative and financial burdens on companies.

1.9.3 Adaptive, Stable and Capability-Based Oversight

This category promotes adaptive, stable, and capability-based oversight that simplifies governance by anchoring requirements in actual risk and outcomes, not rigid technical prescriptions. It emphasizes legal certainty, predictability, and technological neutrality so that Economic Operators, Notified Bodies, and developers can meet obligations efficiently, even as AI capabilities evolve rapidly. The overarching goal is to sustain innovation while maintaining proportionate safeguards and reducing compliance volatility from shifting interpretations. Implementation levers include streamlining or withdrawing overly prescriptive measures (e.g., mandated post-market monitoring plans), introducing derogations where obligations are technically infeasible or counter-productive, and pairing proportionality with a technical feasibility principle. Stakeholders urge a return to the AI Act's original risk-based intent, complemented by objective criteria for emergent capabilities and globally consistent, threshold- or capability-aligned updates. This approach reduces costs, prevents paradoxes that deter safety-enhancing systems, and keeps guardrails agile but stable as AI progresses.

Technology evolves rapidly, while regulation should provide agile but stable, outcome-focused guardrails - not rigid, technical prescriptions. (Meta Platforms Ireland Limited)

The AI legal framework should set requirements that are proportionate to actual (not hypothetical) risks, be flexible enough to remain relevant with rapid technological advancements and allow for streamlined AI adoption. (Digital Poland Association)

As drafted, it creates a paradox that could undermine the very principles of safety and human rights protection that we seek to uphold. (Airbus)

Alternatively, at the very least, a principle of technical feasibility shall be added alongside the principle of proportionality, encompassing a trade-off assessment between the added value of the system and its risks on this post market monitoring requirement. (Airbus)

Technology Industries of Finland: Advocates simplifying and stabilizing oversight by withdrawing new regulatory proposals and removing mandated post-market monitoring plans to allow provider flexibility. Emphasizes proportionate, adaptive monitoring aligned with risk.

Art. 72(3): Delete Art. 72(3) which requires providers to follow a specific post-market monitoring plan, whose framework will be designed by the Commission in an implementing act, giving providers flexibility in developing their own post-market monitoring plan and activities.

Digital Poland Association: Urges proportionate, innovation-friendly AI rules that focus on actual risks and remain flexible amid rapid advances. Calls for streamlined adoption under agile, stable guardrails.

The AI legal framework should set requirements that are proportionate to actual (not hypothetical) risks, be flexible enough to remain relevant with rapid technological advancements and allow for streamlined AI adoption.

Airbus: Calls for derogations when post-market monitoring is technically infeasible and adds a technical feasibility principle to ensure safety-enhancing AI isn't hindered. Seeks adaptive, proportionate oversight aligned with system capabilities and benefits.

Alternatively, at the very least, a principle of technical feasibility shall be added alongside the principle of proportionality, encompassing a trade-off assessment between the added value of the system and its risks on this post market monitoring requirement.

TEAM-NB: Stresses that clear, stable, and predictable rules reduce conformity costs and improve enforcement. Argues that regulatory stability is essential for effective oversight.

Economic Operators and Notified Bodies as independent entities require a clear, stable, and predictable environment to efficiently fulfill the legal requirements set out.

Meta Platforms Ireland Limited: Warns prescriptive ex-ante rules can't keep pace and urges agile, stable, outcome-focused guardrails. Reaffirms risk-based oversight over policing underlying technology.

Technology evolves rapidly, while regulation should provide agile but stable, outcome-focused guardrails - not rigid, technical prescriptions.

Alcon Laboratories Inc: Encourages adaptable regulatory updates so authorities and Notified Bodies keep pace with AI adoption. Calls for flexible frameworks that accommodate rapid capability evolution.

Future regulatory updates should be flexible enough to accommodate the rapid evolution of AI capabilities.

Actuarial Association of Europe: Promotes regulation that respects model autonomy and incorporates adaptive mechanisms for emerging AI. Supports capability-based oversight responsive to evolving system behaviors.

Business & Science Poland: Advocates restoring technological neutrality so oversight focuses on uses and risks rather than specific tech choices. Seeks stable, proportionate rules resilient to change.

European Law Institute: Calls for legal certainty to sustain AI development and deployment. Emphasizes predictable, stable oversight within a proportionate framework.

Federation of the European Sporting Goods Industry (FESI): Supports balanced adjustments to the AI Act that preserve clarity while reducing burdens. Seeks proportionate, stable rules for practical compliance.

U.S. Chamber of Commerce: Recommends globally aligned capability-based oversight rather than blunt compute thresholds. Prioritizes objective assessment of system capabilities for proportionate governance.

TikTok Technology Ltd.: Seeks consistent, predictable regulation that enables responsible AI adoption. Emphasizes stability and clarity to reduce operational uncertainty.

Google: Argues compute thresholds should be updated and raised to reflect real capabilities and risk. Endorses adaptive criteria to avoid overbroad triggers.

CLEPA: Calls for flexible oversight mechanisms that can adapt to diverse industrial AI applications. Favors proportionate controls tailored to capability and context.

European Fund and Asset Management Association (EFAMA): Advocates targeted amendments to enhance proportionality and legal certainty. Supports adaptive, stable oversight that minimizes unnecessary burdens.

Bayer AG: Emphasizes the need for consistent, predictable regulation to support innovation in regulated sectors. Seeks stability and clarity in oversight practices.

Digital Currencies Governance Group (DCGG): Proposes objective criteria to identify emergent AI capabilities for calibrated oversight. Supports capability-based thresholds to keep governance proportionate.

Siemens Healthineers AG: Warns that broad horizontal rules create uncertainty and hinder sector progress. Calls for capability-aware, sector-sensitive oversight to restore stability.

DIGITALEUROPE: Notes case-by-case decisions hamper AI training and predictability. Urges stable, general rules to enable consistent development and compliance.

Wolt: Reports daily operational friction from regulatory ambiguities. Requests clearer, predictable guidance to support adaptive, proportionate oversight.

Mirakl: Seeks clearer interpretations of the AI Act to navigate uncertainty. Emphasizes stable, proportionate rules for effective implementation.

1.9.4 Safety, Security and Fundamental Rights

Stakeholders advocate a proportionate simplification of AI governance that preserves safety and fundamental rights. They caution that streamlining the AI Act must not dilute precision, devolve into tick-box ethics, or lead to rights regression. Priorities include maintaining robust safety standards, conducting fundamental rights impact assessments, broadening bias mitigation and inclusive evaluation across AI systems, prohibiting exploitation of vulnerable users, and providing clarity around permissible uses of biometrics and emotion recognition—all within a rights-preserving, appropriately scoped framework. A central thread is the strict separation of safety and security in risk classification. AI systems used for cybersecurity or operational purposes without a direct safety role should not be labelled high-risk; the notion of safety components should be reserved for systems that directly protect health, physical integrity, critical infrastructure, or property. Mixing safety and security would impose unnecessary burdens—especially in domains like radio equipment—duplicate obligations already covered by NIS2, CRA, and DORA, and can even undermine security (e.g., through inflexible human-oversight mandates). Implementation should pair precise definitions with user-friendly guidance and resources (e.g., via AI-on-Demand) to keep obligations targeted while enabling innovation.

> *The AI Act is complex structurally & linguistically, thus an attempt at simplifying for efficiency/effectiveness is welcome but needs careful implementation strategies so not to lose precision & specificity and cause ambiguity, or less stringent protection of human rights.* (Encode Europe)

It is imperative to avoid the undue classification of AI systems that serve cybersecurity or operational functions, without a direct safety role, as high-risk. (GSMA)

Mixing security and safety in the implementation of the AI Act would result in unnecessary regulatory burdens on the use of AI-cybersecurity solutions in radio equipment (not safety components), potentially discouraging innovation in cybersecurity solutions tailored for telecom networks. (GSMA)

Cybersecurity is already dealt with within a number of pieces of legislation (i.e., NIS2, CRA, DORA etc.). (GSMA)

Encode Europe: Supports simplifying AI governance but insists on careful, precise implementation to avoid ambiguity or weakening protection of fundamental rights; warns against tick-the-box ethics and calls for user-friendly resources.

The AI Act is complex structurally & linguistically, thus an attempt at simplifying for efficiency/effectiveness is welcome but needs careful implementation strategies so not to lose precision & specificity and cause ambiguity, or less stringent protection of human rights.

GSMA: Urges a clear separation of safety and security to keep obligations proportionate and avoid misclassifying AI cybersecurity tools as high-risk, which would stifle innovation and duplicate existing cybersecurity laws.

It is imperative to avoid the undue classification of AI systems that serve cybersecurity or operational functions, without a direct safety role, as high-risk.

Telefonica, S.A.: Argues that cybersecurity-focused AI should not be deemed high-risk for safety unless it directly protects physical integrity, emphasizing a firm distinction between safety and security in the AI Act.

On the other hand, the distinction between safety and security is essential, and AI systems focused on cybersecurity should not be classified as high-risk unless they directly prevent physical harm.

iProov Ltd: Warns that rigid human-oversight mandates can undermine the effectiveness and resilience of security-oriented AI, potentially reducing overall protection.

ENSHPO - The European Network of Safety and Health Professional Organizations: Contends the list of prohibited AI practices lacks safety nuance and may miss context-specific occupational safety realities, calling for more calibrated criteria.

Inter IKEA Group: Seeks clear guidance on when and how emotion-recognition systems are permitted, ensuring safeguards for users' safety and fundamental rights while enabling legitimate uses.

Bocconi University: Advocates for non-regression in fundamental rights protections and robust Fundamental Rights Impact Assessments to ensure simplification does not erode rights guarantees.

Meetic Group, a Match Group Company: Asks regulators to recognize and allow proportionate biometric capabilities within AI tools under safeguards, rather than imposing overly broad restrictions.

Computer & Communications Industry Association (CCIA Europe): Recommends extending bias-mitigation and fairness measures beyond high-risk systems so all AI meaningfully protects fundamental rights.

Hugging Face: Promotes inclusive, transparent evaluation practices and diverse datasets to identify and reduce bias, strengthening fundamental-rights protections.

Euroconsumers: Calls for a clear ban on AI practices that exploit users' vulnerabilities, reinforcing consumer protection and fundamental rights.

BioMed Alliance: Supports simplification only if it preserves high medical safety standards and patient protections, cautioning against any dilution of safeguards.

Cookie Information / Piwik PRO: Urges a proportionate regulatory scope that preserves fundamental rights without imposing unnecessary burdens, aligning obligations to actual risk.

APPLiA (Home Appliance Europe): Proposes separating safety compliance from fundamental-rights requirements to streamline governance while ensuring both dimensions remain properly protected.

1.9.5 Cross-Sector, Cross-Border and IP Alignment

This category advocates proportionate, interoperable AI governance that removes duplication across sectors, clarifies responsibilities, and leverages existing regulatory regimes. Stakeholders call for narrowing broad "high-risk" scopes, focusing compliance where risks materialize, and eliminating overlaps with established horizontal and sectoral rules (e.g., GDPR, DSA/DMA, NIS2, DORA, MDR). They urge EU-level guidance to ensure consistent implementation, clear allocation of duties for upstream models versus downstream deployers (including open-source adaptations), and streamlined pathways under the Digital Omnibus so organizations can integrate AI governance into existing compliance processes without double regulation. Cross-border and IP alignment are central. Contributors seek clear territorial limits for AI Act obligations—especially copyright-related duties—so they do not conflict with international law or create impractical extraterritorial exposure. They ask the EU to define when AI "outputs are used in the EU" and propose practical scoping tools (e.g., terms-of-use restrictions). They also want the interface between training-data transparency and copyright law clarified, with acceptable verification methods that uphold accountability without infringing IP. Beyond the EU, parties encourage interoperable approaches with third countries (e.g., AU initiatives) via co-regulatory alignment and graduated conformity mechanisms that reduce barriers while protecting creators' and users' rights.

Therefore, certain overlaps and conflicts between the AI Regulation and existing legislation (e.g. DSA, DMA, GDPR, NIS2, MDR, etc.) must be eliminated. (WKÖ - Austrian Federal Economic Chamber)

Unclear territoriality of AI Act copyright provisions creates interpretative uncertainty and potential conflicts with international law. (Anitec-Assinform)

This ladder would allow African developers to incrementally meet conformity criteria, reducing barriers to participation in EU digital markets. ()

We would recommend deleting the extraterritoriality provision to avoid regulatory confusion and ensure alignment with established international copyright law principles. (Meta Platforms Ireland Limited)

Unipol Assicurazioni S.p.A.: Proposes narrowing high-risk classifications and aligning GDPR with sector realities to reduce barriers, enabling proportionate, cross-sector AI governance while protecting users.

This includes narrowing the AI Act's high-risk classification and requirements to ensure proportionality and adapting GDPR's provisions to better align with sectoral realities.

Seznam.cz, a.s.: Supports a proportionate easing of AI Act obligations and a balanced approach between content creators and AI developers to sustain innovation across sectors.

Compromises and practical solutions need to be sought that would protect the interests of content creators without overly restricting the development of AI in the EU.

Meta Platforms Ireland Limited: Calls for a system-level focus that leverages existing EU regimes and removes overlapping upstream/downstream rules, with clear territorial scope to avoid cross-border copyright conflicts.

We would recommend deleting the extraterritoriality provision to avoid regulatory confusion and ensure alignment with established international copyright law principles.

Almega: Seeks clarity on how training-data transparency interfaces with copyright, enabling accountability without infringing IP and ensuring consistent cross-sector practice.

The Commission and co-legislators should clarify the interface between the Al Act's transparency requirements for training datasets and EU/national copyright law.

: Advocates interoperable, co-regulatory alignment between African and EU AI frameworks to enable cross-border participation while respecting regional contexts.

Africa's Al strategy should aim for co-regulatory alignment - compatible but not identical to EU Al Act principles, ensuring interoperability while preserving African epistemologies and datasets.

Anitec-Assinform: Urges clarifying that AI Act copyright-related obligations apply only within EU jurisdiction to reduce cross-border legal uncertainty and uphold international law.

We propose clarifying that EU copyright obligations apply only to activities already subject to Union and member state copyright law, not to development processes carried out entirely outside Union jurisdiction.

WKÖ - Austrian Federal Economic Chamber: Calls to narrow risk classifications and eliminate overlaps with existing frameworks (DSA, DMA, GDPR, NIS2, MDR) to deliver proportionate, cross-sector certainty.

Therefore, certain overlaps and conflicts between the AI Regulation and existing legislation (e.g. DSA, DMA, GDPR, NIS2, MDR, etc.) must be eliminated.

European Associations of Co-operative Banks (EACB): Requests clear scope, removal of duplication, and integration with existing financial and risk frameworks so AI rules are proportionate and consistent across the sector and EU.

The AI Act should not impose contradictory or overlapping obligations with existing national and European regulations such as DORA, CCD, MCD, CRR/CRD and the GDPR.

ACEA (European Automobile Manufacturers' Association): Asks for clear guidance on copyright and AI Act compliance, especially when adapting open-source models, to align responsibilities and avoid undue burdens on downstream sectors.

Establish clear guidelines for compliance with copyright obligations and the requirements of the AI Act.

VDMA - Advancing Europe´s machinery industry: Warns that double regulation under the AI Act creates uncertainty and calls for coordinated streamlining across sectors to ensure proportionate compliance.

European Banking Federation: Calls for clarifying and aligning AI Act rules with existing banking and EU frameworks, avoiding duplication and enabling proportionate, cross-sector innovation.

Salesforce, Inc.: Advocates harmonized, interoperable AI rules across jurisdictions to boost innovation while maintaining safeguards.

European Association of Public Banks: Supports using the Digital Omnibus to ensure smooth, consistent AI adoption and legal predictability, reducing overlapping obligations across public banking.

Seznam.cz, a.s.: Urges balanced easing of AI rules and fair alignment with creators' interests so regulation does not unduly restrict development in the EU.

Charter of Trust: Recommends precise AI definitions, sector guidance, and curated categorization lists to support proportionate, cross-sector governance and implementation.

DIGITALEUROPE: Proposes replacing new AI risk assessments with GDPR DPIAs to simplify, align, and avoid duplicative obligations across sectors.

1.9.6 Standards, Sandboxes and Assurance Pathways

This category advances a proportionate governance model that simplifies AI compliance by anchoring rules in clear, principles-based legislation and operationalizing them through guidance, delegated acts, and harmonised technical standards. Stakeholders stress that gaps in standards and codes of practice slow innovation and create uncertainty; they call for rapid, inclusive standardization that can both specify requirements and limit what is deemed high risk when relevant hENs are applied. Several inputs caution against Commission-driven common specifications in favor of industry-led standards, and request sector-specific clarifications (e.g., energy safety components; telecom network management) alongside recognition of effective self-regulatory regimes (e.g., in

advertising) as complementary safeguards. Assurance pathways focus on expanding and resourcing regulatory sandboxes across sectors to provide supervised testing, evidence of compliance, and safe data reuse/bias testing, including for open-source projects. To make sandboxes a credible, scalable route, many recommend conferring a presumption of conformity—or even automatic compliance—upon successful exit, thereby rewarding investment and accelerating conformity assessments. Lightweight licensing-based safeguards are proposed as an additional, flexible mechanism to embed responsible-use constraints without imposing high-risk burdens, collectively delivering predictable, low-friction compliance routes that scale with risk and encourage innovation.

> *Simplification of the EU AI Act can be done (1) by guidelines of the EU Commission, (2) by recommendations and other documents issued by the AI Office, (3) by delegated acts, as foreseen in the AI Act itself, (4) by court interpretations, (5) by adopting quality standards and benchmarks.* ()
>
> *Clarify that AI-based safety components or functionalities are not to be considered high- risk when harmonised standards under relevant Union harmonisation legislation are available and applied, in line with the original intent of Art. 6(1) (b).* (Technology Industries of Finland)
>
> *We therefore recommend amending the current provisions so that a successful exit from the sandbox confers a presumption of conformity on the tested AI system or model.* (European AI Forum)
>
> *Art. 41: Delete Art. 41 on common specifications.* (Technology Industries of Finland)

: Advocates principles-based simplification of the AI Act, relying on guidelines, delegated acts, court interpretations, and adoption of quality standards and benchmarks. Technical details should be specified via secondary legislation and harmonised standards.

> *Simplification of the EU AI Act can be done (1) by guidelines of the EU Commission, (2) by recommendations and other documents issued by the AI Office, (3) by delegated acts, as foreseen in the AI Act itself, (4) by court interpretations, (5) by adopting quality standards and benchmarks.*

SIEMENS AG: Warns that the absence of clear GPAI codes of practice and high-quality harmonised standards creates market barriers and uncertainty in conformity assessment. Calls for simple, consistent standards to enable innovation and collaboration across the AI value chain.

> *Market entrance barriers are likely for high-risk AI if hENs are not available or only in low quality (e.g. high-risk AI might be stopped due to uncertainties in conformity assessment)*

Technology Industries of Finland: Proposes limiting high-risk designations where harmonised standards are available and applied. Urges deletion of Commission-led common specifications in favor of industry-driven standardization.

> *Clarify that AI-based safety components or functionalities are not to be considered high- risk when harmonised standards under relevant Union harmonisation legislation are available and applied, in line with the original intent of Art. 6(1) (b).*

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Calls to expand regulatory and innovation sandboxes, including for data reuse, bias testing, and open-source projects. Seeks a presumption of conformity for AI systems that successfully exit sandboxes to create strong participation incentives.

> *We therefore recommend amending the current provisions so that a successful exit from the sandbox confers a presumption of conformity on the tested AI system or model.*

ENGIE: Requests clear definitions and scope for safety components in the energy sector and practical guidance for classifying complex AI systems as high-risk. This clarity would ensure predictable implementation.

> *As for the identification of high-risk AI systems, clarification on the definition and perimeter of safety components for the energy sector, and on the way companies can classify AI systems as high-risk in complex circumstances outside of the use cases of the Act will be paramount in ensuring certainty in implementation.*

Vodafone Group: Supports a flexible AI Act implemented via practical Commission guidance and use of regulatory sandboxes in strategic sectors. Also seeks certainty that network management AI is not treated as high-risk.

In our view, the Commission could best support the implementation process by issuing guidance on the practical application of the AI Act, and making use of regulatory sandboxes in strategically important sectors.

Anitec-Assinform: Argues that current sandbox recognition is too limited to incentivize participation. Proposes automatic compliance with the AI Act for AI systems that complete a sandbox successfully.

We propose that companies successfully completing sandboxes automatically comply with the AI Act for their tested AI system.

European AI Forum: Recommends that successful sandbox exits confer a presumption of conformity and that sandboxes cover data reuse and bias testing under safeguards. Frames this as both simplification and a clear incentive for startups.

We therefore recommend amending the current provisions so that a successful exit from the sandbox confers a presumption of conformity on the tested AI system or model.

European Advertising Standards Alliance (EASA): Highlights advertising self-regulation as an effective, flexible assurance mechanism that complements regulation. Urges recognition of self-regulatory standards and avoidance of imposing high-risk obligations on these bodies.

Given their proven expertise and recognised independent guidelines, these self- regulatory bodies in the advertising sector are ideally positioned to establish reliable standards and provide societal safeguards.

: Suggests lightweight licensing conditions to embed responsible-use safeguards as a proportionate assurance mechanism. Aligns with RAIL-style licenses and Trustworthy AI guidelines.

Licensing conditions can embed responsible-use rules in a lightweight manner, balancing innovation with accountability.

ENSHPO - The European Network of Safety and Health Professional Organizations: Advocates AI regulatory sandboxes tailored to occupational safety and health, alongside harmonized standards and CAISP, to ensure safe and proportionate oversight. Emphasizes practical, supervised testing environments.

Healthtech Finland: Calls for clearer guidance and standardization pathways for high-risk health AI and medical devices to streamline compliance. Seeks certainty in classification and assessment.

Association of Consumer Credit Information Suppliers: Proposes sequencing high-risk obligations in line with the availability and maturity of harmonised standards. This would ease implementation and reduce undue burdens.

Suomen Yrittäjät - The Federation of Finnish Enterprises: Requests practical guidelines and clarified obligations for SMEs, leveraging standards to simplify compliance. Emphasizes proportionate, usable assurance pathways.

D-Trust: Encourages permitting automation in compliance and permitting processes while regularly reviewing standards. Aims to keep assurance efficient and up to date.

INVERCO: Proposes EU-level accreditation for algorithm auditors to create consistent, reliable assurance pathways. This would harmonize oversight across Member States.

CEN and CENELEC: Supports inclusive, industry-driven European AI standardization as the backbone of proportionate governance and conformity processes. Stresses timely development of harmonised standards.

SAP SE: Cautions against compulsory Commission common specifications and favors harmonised standards and flexible guidance. Seeks to keep assurance pathways innovation-friendly.

Danish Industry: Advocates expanding sandbox exemptions to facilitate experimentation and reduce compliance burdens during development. Aims to accelerate safe innovation.

Zentralverband der deutschen Werbewirtschaft (ZAW): Recommends aligning AI transparency duties with established advertising standards and self-regulatory frameworks. Seeks to avoid misclassifying such systems as high-risk.

Wolt: Argues that current sandboxes are inadequate for realistic AI development contexts. Calls for context-aware, lighter compliance pathways better suited to iterative deployment.

OpenAI: Supports development of AI compliance tools, shared infrastructure, and standards to streamline assurance. Sees tooling as key to proportionate, scalable governance.

The European Crypto Initiative (EUCI): Advocates using cryptographic proofs and verifiable techniques to simplify compliance and evidence obligations. Positions advanced crypto as a scalable assurance pathway.

Adyen: Urges adequately resourced, EU-standard regulatory sandboxes to deliver consistent benefits and accelerate conformity assessments. Emphasizes coordination and capacity.

APPLiA (Home Appliance Europe): Maintains that the absence of harmonised standards should not automatically trigger a high-risk classification and supports self-assessment as a valid compliance route. Seeks proportionate, flexible assurance options.

1.9.7 Streamlined Compliance and Reporting

This category emphasizes making AI governance proportionate by streamlining compliance and reporting obligations so they are clear, non-duplicative, and matched to actual risk. Stakeholders urge slimming down rules and minimizing bureaucracy, particularly where robust sectoral safety regimes already exist, and caution against codes of conduct or ancillary obligations that overshoot the AI Act. The goal is to preserve innovation—especially for SMEs and research—while maintaining safety by focusing on practical, targeted requirements. Concretely, proposals include eliminating registration for systems deemed not high-risk (and scaling back or clarifying registration for others), providing standardized templates to simplify high-risk technical documentation, and modularizing fundamental rights impact assessments to build on existing GDPR DPIAs without duplication. Stakeholders also support clearer scoping of what must be publicly disclosed, pragmatic human oversight expectations, and limiting routine reporting, with documentation shared primarily upon regulator request. Exemptions or lighter-touch treatment are sought for internally developed systems, and for areas already governed by harmonized sectoral legislation. The rationale is that excessive or unclear obligations delay conformity assessments, strain Notified Bodies, burden SMEs, and risk diverting effort into paperwork rather than safety. Some requirements (e.g., exhaustive training data audits or extensive logging retrofits) may be technically impracticable or disproportionately costly, while broad registration could introduce cybersecurity risks. A proportionate, streamlined regime aims to avoid "compliance without safety," ensuring oversight that is feasible, risk-based, and innovation-friendly.

Slim down the Al Act (ZVEI e.V.)

Art. 49(2): Delete Art. 49(2) on registration of AI systems within scope of Annex III but considered not high-risk, as per Article 6(3). (Technology Industries of Finland)

The mandatory registration of all high-risk Al systems (including downgraded ones) imposes a disproportionate administrative burden and creates significant cybersecurity risks without enhancing regulatory oversight. (Airbus)

The training datasets themselves are generally highly heterogeneous, comprising web data, licensed corpora, and synthetic content, which renders comprehensive data auditing technically impracticable at scale. (Meta Platforms Ireland Limited)

SIEMENS AG: Advocates minimizing bureaucratic requirements and avoiding redundant documentation for industrial AI, ensuring innovation without compromising safety.

Additional requirements that are neither appropriate to increase the safety level (additional documentation obligations) or that are not fit for purpose for the industrial domain should be minimized.

ZVEI e.V.: Calls for a simplified, proportionate AI Act with lean, innovation-friendly rules.

Simplify the AI Act and ensure proportional, innovation-friendly rules.

European Alliance for Research Excellence: Warns that detailed training data summaries and intent determinations create heavy compliance burdens, especially for researchers and SMEs, and urges simplification.

a detailed summary of the data used for training GPAI models as part of the AI Act can add a layer of compliance costs for research organisations.

Enel SpA: Welcomes AI Act simplification measures to keep obligations proportionate and practical across sectors.

Enel welcomes the announced simplification measures for the AI Act, as referenced in the consultation.

Technology Industries of Finland: Proposes deleting registration for AI systems deemed not high-risk to avoid unnecessary administrative steps.

Art. 49(2): Delete Art. 49(2) on registration of AI systems within scope of Annex III but considered not high-risk, as per Article 6(3).

Digital Poland Association: Urges that voluntary codes of conduct remain within the Act's scope and not add extra obligations beyond the law.

Existing and future codes of conduct should not impose obligations beyond those provided for in the AI Act.

Volkswagen Group: Requests streamlined documentation for high-risk AI, including standardized templates when no personal data is involved.

Simplification of documentation requirements for high-risk AI systems and provision of templates based on examples as a mandated template if no personal data is involved.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Recommends removing Article 49(2) and related references to avoid registering AI systems that are not ultimately high-risk.

We therefore recommend the removal of Art. 49(2) as well as the phrase "and AI systems that are not considered as high-risk pursuant to Article 6(3) and which are registered in accordance with Article 6(4) and Article 49" in Art. 71(1).

Airbus: Opposes mandatory registration of high-risk and downgraded systems as disproportionate and risky, and seeks exemptions for internal tools from CE marking.

The mandatory registration of all high-risk Al systems (including downgraded ones) imposes a disproportionate administrative burden and creates significant cybersecurity risks without enhancing regulatory oversight.

Bitkom e.V.: Calls for targeted adjustments to reduce implementation hurdles and clarify requirements while preserving risk mitigation and competitiveness.

To support a competitive AI economy in Europe while effectively addressing AI- related risks, targeted adjustments in the AI Act are needed.

ENGIE: Seeks clearer scope and public accessibility rules for the EU database registration of high-risk AI providers.

Clarification regarding the registration process in the EU database affecting providers of high-risk AI systems under Articles 49.1 and 71, including the scope of publicly available (art. 71 par. 4) when it comes to the accessibility of the information registered.

Centre for Democracy and Technology Europe: Argues the AI Act should avoid duplicative risk assessments and focus on limited, context-specific reporting, with most documentation provided on request.

As such, the law is more focused on documentation than reporting, reserving the few concrete reporting obligations for specific types of Al systems presenting high risk - e.g. if deployed by a public authority - or general-purpose Al models with systemic risks.

TEAM-NB: Notes incomplete or complex submissions slow conformity assessments, increasing document management demands and risking market delays.

If this is not the case, we observe economic operators struggling with providing documentation of high-risk AI systems that are complete and fully compliant, which delays the conformity assessment process as incomplete and/or not fully compliant submissions often necessitate additional review cycles, clarifications, and coordination, leading to increased demands on document management and technical expertise within Notified Bodies.

Meta Platforms Ireland Limited: Warns that exhaustive data auditing and logging are impracticable and costly for general-purpose models, leading to burdens that may not improve safety.

These structural flaws culminate in "compliance without safety."

Entrust SAS: Advocates practical human oversight expectations and modular fundamental rights impact assessments that build on existing DPIAs to avoid duplication.

Fundamental rights impact assessments (FRIA) should be modular, building on existing GDPR data protection impact assessments (DPIAs) without duplication.

Anitec-Assinform: Reports rising regulatory complexity and low SME adoption, and urges removal of broad registration obligations that add burden and security risks.

Since most systems will not qualify as high risk in practice, this obligation seems very burdensome and should be removed.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Proposes simplifying rules by shifting industrial AI to sector-specific regimes and addressing regulatory uncertainty as an investment barrier.

The Al Act should be simplified by shifting to sector specific regulation of Industrial Al by excluding Annex I.

American Chamber of Commerce to the EU: Calls to align and clarify AI Act obligations to streamline compliance for businesses.

iProov Ltd: Warns that mandating human-led checks can increase operational costs and compliance burdens.

: Flags duplicative AI Act requirements that could hinder innovation and user access, urging streamlining.

Business & Science Poland: Supports simpler self-assessment for high-risk AI and maintaining provider self-assessment as sufficient where appropriate.

European Law Institute: Suggests deleting redundant provisions to reduce overlap and simplify compliance, including Article 10(5).

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Seeks clarifications to make AI Act compliance more predictable and workable.

Japan Business Council in Europe (JBCE): Urges streamlined documentation and registration processes to reduce unnecessary burdens.

Federation of Austrian Industries: Advocates avoiding duplicative rules and scaling obligations to risk to keep compliance proportionate and business-friendly.

IBM: Calls for removal of disproportionately burdensome obligations to keep compliance practical and innovation-friendly.

IDEMIA: Supports simplifying and clarifying AI Act obligations to ease compliance.

Confederation of Norwegian Enterprise (NHO): Highlights overlapping algorithmic governance obligations and seeks better alignment to avoid duplication.

ITI - Information Technology Industry Council: Recommends aligning fundamental rights impact assessments with DPIAs and pursuing ambitious simplification and streamlined implementation.

ENCIRCLE Research Consortium: Calls for removing registration for AI not considered high-risk to minimize red tape.

Salesforce, Inc.: Advocates limiting retraining obligations to avoid unnecessary compliance and operational burdens.

Sdružení pro internetový rozvoj (SPIR): Proposes removing exposure and accuracy metrics to streamline reporting requirements.

Google: Supports targeted simplifications to obligations and a CAIDA design that prioritizes lean compliance.

CLEPA: Asks for easing dataset constraints to reduce compliance friction while maintaining safety.

Orgalim - Europe's Technology Industries: Requests flexibility in post-market monitoring plans to tailor compliance to context and risk.

Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA): Calls to soften AI literacy obligations to avoid disproportionate burdens on employers and workers.

Dassault Systèmes: Urges simplifying and postponing certain AI Act duties to allow orderly, manageable implementation.

European Savings and Retail Banking Group: Warns against adding extra obligations beyond the Act, advocating proportionate, sector-aware compliance.

Ericsson AB: Suggests deregulatory adjustments and phased timelines to reduce immediate burdens and uncertainty.

Dedalus S.p.A.: Notes that new AI Act obligations add complexity, calling for clearer, lighter compliance paths.

DIGITALEUROPE: Highlights complexity that impedes compliance, calling to abolish AI registration databases and drop the AI Office questionnaire.

Schaeffler AG: Reports significant compliance burdens on EU firms and calls for streamlining to remain competitive.

1.9.8 Proportionate Transparency and Labelling

This category advances a risk-based, proportionate approach to AI transparency and labelling that targets high-risk or potentially misleading outputs while avoiding blanket or tool-specific rules. It supports tiered disclosure (from subtle watermarking to visible labels), practical guidance, and alignment across overlapping legal frameworks to reduce administrative burden and label fatigue without weakening consumer protection. In advertising and other evidently creative contexts, most uses are low risk and should not trigger universal disclosure; deepfake obligations should be narrowly scoped to cases that appreciably resemble identifiable subjects and could deceive, with AI-generated text generally out of scope except when informing the public on matters of public interest (Article 50(4)). To preserve accountability without exposing IP or trade secrets, stakeholders call for machine-readable transparency (model cards, provenance metadata), minimal core obligations (user transparency, human oversight), and AI agent self-identification, while resisting intrusive requirements such as source code access. They warn that over-labelling breeds information overload and the implied truth effect, undermining trust and the purpose of disclosure; flexible, digital information delivery and consistent, risk-weighted labelling keep transparency meaningful where it matters most.

Mandatory labelling should be limited to high-risk or potentially misleading outputs, while obvious or low-impact AI functionalities should remain exempt. (European AI Forum)

Allow for tiered labelling/marking solutions, from subtle digital watermarking to labels, depending on the level of risk and impact. (World Federation of Advertisers)

Additionally, excessive labelling of non-misleading content could inadvertently lead audiences to assume that all unlabelled content is automatically truthful, otherwise known as the "implied truth effect". (European Advertising Standards Alliance (EASA))

Whereas Article 50(4) establishes that Al generated or manipulated text "published with the purpose of informing the public on matters of public interest" shall be disclosed, this does not apply to advertising. (European Advertising Standards Alliance (EASA))

Siinda: Advocates standardized, machine-readable model cards and provenance metadata to enable accountability while protecting IP and security-sensitive details. Emphasizes disclosure formats that avoid exposing sensitive information.

The Omnibus should promote standardised model cards and provenance metadata to support accountability without exposing IP or security-sensitive details.

World Federation of Advertisers: Urges a risk-based, proportionate approach to transparency for AI-generated marketing, avoiding blanket labelling of low-risk creative content. Supports tiered labelling calibrated to risk, context and impact.

We also encourage the Commission to ensure that transparency obligations for AI-generated content are risk-based and proportionate, targeting genuinely high-risk cases without capturing low-risk, creative applications in marketing.

Amazon: Calls for flexible, digital information requirements to prevent consumer overload and streamline AI shopping assistant disclosures. Proposes transparent AI agent self-identification and coordination to reduce regulatory overlap.

Looking ahead, long-term solutions include developing transparent AI agent self-identification mechanisms and creating structured dialogue for monitoring emerging regulatory barriers.

Leading Baltic tech and other businesses and professional associations listed in the submission: Recommends minimal core AI obligations including user transparency, human oversight, and basic safeguards. Seeks simplicity that preserves safety without excessive burdens.

These core obligations could include transparency to users, mechanisms for human oversight and intervention, and basic safeguards to prevent discriminatory or unsafe outcomes.

Finnish Food and Drink Industries´ Federation (ETL): Opposes intrusive access measures by authorities, arguing that transparency should not extend to source code disclosure. Seeks proportionate oversight that safeguards proprietary information.

The provision allowing market surveillance authorities to access the source code of an AI system (Article 74(13)) should be removed.

Union of Entreprenuers and Employers: Warns that broad transparency demands could conflict with trade secrets and IP and expose sensitive data without improving accountability. Calls for proportionate, harmonized disclosure aligned with related legislation.

The Commission should ensure that transparency remains effective but proportionate, and that disclosure practices are aligned across related legislation.

European AI Forum: Requests clarification of Article 4 and a risk-based regime for AI output labelling. Suggests limiting mandatory labels to high-risk or potentially misleading outputs, exempting obvious or low-impact functionality.

Mandatory labelling should be limited to high-risk or potentially misleading outputs, while obvious or low-impact AI functionalities should remain exempt.

European Advertising Standards Alliance (EASA): Advocates a practical transparency framework for AI-assisted advertising that mitigates deception without overlabelling. Warns that indiscriminate disclosures cause label fatigue and undermine consumer awareness.

An indiscriminate, catch-all disclosure requirement for all AI-influenced media content - whether fully generated or merely AI-assisted -would generate labelling fatigue and be no more informative to the average consumer than providing no disclosure at all.

Gen Digital: Supports user-oriented labelling that helps consumers make informed choices about AI content. Emphasizes transparency that is useful without being excessive.

Federation of the European Sporting Goods Industry (FESI): Calls for balancing transparency with protection of intellectual property. Supports proportionate disclosures that inform users while safeguarding competitive assets.

RELX plc: Encourages aligning transparency practices with compliance requirements to ensure clarity and accountability. Seeks coherent, workable disclosure mechanisms across regimes.

Inter IKEA Group: Supports minimal, clear disclosures when users interact with AI, avoiding unnecessary complexity. Favors proportionate transparency tailored to user needs.

DOT Europe: Advocates flexible content labelling approaches instead of rigid, one-size-fits-all rules. Emphasizes calibrating disclosures to risk and context.

Advertising Information Group: Promotes risk-based transparency and cautions against a broad deepfake definition and universal labelling that create fatigue and harm credibility. Urges consistent labelling across workflows while avoiding signals that unintentionally diminish legitimate content.

Google: Recommends simplifying transparency obligations for recommender systems to improve usability and compliance. Supports proportionate disclosures that are understandable to users.

European Fund and Asset Management Association (EFAMA): Asks to limit the scope of AI literacy obligations while ensuring providers clearly mark AI-generated images. Aims for focused, practical transparency that avoids burdening users and firms.

Zentralverband der deutschen Werbewirtschaft (ZAW): Endorses risk-based transparency over universal labelling and seeks clear deepfake rules for advertising. Warns that overlabelling undermines the goals of transparency.

Verband Österreichischer Zeitungen (VÖZ): Opposes excessive AI labelling that could overwhelm audiences. Favors proportionate, context-sensitive disclosure.

AMETIC: Supports transparent AI self-identification and flexible, digital information requirements. Advocates coherence across rules to keep transparency effective and lightweight.

European Society of Radiology: Promotes the use of model cards to provide structured, useful transparency for AI systems. Seeks proportionate, standardized disclosures in healthcare contexts.

VAUNET - German Association of Private Media: Supports proportionate transparency and labelling requirements for media. Emphasizes measures that inform audiences without hindering creative or editorial processes.

1.9.9 SME-Friendly Implementation and Harmonization

This category advocates SME-friendly implementation and harmonization under a proportionate, risk-based AI governance approach. Stakeholders warn that the AI Act's horizontal, overlapping and prescriptive obligations add a disproportionate layer atop sectoral regimes and create legal uncertainty, higher costs and barriers to deployment—felt most acutely by SMEs and startups. Evidence cited includes the Commission's estimate that 5–15% of AI applications may be high-risk, with technical documentation costs of €20,000–€30,000 per downstream high-risk system and additional QMS and conformity-assessment expenses, underscoring the need to calibrate obligations. To simplify and align compliance, the insights call for coherent, harmonized definitions

and a unified framework, complemented by practical, SME-oriented supports: tailored developer guidance, easy-to-use ethical tools and templates, shared best-practice databases, common audit frameworks, approved testing datasets, and reusable compliance components (logging, explainability, oversight). They propose tiered, simplified compliance pathways and detailed roadmaps by risk level, sector and application, proportionate documentation and verification duties, targeted adjustments for small providers, and embedding AI literacy and compliance training without burdensome certifications. Some suggest that using endorsed resources could grant default compliance, aiming to reduce friction while preserving safeguards and EU competitiveness.

> *Compliance obligations, including documentation and verification requirements, should be proportionate and carefully tailored to the capacities of SMEs, so that regulatory safeguards do not inadvertently stifle growth or innovation.* (ACEA (European Automobile Manufacturers' Association))
>
> *In addition, SMEs should receive customized support in the form of simplified compliance pathways depending on the risk classification of their AI applications.* (WKÖ - Austrian Federal Economic Chamber)
>
> *Companies using these endorsed resources should be considered compliant by default.* (2Dyles Services)
>
> *This leads to an unproportional additional layer of AI Act related requirements on top of the existing union harmonization legislation, for instance the Machine Regulation.* (SIEMENS AG)

SIEMENS AG: Critiques the AI Act for layering disproportionate requirements on industrial AI already regulated by sectoral regimes, urging better harmonization and proportionate treatment. Calls to avoid duplicative obligations that hinder SME-friendly implementation.

> *This leads to an unproportional additional layer of AI Act related requirements on top of the existing union harmonization legislation, for instance the Machine Regulation.*

Encode Europe: Advocates practical, SME-focused guidance to implement the AI Act, including tailored developer guidelines and checklists for entrepreneurs. Proposes standardized, easy-to-use ethical tools and shared audit frameworks to simplify adoption.

> *Therefore, we argue for standardized, easy to use/access ethical tools, such as: open-access AI-ethics impact templates, shared databases with best practices & common audit-frameworks within sectors.*

Leading Baltic tech and other businesses and professional associations listed in the submission: Warns that overlapping, prescriptive obligations create legal uncertainty and high costs, especially for SMEs and startups. Calls for simplified, clearer rules to enable European AI deployment.

> *The AI Act currently outlines a complex web of overlapping obligations that are difficult for businesses to interpret and implement, particularly SMEs and startups.*

Union of Entreprenuers and Employers: Highlights that a significant share of applications may be deemed high-risk, with substantial documentation and conformity costs that strain smaller players. Urges proportionate scoping and cost-aware compliance pathways.

> *For such systems, the Commission's estimates put technical documentation costs in the range of €20,000-€30,000 per downstream high-risk system, with additional costs possible where a quality management system (QMS) must be implemented according to the Future Society.*

2Dyles Services: Proposes making compliance accessible via training embedded in AI systems and Commission-provided templates, datasets, and reusable components. Suggests deeming users of endorsed resources compliant by default to ease SME burdens.

> *Companies using these endorsed resources should be considered compliant by default.*

WKÖ - Austrian Federal Economic Chamber: Calls for simplified, customized compliance pathways for SMEs based on risk classification. Recommends a detailed, tiered roadmap tailored to risk level, industry, and application type.

> *In addition, SMEs should receive customized support in the form of simplified compliance pathways depending on the risk classification of their AI applications.*

ACEA (European Automobile Manufacturers' Association): Supports a clear, risk-based framework that preserves safeguards while enabling low-risk innovation. Stresses that documentation and verification duties must be proportionate and tailored to SME capacities.

Compliance obligations, including documentation and verification requirements, should be proportionate and carefully tailored to the capacities of SMEs, so that regulatory safeguards do not inadvertently stifle growth or innovation.

: Urges targeted adjustments to the AI Act that specifically account for the realities of small IT service providers. Emphasizes proportionate implementation to avoid undue burdens.

Finally, targeted adjustments to the Artificial Intelligence Act should especially consider the position of small IT service providers.

Ingka Group IKEA: Promotes AI literacy benchmarks and practical compliance training to support consistent, proportionate implementation. This can particularly help SMEs operationalize requirements without excessive overhead.

MVFP Medienverband der freien Presse e.V.: Advocates simplifying rules to build a coherent, predictable AI framework. Harmonization would reduce fragmentation and ease compliance for smaller actors.

Eurochambres: Calls for a unified, risk-based compliance approach that is workable for SMEs across the EU. Harmonized requirements would streamline implementation and lower costs.

Cigref: Seeks clear, harmonized AI definitions to ensure consistent application and reduce uncertainty. Greater clarity supports proportionate, SME-friendly compliance.

European Entrepreneurs CEA-PME: Opposes gold-plating and additional national burdens that would disadvantage SMEs. Favors proportionate, harmonized implementation to maintain a level playing field.

Eurosmart: Encourages simplifying and harmonizing AI Act obligations with existing sectoral frameworks. This alignment would facilitate implementation and reduce compliance complexity for SMEs.

Middle Tech Europe: Supports simplification and alignment of AI rules to enable practical adoption by mid-sized and smaller tech firms. Urges coherence across jurisdictions to avoid fragmentation.

Wolt: Advocates proportionate implementation and coherent obligations under the AI Act. Simplification would prevent unnecessary burdens and enable SMEs to comply effectively.

European Society of Radiology: Recommends embedding AI literacy without imposing certification mandates. This lowers compliance barriers, especially for smaller providers, while promoting responsible use.

1.9.10 Foundation Models and GPAI Simplification

Across industry and civil society, stakeholders call for simplifying and making obligations for general-purpose AI (GPAI)/foundation models proportionate, practical, and clearly aligned with the AI Act. They seek a user-oriented Code of Practice with authoritative guidance (e.g., decision trees/obligation matrices), standardised machine-readable disclosures, portable low-impact determinations, and avoidance of overreach or gold-plating that shifts responsibilities from model providers to finetuners and deployers. Fine-tuning or narrowing a model's functions should not trigger the full GPAI regime unless it demonstrably creates a GPAI with systemic risk, and routine patches or bug fixes that do not change purpose or materially alter risk should not be treated as substantial modifications; self-use and minor adaptations should face minimal documentation. Stakeholders urge revising or raising thresholds (including systemic risk and compute/FLOPs) to reflect current frontier models, prevent capture of smaller entrants, and keep criteria risk-based and updatable. Obligations for GPAI should remain targeted—systemic-risk duties for model providers without automatic high-risk classification for downstream integrators unless independent high-risk criteria are met. They highlight rushed, overreaching Code of Practice drafts, the infeasibility and cost of end-to-end traceability across interconnected components, and the

rapid obsolescence of compute-based classification. Overall, proportionate simplification should mitigate liability asymmetries, protect platform adoption, and sustain innovation while ensuring trust and safety.

> *Make the GPAI Code of Practice user-oriented, providing clear, practical implementation guidance.* (ZVEI e.V.)
>
> *The GPAI Code of Practice needs to become more user oriented by revising the thresholds for systemic risk and avoid an inappropriate shifting of responsibili- ties from model providers to finetuners and users of these models.* (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)
>
> *Attempts to regulate specific technical parameters - such as using floating point operations ("FLOPs") to classify Al models - may be rendered obsolete almost as soon as they are conceived in a nascent technology environment.* (Meta Platforms Ireland Limited)
>
> *In other words, downstream providers integrating a GPAI model with systemic risk - leading to a general-purpose Al system - will not be required to run a separate risk assessment unless the integrated product itself meets the criteria for high-risk AI systems under the Act.* (Centre for Democracy and Technology Europe)

SIEMENS AG: Siemens urges simplification and clear guidance for obligations triggered by fine-tuning GPAI models to reduce legal uncertainty. It also criticizes GPAI Codes of Practice as overreaching and rushed, undermining usability.

Further simplification (with clear implementing guidelines) of the AIA in relation to obligations following fine-tuning of GPAI models is required to avoid legal uncertainty.

ZVEI e.V.: Calls to make the GPAI Code of Practice user-oriented with clear, practical implementation guidance to support proportionate compliance.

Make the GPAI Code of Practice user-oriented, providing clear, practical implementation guidance.

Volkswagen Group: Advocates revising systemic-risk thresholds and avoiding inappropriate shifts of responsibility from model providers to finetuners and users. Requests clear conditions under which finetuned models are exempt from certain requirements.

The GPAI Code of Practice needs to become more user oriented by revising the thresholds for systemic risk and avoid an inappropriate shifting of responsibilities from model providers to finetuners and users of these models.

Centre for Democracy and Technology Europe: Clarifies that GPAI providers face risk assessment duties only when models pose systemic risk, and that obligations should be targeted accordingly. Notes that integrating a systemic-risk GPAI model does not automatically make downstream systems high-risk absent other factors.

However, GPAI model providers have a specific obligation to assess and mitigate risks where their model is deemed under the Act to pose a systemic risk, namely risks having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain.

European Tech Alliance: Urges updating FLOP-based thresholds for GPAI and systemic-risk classification, warning current levels are outdated and may capture smaller European models.

For instance, the FLOP thresholds for the classification of GPAI models and GPAI models with systemic are already outdated in light of technological and market evolution and could risk capture smaller emerging European models.

Ibec: Seeks a proportionate, AI Act-aligned implementation of the GPAI Code of Practice that supports broad adoption. Warns the Code should not create supply-chain uncertainty or function as de facto legislation.

Ensure implementation of the GP-AI Code of Practice is proportionate, aligns with the Al Act scope and requirements and supports wide adoption across the EU's digital economy.

Meta Platforms Ireland Limited: Argues the AIA's GPAIM regime is complex, outdated, and misaligned with risk, threatening innovation and investment. Criticizes compute-based thresholds and infeasible traceability, urging substantial rollback or removal.

The EU AIA's late-stage addition of complex rules for General Purpose Al Models ("GPAIM") threatens to deter investment, slow Al adoption, and undermine Europe's technological leadership.

Panasonic Europe B.V.: Requests clarity that non-material patches and stability fixes are not substantial modifications and calls for standardized, machine-readable GPAI disclosures and authoritative guidance tools. Aims to prevent regulatory spillover and streamline compliance.

Standardise machinereadable GPAI disclosures, provide a portable LowImpact Determination route, publish authoritative decision trees/obligation matrices, and issue joint AI Office/EDPB guidance to prevent GDPR spillover to nonpersonal partitions.

FiCom ry: Supports balanced GPAI guidelines that foster trust and innovation while simplifying documentation and definitions. Calls targeted improvements on model modifications, compute thresholds, GPAI status for modified models, and proportional documentation for fine-tuning.

To ensure these guidelines are practical, fair, and truly support Al uptake in the EU, targeted improvements are needed, focusing on the regulation of model modifications, the approach to compute thresholds, the definition of GPAI status particularly for modified models, and the proportionality of documentation for fine-tuning.

Anitec-Assinform: Advocates raising GPAI systemic-risk thresholds to reflect current frontier model capabilities and maintain proportionality.

Raise GPAI systemic risk thresholds to reflect current frontier models

UNIFE: Asks that fine-tuning or narrowing a GPAI model not trigger full GPAI obligations unless the result demonstrably becomes a systemic-risk GPAI model. Applies both to fine-tuned model providers and deploying AI system providers.

It should be clarified that narrowing or targeting the functions of an existing GPAI model, regardless of whether systemic risks are present in the original model, must not trigger the full set of obligations applicable to GPAI models, unless the fine-tuning demonstrably results in the development of a general-purpose AI model with systemic risk as defined in Article 52(1).

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Calls for user-oriented GPAI rules with revised systemic-risk thresholds and clear exemptions for finetuned models. Opposes shifting responsibilities from model providers to finetuners and users.

The GPAI Code of Practice needs to become more user oriented by revising the thresholds for systemic risk and avoid an inappropriate shifting of responsibili- ties from model providers to finetuners and users of these models.

Business & Science Poland: Urges proportionate obligations for fine-tuning and model modifications to avoid unnecessary burdens on innovators.

Digital Business Ireland: Warns against overreach and gold-plating in the GPAI Code of Practice, advocating alignment with the AI Act and minimization of undue burdens.

Intesa Sanpaolo: Seeks mitigation of liability asymmetries for GPAI deployers to ensure fair, proportionate responsibility across the value chain.

ITI - Information Technology Industry Council: Recommends simplifying GPAI rules and right-sizing thresholds to maintain practicality and support innovation across the ecosystem.

AI Standards Lab: Proposes exempting self-use GPAI deployments from extensive documentation to streamline internal adoption without compromising safety.

Independent Retail Europe: Supports triggering GPAI obligations only when substantial changes are made, avoiding unnecessary compliance for minor adjustments.

Orgalim - Europe's Technology Industries: Calls to limit integrator liability for GPAI and clarify that obligations attach at the model level when placed on the market. Seeks proportionate accountability across the supply chain.

Insurance Europe: Cautions against treating GPAI integration as a blanket exclusion from high-risk classifications, ensuring risk-based oversight remains intact.

Dassault Systèmes: Requests clearer delineation of GPAI scope and treatment of specialized models to ensure proportionate, appropriate obligations.

Danish Industry: Calls for clear, practical guidance on downstream obligations when integrating GPAI models to prevent undue burden shifting.

DIGITALEUROPE: Seeks clarity on who qualifies as a GPAI provider and on deployer thresholds, warning excessive paperwork could deter platform adoption. Advocates proportionate, streamlined documentation and reporting.

Mistral AI: Supports targeted refinements to the AI Act and careful limits on systemic-risk triggers to avoid over-regulating frontier models while maintaining safety.

1.9.11 Open-Source and Research Flexibility

This category advocates proportionate AI governance that preserves open-source and research flexibility. Stakeholders ask to clarify and broaden the AI Act's Article 2(6) research exemption so that AI developed and used solely for scientific research and development—including private, industrial, pre-commercial, and lifecycle R&D—remains out of scope until commercial deployment. They call for alignment with existing notions of "scientific research purposes" in the GDPR and EHDS, and for clear exclusion of AI used for R&D of commercial products from the Act's obligations to remove legal uncertainty. On open-source, contributors urge a precise legal definition of OSS and explicit exceptions to avoid capturing non-commercial developers and research organisations as "providers." They propose clarifying that publishing code or models under an open licence is not "placing on the market," carving out non-commercial open-source development, and shifting compliance and liability obligations to commercial deployers. Complementary measures include lighter requirements for open-weight models, innovation sandboxes that include open-source projects, audited open AI solutions, and open-source compliance toolkits—together providing legal certainty, lowering entry costs, and supporting innovation while keeping accountability where risks materialise. Finally, they caution that overlapping regimes (AI Act, GDPR, ePrivacy) and broad provider definitions risk chilling early-stage open innovation; clear guidance and consistent interpretation are needed to ensure proportionate, innovation-friendly compliance.

Exempt non-commercial open-source development. (European AI Forum)

Broaden the research exemption. (European AI Forum)

This will provide private stakeholders with the opportunity to use Open-Source AI for commercial purposes without fulfilling these requirements, thus lower operational costs and incentivising innovation while maintaining regulatory standards. (ACEA (European Automobile Manufacturers' Association))

Limit the responsibility of non-commercial developers for downstream uses of open models; compliance duties should rest with commercial deployers. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

Technology Industries of Finland: Advocates excluding AI used for R&D of commercial products from the AI Act's scope and calls for a clear legal definition and exceptions for open-source software to ensure predictability.

Art. 2(6): Clarify that AI used for R&D of commercial products is out of scope.

EFPIA: Calls to clarify and broaden the AI Act's research exemption to reduce legal uncertainty, aligning the definition of scientific research with GDPR and EHDS and covering the medicine lifecycle.

Due to lack of definition of S&R, we suggest alignment with the wording in GDPR (recital 159) and EHDS (recital 61): "The notion of scientific research purposes should be interpreted in a broad

manner, including technological development and demonstration, fundamental research, applied research and privately funded research."

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Warns that broad provider definitions could burden open-source and research actors, urging exemptions for non-commercial OSS, clarity that open releases are not 'placing on the market,' and liability safeguards focusing on deployers.

Clarify that releasing Al models or code under an open licence does not constitute "placing on the market" and is therefore outside the Al Act's provider obligations.

Siinda: Proposes open-source compliance toolkits (logging, testing, bias assessment, DPIA templates) to lower entry costs and support proportionate compliance.

Provide open-source toolkits for logging, model-testing, bias assessment, and DPIA templates to lower entry costs.

National Land Survey of Finland: Urges making audited, open AI solutions available to drive widespread, consistent adoption and productivity gains across the public sector.

Audited, open AI solutions should be made available.

Anitec-Assinform: Seeks to ensure the research exemption covers private-sector R&D and all pre-market phases of commercial products to protect innovation.

We propose clarifying that "scientific research and development" includes all R&D phases for any product, including commercial ones, as long as they're not yet on the market.

European AI Forum: Advocates deregulatory adjustments: exempt non-commercial OSS, broaden research carve-outs until commercial deployment, add liability safeguards, and include OSS in sandboxes to reduce uncertainty and spur innovation.

All academic, pre-commercial and collaborative Al experimentation should remain outside the Al Act's scope until systems are deployed commercially.

ACEA (European Automobile Manufacturers' Association): Calls to exempt open-source AI from full provider/deployer requirements and to distinguish OSS from proprietary models to avoid disproportionate burdens and foster competitiveness.

Open-source AI should be exempt from the full provider-deployer requirements to encourage innovation and maintain competitiveness.

American Chamber of Commerce to the EU: Supports expanding the AI R&D exemption to protect research activities and reduce compliance friction in early-stage innovation.

Ministry of Industry and Trade of the Czech Republic - this entry represents the official position of the Czech Republic for the section "Targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules: Backs targeted exemptions for open-source AI with appropriate limits to maintain proportionality and legal certainty.

Orgalim - Europe's Technology Industries: Recommends excluding R&D AI systems from the AI Act's scope to safeguard innovation and research freedom.

Prosus Group: Requests clearer rules for open-source AI to avoid overburdening non-commercial developers while enabling innovation and responsible use.

Hugging Face: Argues for lighter, proportionate requirements for open-weight/open-source models, with compliance duties concentrated on commercial deployers.

Zentralverband Deutsches Baugewerbe: Seeks legal certainty for open-source AI through clear, proportionate obligations, especially to support SMEs' adoption.

DIGITALEUROPE: Urges broadening and clarifying research exemptions to reduce legal uncertainty and safeguard scientific freedom.

Enedis: Requests clarity on when R&D AI falls in or out of scope so experimentation can proceed without undue obligations.

The European Network of Expertise on Omics: Asks to clarify AI Act application to research to avoid hindering scientific progress in omics and data-driven discovery.

1.9.12 Miscellaneous

This category captures calls to make EU AI governance proportionate and simpler to avoid regulatory drag on innovation and competitiveness. Stakeholders recommend pausing enforcement of the EU AI Act's high-risk provisions to enable targeted reforms, radically simplifying adjacent regimes like GDPR, and using the Digital Simplification Package to correct past missteps. Across industry and professional bodies, there is support for clarity, alignment, and practical guidance that reduce compliance burdens while maintaining ethical safeguards. The insights converge on a risk-based, proportionate approach that balances innovation with ethics. Governments and major firms urge streamlining the AI regulatory regime—citing business risk disclosures and global competition pressures—while sector associations back targeted amendments and clearer frameworks so AI adoption can advance responsibly and sustainably.

But in order to unleash the potential of AI EU must ensure clear and proportionate digital regulation that fosters innovation and growth. (Almega)

Governments from Germany, Sweden, Denmark, Poland and Czechia have raised the need to simplify the AI regulatory regime to restore European competitiveness. (Meta Platforms Ireland Limited)

In a speech on the one-year anniversary of his landmark report on European competitiveness, delivered on September 16, at a conference hosted by Commission President Ursula von der Leyen, Draghi called not only for a pause on the "high risk" section of the AIA, but also for "radical simplification" of the GDPR. (Meta Platforms Ireland Limited)

Major European companies have urged Brussels to simplify digital regulation, including the AIA, and over 70 publicly traded firms now cite the AIA as a business risk in filings to the US Securities and Exchange Commission ("the SEC"). (Meta Platforms Ireland Limited)

Meta Platforms Ireland Limited: Urges pausing the EU AI Act and radically simplifying GDPR and digital rules to prevent competitiveness losses and enable proportionate governance. Notes broad support from governments and major companies for moratorium and simplification to restore European competitiveness.

In a speech on the one-year anniversary of his landmark report on European competitiveness, delivered on September 16, at a conference hosted by Commission President Ursula von der Leyen, Draghi called not only for a pause on the "high risk" section of the AIA, but also for "radical simplification" of the GDPR.

Almega: Calls for clear, proportionate EU digital regulation that fosters AI-driven innovation and growth while maintaining common ethical frameworks. Warns that stricter EU ethics requirements risk undermining competitiveness without proportionality.

But in order to unleash the potential of AI EU must ensure clear and proportionate digital regulation that fosters innovation and growth.

EFCA - European Federation of Engineering Consultancy Associations: Advocates clearer, better-aligned, and supportive AI rules to enable proportionate governance for engineering consultancies. Stresses practical guidance and harmonization to ease compliance and support innovation.

European Federation for Market Research Organisation (EFAMRO): Promotes a proportionate AI governance approach that balances innovation with ethical safeguards in market research. Seeks effective, non-overburdensome rules that maintain trust while enabling progress.

DECATHLON SE: Supports targeted amendments to the AI Act to simplify and streamline obligations while preserving necessary protections. Aims for proportionate, workable compliance for retailers and product developers.

1.10 Sector-Specific Alignment & Legacy Exemptions

The single most compelling insight is adopting clear lex specialis primacy so sector laws prevail where they already manage the risk, embedding horizontal AI, cybersecurity, and data obligations into existing NLF regimes with aligned terminology, binding guidance, and established assessment routes to cut duplication and conflict. Practically, exclude already regulated products and uses from new scopes; integrate AI Act duties into machinery, radio, medical, transport, and energy frameworks; ensure scope clarity to avoid misclassification; and rely on mature baselines like GDPR and product safety law. Health stakeholders place MDR/IVDR at the center of medical AI, while finance seeks DORA-centred cybersecurity, calibrated AI risk, and streamlined, centralised reporting. Industrial, energy, and transport communities anchor compliance in UNECE, maritime, and rail rules, limit CRA overlaps, align new data and battery reporting to rollout realities, and streamline ex ante authorisations. Telecom operators urge retiring legacy asymmetries from ePrivacy and the USO. Cyber and critical-infrastructure actors want coherent NIS2, CER, CSA, CRA, and DORA application, targeted carve-outs, protected sensitive data, and a principle of sufficiency. Product-specific proportionality supports exemptions for wearables batteries and automotive AI under UNECE, plus focused Battery Passports. Intra-group activities should not be treated as third-party exposure, and outsourcing definitions should stay narrow. Media, education, and research seek editorial safeguards, proportionate nonprofit/EdTech treatment, and rationalised sector levies. Legacy safeguards—prospective application, clear substantial modification, and spare-part exemptions—are essential. Cross-cutting enablers include co-developed sector guidance, transparent non-discretionary carve-outs, EU-level EPR, digital judicial systems, and targeted procurement streamlining. Common threads are proportionality, reuse of established sector controls, and lifecycle-aware transitions. The overall trend favours coherence and Single Market harmonisation over duplicative, one-size-fits-all mandates.

1.10.1 Lex Specialis & Cross-Regulatory Harmonization

This category captures the lex specialis approach to cross-regulatory harmonization: sector-specific regimes (e.g., MDR for medical devices, eIDAS for trust services, Machinery Regulation, telecom/RED, energy cybersecurity) should prevail over horizontal digital laws (AI Act, CRA, Data Act, etc.) where they address the same risks. Stakeholders call for explicit primacy rules and binding guidance to resolve norm conflicts, reduce duplicative obligations, and keep conformity assessment and enforcement within established sectoral channels. Operationally, the insights advocate: excluding already regulated products/AI uses from new horizontal scopes; integrating AI Act obligations into existing sectoral management systems and conformity pathways; aligning assessments across instruments (e.g., CRA–AI Act) and clarifying overlaps (e.g., AI–RED). They urge recognizing eIDAS as the stricter framework for QTSP/PKI, ensuring MDR/EHDS precedence in health, and leveraging AI Act provisions that permit integration via Annex I regimes. To protect innovation and the Single Market, several propose delaying or repealing overlapping or premature rules (e.g., parts of ePrivacy, RED III duplication), and relying on mature horizontal baselines (e.g., GDPR or Product Liability) where appropriate.

> *Apply the lex specialis principle to ensure sector-specific rules take precedence by (1) establishing the EHDS as the primary framework for health-data sharing and interoperability, and (2) issuing binding guidance confirming that, in case of conflict, sectoral frameworks prevail; specifically, the MDR over the AI Act and the EHDS over the Data Act.* (Zimmer Biomet)
>
> *Alignment between horizontal digital legislation and sectoral cybersecurity rules is essential to avoid conflicts, reduce administrative burden, and ensure consistent expectations for operators of essential services.* (European Energy Information Sharing and Analysis Centre)
>
> *Connect Europe and the GSMA reiterate our call for the repeal of the ePrivacy Directive entirely, and the incorporation of the principle of the confidentiality of communications into existing and/or future horizontal EU law.* (GSMA)
>
> *o where there is already a (general) act or legislative framework covering the targeted risks, no new digital acts are needed (e.g. Product Liability Act already covers AI liability risks)* (SIEMENS AG)
>
> **SIEMENS AG:** Argues the AI Act duplicates existing machinery safety rules and calls for excluding industrial AI covered by sectoral frameworks. It further asserts no new horizontal acts are needed where existing regimes address the same risks.
>
> *AI systems that already have safety & security rules in sectorial legislative frameworksshould be excluded from the scope of the AI Act (i.e. exclude Annex I).*
>
> **Zimmer Biomet:** Calls for an explicit lex specialis hierarchy to resolve conflicts between horizontal and health-sector rules. Proposes EHDS and MDR should prevail over Data Act and AI Act where overlaps arise.

Apply the lex specialis principle to ensure sector-specific rules take precedence by (1) establishing the EHDS as the primary framework for health-data sharing and interoperability, and (2) issuing binding guidance confirming that, in case of conflict, sectoral frameworks prevail; specifically, the MDR over the AI Act and the EHDS over the Data Act.

European Energy Information Sharing and Analysis Centre: Urges alignment of horizontal digital laws with sectoral cybersecurity frameworks for essential service operators. Emphasizes preventing overlap and reducing administrative burdens.

Alignment between horizontal digital legislation and sectoral cybersecurity rules is essential to avoid conflicts, reduce administrative burden, and ensure consistent expectations for operators of essential services.

Intesi Group: Warns that CRA imposes overlapping duties on QTSPs already strictly regulated by eIDAS. Advocates recognizing eIDAS as the governing lex specialis for PKI and digital certificate software.

Public key infrastructure and digital certificate software are already regulated under the stricter, sector-specific eIDAS regime.

GSMA: Recommends repealing the ePrivacy Directive and embedding confidentiality of communications into horizontal law. Seeks to eliminate sector-specific burdens that exceed GDPR obligations.

Connect Europe and the GSMA reiterate our call for the repeal of the ePrivacy Directive entirely, and the incorporation of the principle of the confidentiality of communications into existing and/or future horizontal EU law.

Telefonica, S.A.: Requests clear scoping between the AI Act and the Radio Equipment Directive to avoid double regulation of radio equipment. Calls for consistent implementation across regimes.

With regards its interaction with the Radio Equipment Directive (RED), a clarification of the scope of AI obligations in radio equipment is needed, to avoid regulatory overlap and support innovation in secure telecom networks.

Bitkom e.V.: Proposes integrating AI high-risk requirements into sectoral legislation and aligning conformity assessments with the CRA. Aims to reduce complexity and duplication.

Furthermore, all high-risk requirements listed in Annex I A should be integrated into relevant sectoral legislation (following the existing logic of Annex I B).

Centre for Democracy and Technology Europe: Notes the AI Act already allows integrating new duties into existing sectoral risk management and conformity processes. Highlights provisions enabling use of sector-specific assessments for compliance.

Article 9 (10) of the AI Act allows providers to integrate risk management obligations within their existing management procedures; Article 8 (2) gives providers a high degree of flexibility to integrate the new obligations into their existing compliance procedures and mechanisms; and Article 43 (3) allows for providers of high risk AI systems that fall within the scope of EU legislation listed in Section A of Annex I to follow the conformity assessments procedures set out in those legal instruments and be considered to be compliant with the AI Act.

Adigital (Asociación Española de la Economía Digital): Argues sector-specific ePrivacy rules hinder telecom innovation and anti-fraud compared to GDPR's horizontal approach. Supports relying on GDPR to protect privacy uniformly across actors.

In contrast, the GDPR, as a horizontal framework applied consistently across actors, would allow such practices while still protecting consumer privacy effectively.

Alcon Laboratories Inc: Requests clarity on how AI or digital requirements align with other EU product and chemical rules like REACH and Battery regulations. Seeks coherent cross-regulatory expectations for manufacturers.

Clarify expectation for other EU legislation REACH, Battery regulations,

ACEA (European Automobile Manufacturers' Association): Cautions against premature sector-specific AI rules before the horizontal framework is implemented to avoid fragmentation. Also urges repealing duplicative energy data provisions to streamline obligations.

More generally, we also caution against premature sector-specific AI rules before the Act's horizontal framework has been tested, as this could fragment the Single Market.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Advocates streamlining Annex I to progressively incorporate AI requirements into sectoral regimes and exclude already regulated products. Emphasizes sector-specific adaptations without disrupting existing governance.

1 This approach is better aligned with Recital 49 AI Act, which calls for sector-specific adaptations 'without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established' under EU product legislation.

Fédération des Industries Ferroviaires: Calls for excluding certain rail-sector data from the Data Act and deferring application to avoid conflicts with existing railway frameworks. Seeks legal certainty through targeted exemptions.

Bayerische Motoren Werke Aktiengesellschaft: Seeks clear CRA exemptions and alignment with RED to prevent double regulation across automotive and telecom equipment. Urges limiting horizontal overreach that burdens sector-specific compliance.

Japan Business Council in Europe (JBCE): Calls to align CRA requirements with telecom rules and repeal overlapping RED provisions. Aims to eliminate duplicative obligations across horizontal and sectoral regimes.

European Signature Dialog: Urges streamlining compliance for QTSPs and narrowing CRA scope given eIDAS oversight. Seeks to prevent overlapping requirements for trust services.

Federation of Austrian Industries: Requests alignment between AI rules and platform work legislation to avoid conflicting requirements. Advocates coherent cross-regulatory implementation for employers and platforms.

U.S. Chamber of Commerce: Prefers sectoral regulation over broad horizontal digital mandates to reduce conflict and complexity. Supports lex specialis approaches where industries already have robust rules.

ITI - Information Technology Industry Council: Supports aligning AI Act Annex I with sectoral legislation to ensure coherent requirements. Encourages harmonized implementation over parallel obligations.

Federation of European Securities Exchanges: Asks for CRA exemptions for products or services covered by DORA to avoid duplicate cybersecurity oversight in financial services. Recognizes DORA as the sectoral lex specialis for digital resilience.

Association des Constructeurs Européens de Motocycles: Requests excluding type-approved vehicles and components from the AI Act to avoid overlap with automotive type-approval regimes. Emphasizes reliance on existing sectoral safety systems.

kaiko.ai: Calls for reducing overlap between horizontal AI rules and sector-specific regulations. Seeks clear guidance to prevent duplicative compliance for AI providers.

CLEPA: Warns against AI Act obligations overlapping with automotive type-approval frameworks. Advocates respecting existing sectoral conformity processes.

European Association of Public Banks: Urges harmonisation that respects banking-sector rules and alignment of the CRA with DORA. Calls for recognising DORA as lex specialis and limiting CRA scope accordingly.

SGI Europe: Seeks clarity on the interface between the AI Act and existing product safety legislation. Aims to avoid double regulation and ensure consistent enforcement.

PPC: Argues sectoral rules should take precedence over horizontal frameworks in utilities. Supports lex specialis to minimize burdens and conflicts.

ESYS Foundation: Recommends avoiding regulatory overlap with sector-specific regimes when applying horizontal digital laws. Emphasizes coherence and proportionality.

BVMed - Bundesverband Medizintechnologie e.V.: Advocates anchoring the Medical Devices Regulation as lex specialis over the AI Act for medical technologies. Seeks reaffirmation to prevent duplicative processes.

Computer & Communications Industry Association (CCIA Europe): Warns proposed customs reforms risk contradicting the DSA's horizontal principles. Calls for cross-regulatory consistency to avoid conflicting obligations for intermediaries.

Dedalus S.p.A.: Supports integrating AI Act requirements into medical device standards to leverage existing conformity systems. Aims to reduce duplication in health IT compliance.

DIGITALEUROPE: Calls to avoid interfering with established sectoral governance and enforcement when implementing horizontal AI rules. Endorses lex specialis alignment to streamline compliance.

ECIS, European Committee for Interoperable Systems: Urges repeal of inconsistent applications of the Radio Equipment Directive that conflict with other digital rules. Seeks coherent scoping across regimes.

APPLiA (Home Appliance Europe): Highlights New Legislative Framework safeguards to avoid double regulation of products. Advocates using existing mechanisms rather than layering new overlapping rules.

Logitech: Calls for alignment between the Radio Equipment Directive and the AI Act to prevent duplicative requirements for connected devices. Seeks clear, coherent scoping.

1.10.2 Sector Law Integration & Streamlining

Stakeholders call for integrating and streamlining sector laws by embedding horizontal AI requirements into existing New Legislative Framework (NLF) regimes and exempting products already covered. They propose merging Annex I sections A and B of the AI Act so sectoral legislation (e.g., machinery, radio equipment, medical devices) can flexibly absorb AI obligations during regular updates, reducing duplication and inconsistent scoping. A parallel priority is aligning terminology with established NLF definitions (e.g., "safety component", "substantial modifications") to close gaps that currently fuel uncertainty and costly compliance checks. In telecoms, legacy, sector-specific instruments—especially the ePrivacy Directive and the Universal Service Obligation—are seen as creating regulatory asymmetries, national fragmentation, and competitive disadvantages versus other digital services. Operators urge urgent inclusion of telecom measures in simplification initiatives (e.g., a Digital Omnibus), repeal or overhaul of USO in favor of targeted vouchers, and harmonisation via refreshed primary acts, noting that disproportionate and inconsistent obligations deter investment and slow innovation (e.g., Open Gateway, advanced anti-fraud and security technologies). Beyond AI and telecoms, sector law integration also entails clarifying scope to avoid misclassification (e.g., excluding product-sellers from the Platform Work Directive where work organization is merely ancillary), establishing sector-specific simplification workstreams (e.g., advisory forum groups), and enabling practical compliance tools (e.g., EU-level EPR). Where safety regimes are simplified (e.g., food and feed), stakeholders emphasize preserving robust protections for health, welfare, and the environment.

> *Products that are already covered by NLF legislation (Annex I, Section A) should therefore be exempted from the provisions of the AI Act.* (ZVEI e.V.)

> *Merge Annex I sections A and B to allow sectoral frameworks (e.g. machinery, radio equipment, medical devices) to integrate AI Act requirements flexibly, reducing duplication.* (Technology Industries of Finland)

More specifically, the Directive imposes unique legal requirements exclusively on telecommunications operators that do not apply to other digital service providers and even within the ePrivacy Directive cookie - related provisions- are stricter than telco related ones (although the first is usually the one that impacts and worries EU citizens the most, leading to a great number of interventions and fines by DPAs). (Telefonica, S.A.)

Given the current context-with broad coverage and multiple affordable options-the USO has largely lost its justification. (Adigital (Asociación Española de la Economía Digital))

ZVEI e.V.: Calls for exempting NLF-covered products from the AI Act and integrating AI-specific requirements into sectoral NLF rules, with aligned terminology to reduce uncertainty.

Where it has not been done already, necessary AI-specific requirements should be integrated into the relevant NLF sector regulation without going beyond the requirements of the AI Act.

Technology Industries of Finland: Urges merging Annex I sections to let sectoral frameworks integrate AI Act requirements flexibly and aligning terminology with NLF definitions to avoid duplication.

Merge Annex I sections A and B to allow sectoral frameworks (e.g. machinery, radio equipment, medical devices) to integrate AI Act requirements flexibly, reducing duplication.

Encode Europe: Proposes a sector-specific digital omnibus and a simplification working group to ensure streamlining reflects diverse business needs.

Secondly, we encourage a sector-specific digital omnibus and suggest that the recently announced AI Act Advisory Forum sets up a working group around simplification, including representatives of advocates for entrepreneurial affairs (e.g. Chambers of Commerce & advocacy organizations).

GSMA: Highlights telecom-specific asymmetries and fragmented ePrivacy implementation that hinder innovation, calling for sectoral streamlining and alignment.

More specifically, the Directive (article 6) imposes unique legal requirements exclusively on telecommunications operators that do not apply to other digital service providers.

Telefonica, S.A.: Advocates accelerating telecom regulatory simplification to address asymmetry with digital services and reduce duplicative ePrivacy burdens.

While we are supportive of common-sense modifications to reporting requirements under the EU's Digital Aquis, these efforts must be matched if not exceeded in terms of pace and ambition with simplification of the telecom's regulatory framework; recognising the regulatory asymmetry that exists between digital services and telecoms operators.

Vorwerk SE & Co. KG: Seeks to exclude product sellers from platform rules by clarifying the PWD scope, using the simplification omnibus to prevent misclassification.

The PWD should be amended to clarify that digital labour platform regulations do not apply to businesses whose main purpose is to sell their own products and where the organisation of the work performed by individuals is a minor and ancillary component of such sales - in the spirit of recital 20 of the PWD which explicitly states that the definition of digital labour platforms "limited to providers of a service for which the organisation of work performed by the individual, [...] constitutes a necessary and essential component, and not only a minor and purely ancillary component."

Adigital (Asociación Española de la Economía Digital): Presents sector-specific simplification proposals across data protection, cybersecurity, and AI, and suggests modernising telecom obligations like USO with targeted instruments.

In particular, chapter 5 includes a series of proposals for regulatory simplification by regulation or sectoral case, including: (i) Data Protection, Privacy and GDPR; (ii) Cybersecurity; and (iii) AI Act.

POLKARMA Polskie Stowarzyszenie Producentów Karmy dla Zwierząt Domowych: Supports simplifying food and feed safety legislation while keeping robust safeguards for public, animal, and environmental health.

As an association committed to promoting high standards of pet nutrition, animal welfare and sustainable development, we appreciate the Commission's efforts to streamline the rules while maintaining mechanisms to protect human health, animal health and the environment.

Vodafone Group: Calls for urgent telecoms simplification and harmonisation, including repealing outdated USO and resetting policy through a Digital Networks Act.

This is where the focus of regulatory simplification is most needed, and where its effect will deliver the broadest benefit to the EU.

Swedtrain - the Swedish Railway Industry Association: Requests sector-specific flexibility for industries with long product lifecycles so AI rules can be integrated pragmatically.

DigitalTrade4.EU: Suggests aligning organic production rules with EUTIR to streamline sector compliance and reduce overlap.

Telekom Austria AG: Urges addressing sector needs directly in primary legislative acts to ensure coherent integration and simplification.

BusinessEurope: Calls for clarifying and whitelisting specialised services to reduce regulatory ambiguity and streamline sectoral obligations.

Healthtech Finland: Recommends sector-specific support and methodologies to implement AI requirements efficiently in healthtech.

Federation of Austrian Industries: Advocates simplified, predictable telecom regulation to foster investment and reduce administrative complexity.

ITI - Information Technology Industry Council: Proposes voluntary sectoral access pathways and preserving manufacturer discretion in how requirements are integrated.

European Casino Association (ECA): Argues that targeted simplification of gambling rules will curb illegal operators while licensed casinos uphold consumer protection.

Forvis Mazars: Requests clear sector-specific guidance for high-risk systems to streamline assessments and compliance.

Connect Europe: Urges greater ambition and speed in telecom simplification to deliver broad benefits across the EU.

PPC: Calls for consistent, sector-specific assessment templates to harmonise and streamline compliance processes.

Global Data Alliance: Emphasises prioritising sector-specific data frameworks to enable lawful cross-border data flows without unnecessary overlap.

SPMS – Shared Services of the Ministry of Health: Recommends a sector-focused simplification approach with strong references to cybersecurity requirements to ensure coherence.

Siemens Healthineers AG: Supports shifting from horizontal AI rules toward integrating AI requirements into sectoral medical device legislation for better alignment.

Computer & Communications Industry Association (CCIA Europe): Advocates applying general sector-wide rules to avoid fragmentation and streamline obligations across industries.

DIGITALEUROPE: Favours integrating AI requirements into sectoral frameworks rather than relying on broad horizontal mandates.

European Games Developer Federation (EGDF): Suggests reallocating telecom-related rules to the EECC to consolidate and streamline the sector's legal framework.

1.10.3 Legacy, Grandfathering & Transition Safeguards

Stakeholders call for robust legacy, grandfathering and transition safeguards to preserve continuity for long-lived, safety-critical sectors. Obligations should apply prospectively and avoid retroactive impacts on systems already placed on the market or contracts signed before new rules, with exemptions for compatible extensions, identical spare parts, and replacement components. Clear guidance on what constitutes a "substantial modification" is needed to assign responsibility and avoid unintended compliance burdens, while legitimate expectations for devices developed before key dates (e.g., 1 August 2024) should be protected. In AI and cybersecurity regimes, industry urges explicit legacy clauses, including for GPAI, and timeline adjustments where standards are not yet available. Operational realities underpin these requests: railway and industrial systems run for decades, and introducing CRA requirements mid-project (e.g., from 11 December 2027) creates mixed fleets and compatibility gaps, inflating costs without added security. Risk-based alternative measures are proposed to justify non-application of certain requirements in ongoing projects, maintaining delivery continuity with adequate protection. Technical constraints—such as protocol changes that break backward compatibility or vehicles that cannot be retrofitted to transmit new data—mean extensions should not force wholesale replacements, and legacy replacement parts should remain exempt to ensure safety, interoperability and proportionality.

> *Protect existing projects by exempting contracts signed before 11 December 2024 for the CRA (i.e. entry into force) and before 12 September 2025 for the Data Act (i.e. entry into force).* (UNIFE)
>
> *Unlike the MDR, which includes transitional provisions under Article 120, the AI Act does not offer any form of grandfathering for existing AI systems.* (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)
>
> *Art. 111: Apply the legacy clause (Art. 111) to all AI already on the market, including GPAI models.* (Technology Industries of Finland)
>
> *Consequence: If the asset owner wants to extend the system, the asset owner will be forced to exchange substantial parts of the installed base, resulting in significant costs without any security benefit.* (SIEMENS AG)
>
> **SIEMENS AG:** Argues that extending existing infrastructure should be exempted or controlled to avoid costly, unnecessary replacements when CRA-compatible products break compatibility. Emphasizes disproportionate compliance costs without security gains.
>
> *Consequence: If the asset owner wants to extend the system, the asset owner will be forced to exchange substantial parts of the installed base, resulting in significant costs without any security benefit.*
>
> **LightingEurope:** Requests clear guidance and responsibility allocation for 'substantial modifications' to existing products. Seeks definitions to determine which components and parties are implicated.
>
> *Manufacturers also hope for clear guidance on 'substantial modifications' to define which product components are affected and to determine responsibility for modifications to existing assets.*
>
> **Technology Industries of Finland:** Advocates applying the AI Act legacy clause to all AI already on the market, including GPAI. This would grandfather existing systems to avoid retroactive compliance.
>
> *Art. 111: Apply the legacy clause (Art. 111) to all AI already on the market, including GPAI models.*
>
> **COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry:** Calls for grandfathering and transitional safeguards for medical AI devices developed before Aug 2024. Notes the AI Act lacks such provisions, unlike MDR, risking legitimate expectations.
>
> *Unlike the MDR, which includes transitional provisions under Article 120, the AI Act does not offer any form of grandfathering for existing AI systems.*
>
> **ANIE Federazione - ANIE ASSIFER:** Proposes exemptions and risk-based alternatives for railway project extensions and ongoing deliveries to preserve continuity and compatibility across long lifecycles. Seeks flexibility around CRA obligations and vulnerability management for legacy systems.
>
> *ANIE ASSIFER considers it essential to preserve delivery continuity for existing projects by allowing manufacturers to adopt alternative measures that ensure an adequate level of cybersecurity protection, to justify the non-application of CRA cybersecurity requirements.*

Bitkom e.V.: Urges postponing high-risk AI timelines to align with standardization, effectively providing transitional relief for existing systems. Aims to prevent premature compliance before standards are finalized.

In particular, the application of high-risk requirements should be postponed by at least 24 months, as key standards are unlikely to be finalised before December 2026 due to the complexity of the consensus-building process.

ALSTOM: Requests exemptions for tailor-made products initiated before Nov 2024 and risk-based measures for ongoing projects to avoid mixed compliance fleets and added costs. Highlights complexities when deliveries straddle the 2027 CRA applicability date.

Tailor made products whose development was launched before November 2024 should be exempted from the CRA.

ACEA (European Automobile Manufacturers' Association): Seeks explicit exemption for legacy replacement batteries in vehicles already on the market. States retrofitting vehicles to meet new data transmission requirements is infeasible.

Clarify the treatment of legacy spare parts, by explicitly stating that batteries used as replacement parts in vehicles already placed on the market shall be exempted from any new requirements that did not apply when the original battery was first placed on the market.

UNIFE: Asks to exempt railway contracts signed before CRA and Data Act entry into force to protect ongoing projects. Warns new rules mid-execution would cause cost and delivery disruptions.

Protect existing projects by exempting contracts signed before 11 December 2024 for the CRA (i.e. entry into force) and before 12 September 2025 for the Data Act (i.e. entry into force).

Swedtrain - the Swedish Railway Industry Association: Advocates excluding legacy contracts and exempting project extensions in the railway sector to safeguard continuity. Emphasizes proportionality for long-running deployments.

Business & Science Poland: Notes late RED standardization forces testing against future requirements, implying need for transitional safeguards. Seeks to avoid retroactive burdens on products already in development.

VDMA - Advancing Europe´s machinery industry: Proposes exempting used products placed on the market before 2025 from new obligations. Aims to prevent retroactive compliance for legacy machinery.

Mafex – Spanish Railway Association: Urges limiting retroactivity and exempting legacy railway contracts to maintain delivery and operational continuity. Supports transition measures tailored to sector complexity.

Polish Confederation Lewiatan: Calls to apply Article 50(4) exemptions to protect legacy products and contracts during transition. Seeks clarity on scope and conditions of such relief.

Association des Constructeurs Européens de Motocycles: Requests exemptions for identical replacement spare parts to keep legacy motorcycles serviceable. Avoids imposing new requirements on maintenance of existing vehicles.

Google: Recommends grandfathering RED-assessed devices under the CRA and streamlining legacy reporting. Seeks to minimize duplication and burden on older product lines.

Business Software Alliance: Urges protection of existing contract terms from new penalties or obligations. Emphasizes prospective application to safeguard legitimate expectations.

Orgalim - Europe's Technology Industries: Supports a strong legacy clause and non-retroactivity to shield existing products and contracts from new rules. Calls for clear, predictable transition safeguards.

Siemens Healthineers AG: Advocates grandfathering legacy medical devices to avoid disruptive re-compliance and protect patient care. Requests transition measures aligned with prior regulatory regimes.

Dassault Systèmes: Warns that legacy product constraints impede full CRA compliance, necessitating transitional flexibility. Seeks proportional, risk-based pathways for older offerings.

Eurosmart: Proposes conditional, risk-based continuity for existing QSCDs to maintain trust services during transition. Balances security with practical legacy constraints.

Dedalus S.p.A.: Asks to exclude legacy devices from data-sharing obligations to preserve compliance and operations. Calls for sector-specific transition safeguards in healthcare IT.

DIGITALEUROPE: Calls for obligations to apply only prospectively, broader legacy clause coverage including GPAI and transparency duties, and expanded exemptions that exclude legacy products from scope. Aims to prevent retroactive burdens across contracts and products.

ECIS, European Committee for Interoperable Systems: Seeks protection of legitimate expectations in existing contracts via grandfathering. Emphasizes stability during transitions to new frameworks.

WindEurope: Requests proportionate treatment of legacy OT across multi-country wind projects. Aims to avoid disruptive retrofits and maintain operational continuity.

APPLiA (Home Appliance Europe): Argues for prospective application of obligations and limited legacy burdens on appliances. Clarifies that 'readily available' data should refer only to new data.

1.10.4 Intra-Group & Outsourcing Carve-outs

This category advocates explicit carve-outs for intra-group activities and narrowly scoped outsourcing to better align sector-specific EU regimes and avoid treating group-internal functions as third-party exposure. Stakeholders argue that intra-group data transfers and services should count as internal processing, with exemptions under NIS2 (including Annex I No. 8 digital infrastructure and Implementing Regulation 2024/2690), DORA (exceptions for treasury services within non-financial groups), the DSA (a corporate privilege for intra-group hosting), and even the CRA (lighter or exempt treatment for products used only within the group). The unifying rationale is risk-proportionate regulation that removes duplicative obligations for entities operating solely within a corporate perimeter, correcting situations where affiliates are currently treated like independent market actors. On outsourcing, contributors seek to prevent expansive classifications that trigger heavy third-party regimes where risks are limited or already addressed. They oppose labeling EBW/EUDIW-based authentication as outsourcing under PSD2 revisions, arguing it would force PSPs into dozens or hundreds of contracts and slow adoption of strategic EU initiatives. Several propose alignment mechanisms—such as allowing purely group-internal IT providers to follow DORA-style reporting instead of full NIS2—so compliance reflects real operational risk rather than corporate structure.

For intra-group data transfers, an exception should be made so that such transfers are treated as internal processing, not as disclosure to third parties. (Volkswagen Group)

To alleviate these issues, a corporate privilege should be introduced, whereby the DSA does not apply to intra-group hosting. (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)

Treating these solutions as outsourcing as currently proposed by the EC as part of the revision of the PSD2 would significantly restrict PSPs' ability to make use of them as card issuers would need to conclude dozens, if not hundreds, of outsourcing agreements with all possible providers of authentication and authorization solutions. (Mastercard Europe SA)

In order for the EBW and EUDIW to be used for the authentication of payments, PSPs would be required to enter into outsourcing agreements with each EBW/EUDIW provider, creating unnecessary friction and regulatory burden and potentially delaying consumer adoption of these strategic EU initiatives. (Mastercard Europe SA)

Volkswagen Group: Calls for deregulating intra-group data transfers and services by treating them as internal processing and exempting group-only digital infrastructure from NIS2 implementing requirements.

For intra-group data transfers, an exception should be made so that such transfers are treated as internal processing, not as disclosure to third parties.

German Insurance Association: Requests carve-outs from NIS2 for purely group-internal IT service providers, proposing alignment with DORA reporting as an alternative. Seeks to exempt non-financial intra-group providers to avoid duplicative obligations.

llow purely group-internal IT service providers to voluntarily follow DORA- aligned reporting obligations, in which case they would be exempted from NIS2 requirements.

Mastercard Europe SA: Opposes classifying EBW/EUDIW-based authentication solutions as outsourcing under PSD2, warning it would impose extensive contracting burdens on PSPs. Argues such treatment would hinder adoption and create unnecessary friction.

Treating these solutions as outsourcing as currently proposed by the EC as part of the revision of the PSD2 would significantly restrict PSPs' ability to make use of them as card issuers would need to conclude dozens, if not hundreds, of outsourcing agreements with all possible providers of authentication and authorization solutions.

Adigital (Asociación Española de la Economía Digital): Urges exemptions for intra-group financial services, particularly corporate treasury within non-financial groups, citing minimal systemic risk. Calls for DORA exceptions for group-managed treasury functions to remove unjustified compliance burdens.

Additionally, it is critical to exempt intra-group financial services (e.g., treasury services for subsidiaries of a non-financial group) from the regulatory framework.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Proposes a corporate privilege that excludes intra-group hosting from DSA obligations. Aims to relieve companies from stringent DSA requirements for services and data hosted within their own group.

To alleviate these issues, a corporate privilege should be introduced, whereby the DSA does not apply to intra-group hosting.

Bayerische Motoren Werke Aktiengesellschaft: Advocates exempting products provided solely within a corporate group from the CRA to avoid disproportionate compliance burdens for non-external deployments. Seeks recognition that intra-group use warrants lighter regulation.

Association des Constructeurs Européens de Motocycles: Calls for a CRA exemption for products used internally within corporate groups, separating them from consumer-facing obligations. Argues intra-group provisioning should not trigger full CRA compliance.

1.10.5 Product-Specific Proportionality

Product-Specific Proportionality prioritises tailoring horizontal rules to the realities of particular products and sectors, and aligning with existing regimes. For AI wearables, stakeholders argue that the Batteries Regulation's Article 11 on user-removable batteries is misaligned with miniaturised devices, forcing redesigns that would weaken performance and durability, raise safety risks, and paradoxically undermine Circular Economy and Ecodesign goals. They also flag an unworkable implementation timeline that creates a regulatory cliff edge, urging exemptions or delegated acts to calibrate obligations. In automotive, proponents seek full exemption of motor vehicles from the AI Act given the comprehensive UNECE type-approval system already covering functional safety, cybersecurity, and software updates, warning that duplicate EU requirements would add costs and inconsistency without additional safety benefits. Consistent with proportionality, they urge limiting the Battery Passport to relevant static parameters (e.g., linking state-of-health to Euro 7), cautioning that dynamic data mandates without mature standards would inflate costs, legal uncertainty, and fragmentation. Across other sectors, the theme is targeted scope and legacy-aligned carve-outs: recognizing unique customs-controlled retail environments, streamlining rules for safety technologies, focusing battery and vehicle data reporting on key parameters and shorter collection periods, curbing over-broad device obligations (e.g., under RED delegated acts), avoiding generalized common specifications, and clarifying or broadening exemptions for essential functionalities and spare parts. The common thread is to preserve innovation and competitiveness while ensuring safety and sustainability through sector-specific calibration rather than one-size-fits-all mandates.

Motor vehicles should be fully exempted from the AI Act, as they are already regulated under a robust international framework, through the UNECE type-approval system. (ACEA (European Automobile Manufacturers' Association))

The requirement may seem reasonable for household appliances, but it is fundamentally misaligned with the realities of miniaturised, sophisticated devices like AI wearables. (Meta Platforms Ireland Limited)

Mandating consumer-removable batteries in these devices results in weaker, shorter-lived batteries, excess expired inventory, and increased electronic waste. (Meta Platforms Ireland Limited)

Even with derogations by 2026, manufacturers would have less than one product cycle to adapt before rules apply in February 2027-a regulatory cliff edge that creates legal uncertainty and risks freezing investment in next-generation technologies. (Meta Platforms Ireland Limited)

Meta Platforms Ireland Limited: Calls to reform and simplify the Batteries Regulation, noting Article 11 is misaligned with AI wearables. Urges delay or exemptions to protect device integrity, safety, design and circular economy objectives.

The requirement may seem reasonable for household appliances, but it is fundamentally misaligned with the realities of miniaturised, sophisticated devices like AI wearables.

ACEA (European Automobile Manufacturers' Association): Advocates full exemption of motor vehicles from the AI Act due to comprehensive UNECE type-approval, and limiting the Battery Passport to static parameters. Warns that overlapping EU requirements would add costs without safety benefits.

Motor vehicles should be fully exempted from the AI Act, as they are already regulated under a robust international framework, through the UNECE type-approval system.

European Travel Retail Confederation (ETRC): Highlights the duty- and tax-free retail sector's unique customs-controlled environment, arguing for proportionate, sector-specific treatment and exemptions aligned to that context.

ENSHPO - The European Network of Safety and Health Professional Organizations: Supports targeted, streamlined regulatory reforms for safety technologies to ensure proportionate, product-specific requirements that accelerate safe deployment.

Japan Business Council in Europe (JBCE): Urges limiting the Battery Passport to key static parameters and shortening OBFCM data collection periods to ensure proportionate obligations for automotive batteries and monitoring.

Confederation of Industry of the Czech Republic: Calls to withdraw or revise the RED delegated act and narrow device obligations, applying a proportionate, product-specific approach to connectivity and cybersecurity requirements.

Verband der Automobilindustrie e.V.: Promotes a tailored scope and sector-specific criteria so automotive AI and digital systems face proportionate obligations reflecting existing frameworks and risk profiles.

Computer & Communications Industry Association (CCIA Europe): Opposes broad generalisation of common specifications, favoring flexible, product-specific standards to avoid one-size-fits-all compliance burdens.

European Publishers Council: Seeks exemptions for essential publishing functionalities to maintain proportionality and avoid undue burdens on sector-specific tools and workflows.

DIGITALEUROPE: Requests clearer and broader spare parts exemptions to ensure proportionate, product-specific compliance across repairs and maintenance.

1.10.6 Cybersecurity, Critical Infrastructure & Digital Services Carve-outs

Stakeholders call for targeted carve-outs and alignment across cybersecurity, critical infrastructure, and digital services to avoid duplicative or ill-suited obligations while preserving high assurance. Proposals include simplifying and clarifying rules for critical infrastructure, distinguishing defensive cybersecurity AI from high-risk categories, and automatically exempting highly sensitive infrastructure data from mandatory sharing. They urge coherence between horizontal frameworks (e.g., NIS2, CER, CSA, CRA, DORA) and sector regimes—clarifying the scope of "critical digital infrastructure," keeping SIPS/core processing outside overlapping oversight where already regulated, and recognizing existing sector risk practices. Sensitive use contexts should get tailored treatment (e.g., a non-public registry for certain high-risk AI uses, and an eID framework compatible with critical sectors' operational and security needs). Sector-specific and legacy exemptions are sought to respect technical realities and deployment timelines: explicit CRA carve-outs for maritime equipment and engines; exemptions to allow extensions of rail/grid systems without forcing full retrofits; postponing machinery cybersecurity requirements; restricting public vulnerability disclosure in rail; and adopting CER-style duplicate exemptions. Digital service carve-outs include removing ill-fitting telecom-style rules from IoT M2M connectivity, avoiding the extension of telecom obligations to cloud, streamlining ICT oversight in finance, and clarifying component and sectoral exemptions (e.g., for financial services, automotive UN-R155, defense/classified products). A "principle of sufficiency" is widely advocated: compliance with a comprehensive horizontal law should satisfy similar obligations in overlapping acts, supported by EU guidance, cost-benefit tests, and a roadmap for repeal or streamlining of sectoral provisions.

> *Sector-specific cybersecurity laws should be repealed or significantly streamlined where horizontal regulations, such as NIS2, already impose equivalent security requirements.* (Telefonica, S.A.)
>
> *Accordingly, targeted simplifications or exemptions for cybersecurity-related Al use cases could enhance Europe's defensive capabilities while maintaining transparency and accountability.* (Kaspersky Labs Limited)
>
> *However, high-risk AI systems used for law enforcement, migration, asylum and border control are registered in a different non-public EU database where less information is required.* (Centre for Democracy and Technology Europe)
>
> *However, based on independent legal assessments, this exemption does not apply to marine engines, as they are not listed in the annex of Implementing Regulation (EU) 2024/1533.* (EUROMOT - The European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers)

Verband kommunaler Unternehmen e.V.: Calls for simplified and clarified AI rules for critical infrastructure, along with prompt guidance on substantial modifications to enable timely compliance.

> *Specifically, simplification and clarification of the rules for critical infrastructure would be important.*

Kaspersky Labs Limited: Supports targeted carve-outs or simplifications for defensive cybersecurity AI, distinguishing it from high-risk systems to enhance Europe's defenses while ensuring accountability.

> *Accordingly, targeted simplifications or exemptions for cybersecurity-related Al use cases could enhance Europe's defensive capabilities while maintaining transparency and accountability.*

Enel SpA: Urges automatic exemptions from mandatory data sharing for highly sensitive critical infrastructure data to protect security and operational integrity.

> *Establishing automatic exemptions for highly sensitive data related to critical infrastructure, ensuring that such data is protected from mandatory sharing obligations.*

EUROMOT - The European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers: Highlights a regulatory gap that subjects marine engines to the CRA despite maritime regimes, proposing an explicit maritime carve-out for equipment and propulsion systems.

> *The scope exemption provided for in Article 2(4) of this Regulation applies to equipment :selected: covered by Directive 2014/90/EU (Marine Equipment Directive) and applicable to marine equipment, devices, propulsion systems that are subject to other international conventions and fall within the scope of the EU Cyber Resilience Act.*

European Energy Information Sharing and Analysis Centre: Stresses that the European Digital Identity framework must align with the operational and security needs of critical sectors, ensuring compatibility with high-assurance environments.

The European Digital Identity framework must meet the operational and security needs of critical sectors.

Telefonica, S.A.: Advocates streamlining by repealing sector-specific cybersecurity rules where horizontal frameworks like NIS2 already apply, using a sufficiency principle across overlapping laws.

Where other legislation imposes similar security requirements on digital service providers (eg. DORA, RED), full compliance with the similar comprehensive relevant law (eg. NIS2) must be deemed sufficient to satisfy the obligations under all related acts, for example on audits or supply chain requirements.

Centre for Democracy and Technology Europe: Notes tailored treatment for sensitive public-sector uses of high-risk AI via a separate non-public registry with reduced disclosures.

However, high-risk AI systems used for law enforcement, migration, asylum and border control are registered in a different non-public EU database where less information is required.

Mastercard Europe SA: Seeks to exclude SIPS and core processing from DORA's direct scope given existing robust oversight, avoiding duplicative ICT regulation.

Under DORA, for example, systemically important payment systems (SIPS) should remain out of scope of the direct applicability of DORA, as they are already regulated under existing frameworks and subject to cyber risk and operational resilience requirements under it SIPS designation, in particular Article 21 of SIPS Regulation on Cyber Risk and the Cyber Resilience Oversight Expectations framework.

LSEG: Requests clarity on the scope of "critical digital infrastructure" to avoid overlap with DORA and inconsistent treatment of financial entities, potentially via explicit exclusions.

To avoid confusion, it would be helpful to clarify how these frameworks interact or explicitly exclude these categories from the definition of 'critical digital infrastructure'.

Finnish Food and Drink Industries´ Federation (ETL): Asks that existing, business-driven CER risk management practices be recognized to avoid duplicative or misaligned obligations for the sector.

Regarding risk management obligations, particularly under the CER Directive, companies existing business-driven risk management practices should be recognised and accepted.

Vodafone Group: Calls for a carve-out so IoT services are not subject to ill-suited, person-to-person telecom rules and fragmented national requirements, enabling pan-EU deployment.

A carve-out would accelerate cross-border service deployment, reduce compliance costs, and allow operators to reinvest in innovation, infrastructure and pan-EU connectivity platforms.

UNIFE: Warns that legal uncertainty in CRA application to rail could disrupt critical projects, and urges exempting extensions to existing rail or grid systems from CRA scope.

Ensure that extensions to existing major infrastructure systems, such as rail or grid systems, are exempted from the scope of the CRA.

EVOLIS: Recommends postponing application of cybersecurity requirements under the Machinery framework as a sector-specific timing carve-out to ensure readiness.

Mafex – Spanish Railway Association: Advocates restricting vulnerability disclosure obligations for the rail sector to mitigate security risks while maintaining proportionate transparency.

CENTR - Council of European Top Level Domain Registries: Urges adopting CER-style duplicate exemptions to shield critical internet infrastructure operators from overlapping cybersecurity obligations.

Association des Constructeurs Européens de Motocycles: Requests explicit exemptions for defence-related and classified products from civilian cybersecurity regimes to preserve security and regulatory coherence.

Google: Opposes extending telecom-style regulations to cloud services, favoring sector-appropriate frameworks to avoid misaligned obligations.

AFME: Supports sectoral exemptions in the CRA for financial services to prevent duplication with DORA and ensure coherent oversight.

CLEPA: Seeks clarification on CRA component exemptions so automotive parts integrated into vehicles align with sectoral rules and avoid duplicative compliance.

European Fund and Asset Management Association (EFAMA): Calls for streamlined ICT risk oversight under DORA with clear exclusions to prevent overlap for asset managers and related entities.

Orgalim - Europe's Technology Industries: Proposes limiting NIS2 scope to main energy producers to reduce unnecessary burdens on ancillary industrial actors.

Renault Group: Urges alignment with UN R155 by recognizing exemptions and legitimate-interest bases to ensure practicable, consistent automotive cybersecurity rules.

Estonian Ministry of Justice and Digital Affairs: Recommends refining NIS2 sector definitions to better align with sector boundaries and legacy regimes, reducing ambiguity and overreach.

1.10.7 Financial Services & Digital Regulation Alignment

Stakeholders call for digital regulation that treats sectoral financial rules as lex specialis. They urge exempting DORA-regulated entities from overlapping horizontal regimes like the Cyber Resilience Act, harmonising cybersecurity obligations and centralising incident reporting, and allowing firms to rely on existing governance and third-party oversight under frameworks such as AIFMD/UCITS and Solvency II. The aim is to avoid duplicative or diverging requirements in an already highly regulated sector and ensure proportionality. For AI, they seek consistency between the AI Act and sectoral rules and supervisors, with limited, targeted derogations where robust sectoral controls exist. Priorities include clarifying and narrowing high-risk classifications for financial use cases; recognising EIOPA-guided insurance governance as sufficient; reconsidering Annex III for insurance risk/pricing and acknowledging that profiling in insurance can be an operational necessity; reducing extra burdens like FRIA where GDPR and anti-discrimination rules already apply; and providing practical guidance and templates ahead of application. They also ask the AI Act to recognise established AML/financial crime compliance frameworks and to interpret fraud-detection exceptions as covering financial crime more broadly, while deeming algorithmic evaluations mandated by finance law compatible to avoid duplication. Adjacent alignment in digital finance includes calibrating payment rules (e.g., refund obligations for merchant-initiated transactions under PSD3/PSR) to avoid market distortions and excluding gatekeepers from registering as financial information service providers to safeguard competition and stability.

We recommend that the Digital Operational Resilience Act (DORA) be explicitly recognised as lex specialis within the context of the Cyber Resilience Act (CRA). (European Associations of Co-operative Banks (EACB))

Cyber Resilience Act: financial entities in scope of DORA should be excluded. (ALFI - Association of the Luxembourg Fund Industry)

Such a provision risks encompassing systems that are legitimately and routinely used in certain sectors and may inadvertently include AI applications that are intrinsic to the business models of industries such as insurance, where profiling is a technical necessity rather than a risk factor. (Unipol Assicurazioni S.p.A.)

For further clarity, it would be helpful to specify in the AI Act that the exception for AI systems 'used for detecting financial fraud' should be understood as referring to financial crime more broadly since fraud is just one of many financial crime predicate offences together with anti-money laundering and others. (LSEG)

ALFI - Association of the Luxembourg Fund Industry: ALFI urges leveraging existing sectoral governance for delegations and third-party oversight to avoid overlap with DORA. It calls for fully excluding DORA-covered financial entities from the CRA to prevent duplicative compliance.

We would reiterate that Financial Entities in the scope of DORA should be fully excluded from the scope of the CRA, so as to avoid redundancy of regulatory requirements.

Unipol Assicurazioni S.p.A.: Unipol argues insurance's sectoral frameworks (Solvency II, IDD, DORA and EIOPA guidance) sufficiently manage AI risks. It seeks scoping and classification adjustments (Annex III removal, Article 6 flexibility, and excluding gatekeepers from FISPs) to align the AI Act with insurance practices.

The insurance sector is already governed by strong sectoral regulatory frameworks (e.g. Solvency II, IDD, DORA), which includes also guidance on AI governance and risk management recently issued from EIOPA.

Eurofinas: Eurofinas warns that extending regulation beyond intended scope risks over-regulation in a sector already covered by extensive rules. This could reduce credit availability and hinder digitalisation and financial inclusion.

The financial services sector is already among the most highly regulated in Europe, operating under an extensive framework that includes both sector- specific and horisontal legislation, i.e., for our industry, notably the Consumer Credit Directive (CCD), GDPR, cybersecurity legislation, Anti-Money Laundering rules, as well as the advancing AI Act.

German Insurance Association: The German Insurance Association advocates exempting DORA-regulated financial companies from CRA requirements and minimally adapting Solvency II to align with DORA. It also opposes additional FRIA burdens where sectoral protections already exist.

We therefore call for the Commission to exempt DORA-regulated financial companies from the equivalent but not identical CRA requirements.

Centre for Democracy and Technology Europe: CDT Europe notes concerns about added regulatory burden for sectors with existing rules and highlights AI Act measures to ensure consistency. It points to maintaining common supervisors and limited derogations for quality management and monitoring to avoid duplication.

Noting that these sector-specific laws are expected to apply to financial entities when they use AI systems in addition to the AI Act itself, the Act takes steps to ensure consistency by ensuring the supervisory authorities under all applicable laws remain the same and by envisaging limited derogations to core obligations within the AI Act relating to quality management and monitoring obligations.

LSEG: LSEG requests clearer high-risk criteria for financial services under Annex III and early guidance to ensure legal certainty. It also seeks clarity that fraud exceptions cover broader financial crime and notes AML frameworks already enable compliant AI use.

Clearer criteria are needed for what constitutes high-risk AI systems under Annex III in relation to financial services.

Adigital (Asociación Española de la Economía Digital): Adigital recommends adjusting PSD3/PSR refund rules to avoid distortions in digital payments and creating a single EU license for non-bank consumer credit. It calls for treating algorithmic checks mandated by finance rules as compatible with AI Act obligations to avoid duplication.

Algorithmic evaluations already required under financial regulations (e.g., CCD2, MiFID) should be considered compatible with the AI Act requirements to avoid duplication.

ING Group: ING urges harmonizing cybersecurity rules by exempting financial services from CRA and centralising incident reporting. It stresses that banking ICT is integral to regulated services already meeting DORA's resilience requirements.

Cybersecurity: Harmonise overlapping cybersecurity requirements, exempt financial services from CRA, and centralise incident reporting through a single EU channel.

European Associations of Co-operative Banks (EACB): EACB supports simplifying cybersecurity regulation by recognizing DORA as lex specialis over CRA for financial entities. This would clarify primacy and reduce duplicative obligations.

We recommend that the Digital Operational Resilience Act (DORA) be explicitly recognised as lex specialis within the context of the Cyber Resilience Act (CRA).

DigitalTrade4.EU: DigitalTrade4.EU seeks EU recognition of digital negotiable instruments to align financial services rules with digital transaction realities. This would modernize sectoral frameworks without duplicative obligations.

Bayerische Motoren Werke Aktiengesellschaft: BMW highlights that DORA oversight can impose disproportionate burdens on ancillary insurance intermediaries. It calls for proportional, sector-appropriate application and exemptions where activities are incidental.

BusinessEurope: BusinessEurope advocates including electronic communications networks in the EU taxonomy to align financing criteria with digital infrastructure realities. This aims to improve consistency across sectoral and financial frameworks.

Confederation of Norwegian Enterprise (NHO): NHO seeks the inclusion of ECNs in taxonomy eligibility to align sustainable finance criteria with essential digital infrastructure. This supports coherent sector-specific recognition in financial regulation.

Inter IKEA Group: Inter IKEA urges aligning digital acts with sustainability regulations to avoid conflicting obligations and ensure coherent compliance frameworks across sectors. This alignment supports predictable obligations for businesses.

CENTR - Council of European Top Level Domain Registries: CENTR argues DORA oversight is ill-suited to DNS operations and ccTLD registries and seeks exemptions from financial-sector style oversight. It warns that the model does not fit the DNS ecosystem and could create misalignment.

ASNEF: ASNEF calls for explicit authorization of automated decision-making in financial services in line with sectoral and data protection rules. This would enable digital credit processes while maintaining compliance.

Federation of European Securities Exchanges: FESE proposes excluding standard ICT services from DORA's scope and resolving conflicts with MiCAR requirements to avoid duplication. This alignment would better reflect capital markets infrastructure realities.

Association des Constructeurs Européens de Motocycles: ACEM suggests using insurance revenue-based metrics when setting regulatory thresholds to better calibrate applicability. This would align requirements with sectoral business models.

AFME: AFME seeks streamlining and alignment of DORA with existing regimes, removing duplicative requirements and clarifying scope. The aim is a coherent framework that supports operational resilience without unnecessary burden.

Business Software Alliance: BSA supports contractual flexibility under DORA to tailor risk and resilience obligations between financial entities and ICT providers. This helps avoid rigid, duplicative requirements while maintaining accountability.

European Fund and Asset Management Association (EFAMA): EFAMA notes asset managers already comply with strict sectoral requirements and seeks avoiding duplicate AI disclosure obligations for fund materials while ensuring oversight. It emphasizes proportionate alignment with existing governance.

Digital Currencies Governance Group (DCGG): DCGG urges recognition of MiCA taxonomy for crypto-asset service providers to ensure consistent classification and alignment across digital and financial regulations. This would streamline oversight and reduce ambiguity.

Insurance Europe: Insurance Europe calls for standardized EU DORA templates and contractual terms and for insurance supervisors to oversee AI Act implementation. These steps would ensure consistent, sector-aligned compliance.

European Savings and Retail Banking Group: The European Savings and Retail Banking Group advocates excluding the financial services industry from CRA, clarifying eIDAS2/EUDIW payment obligations, and recognizing DORA as lex specialis. This alignment would reduce duplication and improve supervisory coherence.

1.10.8 Health & Medical AI Alignment

This category argues for a sector-specific alignment of the EU AI Act with the existing medical device framework (MDR/IVDR), treating MDR as the lex specialis for health AI. Stakeholders call to avoid duplicative and potentially conflicting obligations by embedding core AI requirements (e.g., human oversight, data governance, logging) directly into MDR/IVDR and shifting medical AI from horizontal "high-risk" to sector-specific provisions. They emphasize using existing governance and Notified Bodies, leveraging established conformity assessment, post-market surveillance, and PMCF as effective, ongoing human oversight; and harmonizing definitions and interpretations (including AI, significant/substantial change) across the EU with joint guidance, glossaries, and a uniform, "stop-clock" approach. Operationally, contributors warn that MDR Rule 11 overclassifies software and that additional AI Act documentation, combined with limited Notified Body capacity, threatens timelines, innovation, and patient access. They propose streamlined documentation (e.g., EUDAMED), convergence on harmonized standards (CEN/CENELEC, IMDRF), targeted pathways for orphan/pediatric/breakthrough devices (including conditional certifications), and clear treatment of investigational/pre-market research. The overarching aim is coherent, feasible, and proportionate rules that protect patients, support clinical workflows, and deliver legal certainty without burdening clinicians or slowing beneficial medical AI.

We strongly support a sector-specific approach for AI-enabled medical technologies, alignment with MDR/IVDR, protection of well- established products, structured and interoperable health data, and practical implementation strategies to support both Member States and industry. (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)

COCIR recommends moving AI systems regulated under MDR and IVDR from Annex I Section A (horizontal high-risk AI) to Section B (sector-specific legislation). (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)

As a result, common sense tools such as clinical calculators, medication advisories, and risk scoresreadily managed under healthcare organization protocolsface slow, burdensome approvals in the EU, delaying innovation and patient benefit. (Epic Systems)

We propose embedding relevant high-risk AI requirements, such as human oversight, data governance, logging, directly into Annex I of MDR/IVDR during upcoming revisions or as part of the Digital Omnibus Package. (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)

Epic Systems: Argues MDR Rule 11 overclassifies most healthcare software and, combined with new AI Act documentation and capacity constraints, slows innovation and patient benefit. Calls for sensible exemptions and alignment to avoid duplicative burdens.

Rule 11 of MDR effectively classifies nearly all healthcare software as at least a Class II device.

DigiFinland: Urges harmonizing AI Act definitions with MDR/IVDR, aligning the concept of significant change by sector, and providing joint guidance with practical use cases. Stresses assessing the AI Act alongside MDR/IVDR, EHDS, and the Data Act for coherence.

It is vital that the AIA is assessed as a whole, together with the medical device legislation (MDR, IVDR), as well the EHDS and data act.

Zimmer Biomet: Calls for aligning horizontal digital rules and the AI Act with MDR to protect patient access while minimizing unnecessary administrative burden. Notes MDR already provides robust safety and security safeguards.

When horizontal digital rules apply on top of MDR obligations, alignment is essential to safeguard patient access to high-quality, modern devices while avoiding unnecessary administrative burden.

PHOENIX group: Supports enabling online prescription authentication via nationally approved electronic identity methods to reduce the need for in-person ID checks. Aims to improve access and efficiency in pharmacy services.

That said, we support facilitating patient authentication for online ordering of prescription (Rx) medicines via range of nationally approved electronic identity verification methods (eID, bank ID, trusted video ID, or equivalent).

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Advocates a sector-specific approach for medical AI by moving MDR/IVDR-regulated systems out of horizontal high-risk AI and embedding key AI requirements into MDR/IVDR. Seeks to avoid duplicate obligations and ensure regulatory clarity and feasibility.

COCIR recommends moving AI systems regulated under MDR and IVDR from Annex I Section A (horizontal high-risk AI) to Section B (sector-specific legislation).

TEAM-NB: Recommends using existing MDR/IVDR frameworks and Notified Body structures to implement AI oversight smoothly and uniformly. Emphasizes avoiding duplication and ensuring continuity for a high-safety sector in transition.

Team NB and NBCG-Med therefore suggest using existing frameworks for appointing NBs under the regulations to avoid duplicate efforts for NBs.

: Proposes recognizing MDR as lex specialis for medical AI, avoiding duplicative AI Act human oversight where MDR provides comparable protections. Highlights MDR's continuous clinical oversight and stringent NB involvement as sufficient safeguards.

Article 14 (6) Without prejudice to paragraphs 1 and 2, in the case of high-risk AI systems which are also medical devices pursuant to Regulation (EU) 2017/745 (MDR), the human oversight requirements laid down in this Article and in the related implementing acts shall not apply to the extent that Regulation (EU) 2017/745 (MDR) and subsequent sectoral Union legislation lay down specific requirements to ensure the protection of the health, safety and fundamental rights of data subjects comparable to the objectives of human oversight under this Regulation.

Alcon Laboratories Inc: Calls to streamline EUDAMED registrations, expand harmonized standards, and promote global convergence. Recommends special pathways and conditional certifications to accelerate safe patient access.

Expand use of harmonised standards developed by CEN/CENELEC to align with global norms

EHIMA: Advocates aligning AI obligations with MDR to avoid duplication and ensure clear, proportionate responsibilities for manufacturers in hearing health. Emphasizes coherence to protect patient access and safety.

VDGH – Verband der Diagnostica-Industrie e.V.: Urges prioritizing MDR/IVDR as the primary regime for medical AI and limiting extra AI Act obligations. Aims to reduce regulatory burden while maintaining patient safety and innovation.

Japan Business Council in Europe (JBCE): Calls for flexible sector-specific integration of AI rules and clearer delineation for MDR/IVDR-governed systems. Seeks to prevent overlap and provide predictable compliance pathways.

Healthtech Finland: Proposes a practical framework for clinical evidence and pre-market research for AI-enabled medical devices. Seeks streamlined, consistent processes aligned with MDR/IVDR.

Brighten Digital: Recommends piloting AI governance in healthcare and the public sector to refine practical implementation. Aims to generate lessons for broader, effective rollout.

MedTech Europe: Seeks AI Act alignment with MDR/IVDR, exemptions for investigational devices, and clearer definitions including EHR scope. Aims to avoid duplication and reduce uncertainty for medical AI developers.

kaiko.ai: Suggests reimagining conformity assessment for medical AI to fit iterative development cycles while safeguarding patients. Emphasizes proportionate, risk-based oversight.

Bayer AG: Advocates uniform EHDS implementation with clear scope and targeted exemptions. Aims to enable health data use while minimizing regulatory friction and overlap.

Johnson & Johnson: Calls to streamline overlapping MDR and AI Act assessments and optimize clinical trial processes. Seeks faster, safe deployment of AI-enabled medical technologies.

BVMed - Bundesverband Medizintechnologie e.V.: Warns that overlapping rules risk market disruption and reduced patient access. Urges integrating AI requirements into MDR and enabling MDR Notified Bodies to handle AI oversight.

Siemens Healthineers AG: Supports a sectoral approach embedding AI requirements within MDR/IVDR and leveraging specialized expertise. Emphasizes aligning AI and device rules to target medical risks effectively.

BioMed Alliance: Stresses that AI regulation should not add administrative burdens to healthcare professionals. Calls for alignment with clinical workflows and existing safety frameworks.

Dedalus S.p.A.: Endorses sector-specific medical AI rules coordinated with MDR/IVDR to ensure feasibility and interoperability. Aims for practical, patient-safe implementation.

European Society of Radiology: Urges harmonization between the AI Act and MDR post-market surveillance for coherent safety monitoring. Seeks clarity to support safe adoption of AI in radiology.

Relyens Mutual Insurance: Recommends adapting AI technical requirements and oversight to caregivers' realities and healthcare settings. Focuses on pragmatic risk management and usability.

The European Network of Expertise on Omics: Proposes a one-stop-shop for health AI compliance and coherent Union-wide omics rules, prioritizing patient safety and ethics. Seeks streamlined, ethical adoption across Member States.

1.10.9 Industrial, Energy & Transport Alignment

Stakeholders across industrial, energy, and transport domains call for sector-specific alignment that builds on existing sectoral regimes to avoid duplicative and conflicting obligations. They urge tailored guidance on applying horizontal digital laws (AI Act, Data Act, NIS2, GDPR) to sector use cases, legal certainty anchored in established frameworks (e.g., UNECE automotive type-approval, maritime regulations, rail standards), and prevention of double regulation and disproportionate costs. In energy, this includes clarifying high-risk classifications, reflecting the interplay with digital policies in sector statutes, and, upstream, harmonising fiscal levers that enable grid, storage, and alternative-fuel investments. Continuous dialogue with sector communities is emphasized to track real-world impacts and adapt rules as risks evolve. Legacy exemptions and lifecycle realities are central: long-lived assets (notably rail) require proportionate cybersecurity and update obligations, with exemptions or tailored timelines to reflect 20–40 year lifecycles and B2B, safety-critical contexts. Calls include dedicated sectoral law for in-vehicle data, limiting duplicative CRA coverage (e.g., maritime and automotive components), and aligning new data/reporting requirements (e.g., battery SOCE) with sector rollouts to avoid premature burdens. Practical enablers—streamlining ex-ante authorisations, deploying AI for customs and eFTI freight digitalisation—are highlighted to reduce fragmentation, accelerate secure deployment, and ensure consistency across EU and international regimes.

Adopt sector-specific regulation for Industrial AI to reflect practical use cases and reduce unnecessary burdens. (ZVEI e.V.)

Need for sector-specific guidance in energy. (Enel SpA)

Articles 107 and 109 of the AI Act, and the corresponding amendments to Regulations (EU) 2018/858 and 2019/2144 should be repealed. (ACEA (European Automobile Manufacturers' Association))

Article 22 of the GDPR restricts automated decision-making, whereas the AI Act adopts a more risk-based, flexible approach for high-risk AI systems. (Adigital (Asociación Española de la Economía Digital))

: Calls for harmonising energy taxation and fees across Member States to align incentives for investment in critical energy infrastructure and hard-to-electrify industrial use cases.

This new framework will harmonise energy taxation and fees across Member States and introduce tax incentives and state aid rules to encourage large-scale investments in smart grids and smart meters, heating and cooling tech- nologies, storage solutions, high-voltage power lines and alternative energy carriers like hydrogen for hard- to-electrify industrial use cases.

SIEMENS AG: Requests clarification of AI Act Article 106 to allow necessary flexibility for railway products, aligning obligations with rail sector specifics.

To effectively address the specific requirements for railway products, a clarification of Art. 106 Al Act is needed, indicating the necessary flexibility, e.g. by adding: "(...) [shall be taken into account] to the extent necessary for the specific application".

ZVEI e.V.: Advocates sector-specific regulation of Industrial AI to reflect practical use cases and reduce unnecessary burdens on industry.

Adopt sector-specific regulation for Industrial AI to reflect practical use cases and reduce unnecessary burdens.

Enel SpA: Seeks sector-specific guidance for energy and clarity on high-risk classifications, proposing that impacts of digital laws be embedded in sectoral energy legislation for coherence.

Though guidance about the interplay of the Data Act with energy laws such as the RES Directive is welcomed, Enel would like to propose inserting the impacts of digital laws in the revisions of sectorial laws, as it has been already done with the GDPR.

EUROMOT - The European Association of Internal Combustion Engine and Alternative Powertrain Manufacturers: Urges recognition of comprehensive international maritime rules to avoid duplicative CRA requirements, ensure legal certainty, and prevent disproportionate costs.

Applying CRA requirements to maritime propulsion systems would duplicate existing international obligations and create legal uncertainty.

Volkswagen Group: Calls to simplify the AI Act by shifting Industrial AI to sector-specific regimes and excluding Annex I to avoid overlap.

The AI Act should be simplified by shifting to sector specific regulation of Industrial AI by excluding Annex I.

European Energy Information Sharing and Analysis Centre: Encourages ongoing engagement with energy-sector communities to align frameworks with real-world resilience goals and adapt to evolving threats.

Ongoing engagement with sector-specific communities like EE-ISAC can help the Commission monitor unintended consequences and adapt the framework as threats evolve.

Unipol Assicurazioni S.p.A.: Argues that fair access to in-vehicle data requires dedicated sectoral legislation beyond horizontal frameworks to ensure harmonised implementation.

Furthermore, ensuring fair access to in-vehicle data requires dedicated sectoral legislation that moves beyond the Data Act.

ANIE Federazione - ANIE ASSIFER: Highlights mismatch between CRA update obligations and 30-year rail lifecycles, warning of extreme costs and calling for tailored exemptions for railway systems.

In railway sector, trains have a long lifecycle, typically around 30 years, resulting in extremely high costs for manufacturers.

Adigital (Asociación Española de la Economía Digital): Notes the complexity of aligning GDPR, AI Act, and NIS2 with transport-specific laws and that legacy ex-ante authorisations slow digital network rollout; supports AI and digital tools in customs and freight.

In the transport sector, for instance, aligning the GDPR, AI Act, and NIS2 with specific laws such as the eTIAS Regulation is complex.

ALSTOM: Points out CRA's continuous vulnerability management conflicts with long-lived rail assets, urging alignment with sector lifecycles.

The CRA, however, requires continuous vulnerability management, including regular security updates and provision of security mitigations by product manufacturers, throughout the products lifecycle.

ACEA (European Automobile Manufacturers' Association): Supports international harmonisation and automotive type-approval as the exclusive path for regulating vehicle AI, seeking to repeal overlapping AI Act articles and align related requirements.

Requirements for AI systems or models should be regulated exclusively through the type- approval framework.

UNIFE: Stresses that rail is a tailor-made industrial B2B sector with long lifespans and complex supply chains, so digital and cybersecurity rules must align with sector characteristics rather than consumer goods models.

While fully committed to EU policy objectives in the digitalisation field, in particular when it comes to the critical topic of cybersecurity, UNIFE - the Association of the European Rail Supply Industry - underlines that certain regulations focus on consumer goods sectors and not on the characteristics of tailor-made industrial goods sectors such as rail (e.g. B2B, public procurement, long project timelines, long lifespan of rail products and assets in operation).

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Warns of double regulation in automotive where UNECE and EU type-approval already cover high-risk AI, calling to avoid overlaps to preserve competitiveness.

Due to the extensive approval requirements set out in Regulation (EU) 2018/858, combined with the diverse technical regulations of the UNECE, all relevant aspects of AI in high-risk applications are already covered in the automotive sector - particularly in the area of autonomous driving and driver assistance systems.

Fédération des Industries Ferroviaires: Calls for rail-specific calibration of digital and cybersecurity rules and standards, avoiding over-regulation and aligning with sector practices and long project timelines.

DigitalTrade4.EU: Advocates sector-tailored updates across battery, fisheries, steel, and automotive policies, including integrating digital product passports and phasing obligations to match industrial realities.

Elia Group: Seeks energy-sector clarity on the AI Act and support for behind-the-meter digital metering and billing, underscoring digitalisation as key to grid and transition goals.

Bayerische Motoren Werke Aktiengesellschaft: Proposes limiting AI Act applicability where automotive type-approval governs and aligning CRA exception timing for L-category vehicles with sector timelines.

VDMA - Advancing Europe´s machinery industry: Requests sector-specific exemptions for maritime equipment and refined scoping for energy and chemical actors to avoid duplicative cybersecurity and compliance burdens.

Mafex – Spanish Railway Association: Asks for rail AI exclusions and exemptions consistent with long lifecycles and bespoke systems to ensure proportional, sector-aligned obligations.

Verband der Automobilindustrie e.V.: Supports harmonised deregulatory access to vehicle data and sector-specific AI regulation for automotive to prevent overlap and fragmentation.

Association des Constructeurs Européens de Motocycles: Seeks exemptions for already certified aviation and marine equipment and inclusion of L-category vehicles in omnibus fixes to align obligations with sector frameworks.

Orgalim - Europe's Technology Industries: Urges excluding articles from chemical sector coverage to align scope with industrial reality and avoid unintended burdens on manufacturers.

Renault Group: Calls to harmonise EU vehicle data rules and align RED III implementation to reduce fragmentation across the automotive sector.

Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA): Opposes harmonised cross-sector AI occupational safety and health standards, preferring flexible, sector-specific approaches.

Free ICT Europe Foundation: Calls for harmonised, enforceable access to repair and maintenance data for the aftermarket to support competition and lifecycle resilience across sectors.

DIGITALEUROPE: Advocates tailored flexibility in industrial system regulation to account for sector-specific constraints and legacy infrastructure.

Enedis: Requests clarification to prevent retroactive smart meter obligations, aligning energy sector rules with existing deployments and investments.

WindEurope: Calls to exempt certified long-lifecycle wind assets from duplicative new requirements, aligning obligations with asset certification and lifespan.

Schaeffler AG: Urges avoiding duplicative CRA obligations for automotive components already covered by sectoral rules to maintain proportionality and efficiency.

1.10.10 Media, Education & Research Adjustments

This category captures calls to fine-tune horizontal digital rules to the realities of media, education, and research, often by preserving legacy sectoral safeguards and clarifying exemptions. Media stakeholders seek clear carve-outs that protect editorial freedom and pluralism, reduce DSA-induced burdens on publishers' editorial forums, and avoid new EMFA ambiguities, including in multi-stakeholder processes. They urge differentiation between gatekeepers and media, preservation and alignment of audience measurement exemptions, and clarification that commercial content is addressed by existing national and self-regulatory advertising frameworks—rather than duplicative EU-level obligations—while allowing nuanced, fit-for-purpose ad rules (including for e-commerce). They also emphasize maintaining established copyright norms and resisting extraterritorial experiments that could upend settled jurisprudence, and caution against policies that constrain journalism monetisation or fail to assess cumulative impacts on media sustainability. Education and research actors argue for simplification and proportionate treatment, extending light-touch regimes to nonprofit research and adopting deregulatory, clarity-first approaches to AI-assisted EdTech. A concrete legacy-financing example illustrates the theme: replacing sector-specific levies (like Spain's RTVE tax on broadband providers) with general-budget funding to avoid distortions, administrative complexity, and asymmetries that undermine competitiveness and the Single Market.

The RTVE levy applied to broadband providers should be repealed, as it is highly asymmetric and unjustified. (Adigital (Asociación Española de la Economía Digital))

Financing of public services like RTVE should not be assigned to a specific sector but ensured through the General State Budget. (Adigital (Asociación Española de la Economía Digital))

The taxation falls on a sector without significant participation in the advertising market, making this tax even more unjustified and asymmetric, as broadband providers do not potentially benefit from the elimination of an advertising channel as other actors might. (Adigital (Asociación Española de la Economía Digital))

These measures not only generate administrative complexity but also result in multiple fiscal burdens on the same transaction, disproportionately penalize broadband providers' business models, and distort competition. (Adigital (Asociación Española de la Economía Digital))

Meta Platforms Ireland Limited: Argues to preserve established copyright jurisprudence and avoid extraterritorial provisions that could complicate media rights management and create legal uncertainty.

Preserve Established Copyright Norms: Avoid creating unnecessary complexity and uncertainty by adding provisions on extraterritoriality that goes against established copyright law and jurisprudence

Adigital (Asociación Española de la Economía Digital): Calls for repeal of Spain's sector-specific RTVE levy on broadband providers, arguing it distorts competition, imposes duplicative burdens, and should be replaced by general-budget funding of public broadcasting.

The RTVE levy applied to broadband providers should be repealed, as it is highly asymmetric and unjustified.

Advertising Information Group: Requests clearer exemptions for commercial communications so advertising-related content is not inadvertently captured by broader media or platform rules.

Sdružení pro internetový rozvoj (SPIR): Urges reliance on existing national advertising regulations rather than introducing overlapping EU-level measures in the media space.

MVFP Medienverband der freien Presse e.V.: Warns that DSA obligations unduly burden publishers' editorial forums and seeks adjustments to protect editorial autonomy and discussion spaces.

Computer & Communications Industry Association (CCIA Europe): Notes that EMFA provisions on media service providers create ambiguity and potential conflicts with platform obligations, calling for clearer delineation and safeguards.

European Publishers Council: Advocates policies that protect editorial independence, enable monetisation of journalism, preserve flexible audience measurement, and assess impacts to sustain a viable media ecosystem.

BioMed Alliance: Asks that simplification measures and exemptions be extended to non-profit research organisations to reduce administrative burden in education and research contexts.

Zentralverband der deutschen Werbewirtschaft (ZAW): Recommends new rules complement existing advertising laws and leverage proven advertising self-regulation instead of duplicating oversight.

Verband Österreichischer Zeitungen (VÖZ): Calls to distinguish gatekeepers from media companies and to streamline recent media regulations to avoid disproportionate burdens on publishers.

Mirakl: Supports nuanced, fit-for-purpose advertising rules for e-commerce marketplaces that reflect the specificities of product ads and seller dynamics.

Esomar: Urges preservation of essential exemptions for audience measurement to support media funding models and research integrity.

Software & Information Industry Association (SIIA): Seeks clearer, lighter-touch rules for AI-assisted educational technologies and broader simplification of education-sector compliance obligations.

VAUNET - German Association of Private Media: Calls to broaden and safeguard media exemptions in the AI Act to protect editorial activities and media freedom.

1.10.11 Miscellaneous

This category captures calls for sector-specific alignment to make compliance practical and consistent. Stakeholders advocate guidance co-developed with relevant communities—complete with FAQs, examples, and domain-tailored instructions—to translate abstract obligations into concrete steps across areas like healthcare, finance, transportation, recruitment, infrastructure, and content regulation. It also surfaces legacy exemptions and carve-outs, emphasizing that exemptions must be transparent, non-discretionary, and carry downstream responsibilities. Proposals include amending sectoral rules for producers, supporting record-keeping exemptions

(e.g., under Omnibus IV), recognizing the digital sector's distinct needs, and advancing digital judicial systems (EUTIR). Some urge pausing sector-specific AI legislation to prevent fragmentation, and suggest exempting public procurement from negotiation requirements to reduce administrative friction.

> *Sector-specific guidance and FAQs with examples, developed in collaboration with relevant stakeholders should be the first step to facilitate compliance.* (Schneider Electric)
>
> *Offer industry-specific guidance (e.g., healthcare, finance, transportation, recruitment, infrastructure, content regulation) that breaks down abstract regulations into practical steps.* (2Dyles Services)
>
> *Offer industry-specific guidance (e.g., healthcare, finance, transportation, recruitment, infrastructure, content regulation) that breaks down abstract regulations into practical steps.* (2Dyles Services)

Schneider Electric: Advocates developing sector-specific guidance and FAQs, co-created with relevant stakeholders, to make compliance more straightforward. Emphasizes practical, example-based support as the first step toward compliance.

> *Sector-specific guidance and FAQs with examples, developed in collaboration with relevant stakeholders should be the first step to facilitate compliance.*

2Dyles Services: Calls for industry-specific guidance that translates abstract regulations into concrete, actionable steps across sectors such as healthcare, finance, transportation, recruitment, infrastructure, and content regulation.

> *Offer industry-specific guidance (e.g., healthcare, finance, transportation, recruitment, infrastructure, content regulation) that breaks down abstract regulations into practical steps.*

American Chamber of Commerce to the EU: Urges delaying or pausing sector-specific AI legislation to avoid premature or fragmented rules. Suggests a cautious approach before layering additional sectoral mandates.

European Law Institute: Stresses that exemptions must be transparent and carry downstream obligations, ensuring accountability along the chain. Clarifies that exemptions do not grant administrative discretion and should be narrowly applied.

DigitalTrade4.EU: Recommends amending sectoral rules to better align producer responsibilities with digital realities. Also highlights that EUTIR is advancing digital judicial systems, signaling cross-sector modernization.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Supports an Omnibus IV exemption from record-keeping obligations, particularly to ease burdens in affected sectors. Frames this as a targeted legacy exemption to reduce administrative load.

Sdružení pro internetový rozvoj (SPIR): Appreciates the policy's focus on the digital sector, endorsing sector-tailored approaches. Sees value in aligning measures with the specific needs of internet and digital services.

Siemens Healthineers AG: Proposes exempting public procurement from negotiation requirements to preserve efficiency and predictability. Seeks a sector-specific carve-out for procurement processes.

1.11 Miscellaneous

A cross-cutting theme is pragmatic, evidence-based governance that balances autonomy, open markets, and tangible public-interest outcomes. In media, sustainable journalism depends on advertising backed by strong marketing, responsible personalization, and fair audience measurement; performance-based affiliate models reinforce post-ad attribution and reward genuine consumer actions. In health, safety, and accessibility, AI shows measurable benefits when rooted in "safety-by-design", clinical integration, and platform risk reduction; stakeholders call for rigorous evaluation, transparency, standards, and cross-sector coordination to protect vulnerable groups and workers. EU digital sovereignty efforts aim to make rules global benchmarks, tighten control over identity and data layers, and modernize energy and network infrastructures, while maintaining interoperable, investable markets and proportionate FDI screening. Business law proposals seek harmonized company regimes, clearer competition procedures, calibrated contract remedies, reduced litigation and overreach, and tax and administrative simplification that shifts accountability directly to businesses; operational

practices emphasize selling products, free demonstrations, simple digital collaboration with freelancers, and navigating sectoral change. Compliance insights converge on coherent, proportionate frameworks aligned across overlapping instruments, feasibility-checked measurements, precise definitions, practical guidance and tools, safeguards against abuse, high-quality data, and right-sized reporting that removes outdated burdens. Across sub-categories, stakeholders favor outcome-oriented rules, credible measurement and attribution, and coordination among regulators, industry, and civil society. The dominant trend is balancing sovereignty and innovation with practical enforcement that sustains media pluralism, health and safety, and competitive markets.

1.11.1 Trade, Infrastructure & Market Sovereignty

This category traces how the EU seeks market sovereignty through digital rulemaking, standard-setting, and control of strategic infrastructures, while remaining integrated in global trade. Key threads include making EU rules de facto global benchmarks, streamlining IPR enforcement at the border, increasing transparency around standard-essential patents, and tightening autonomy in critical identity/data layers (e.g., limits on outsourcing for the EU Digital Identity Wallet). Industrial actors from AI to national sectors endorse "ethical" or "balanced" digital sovereignty, even as others urge clearer, risk-based FDI screening (control-based definitions, funding-participation criteria) to protect security without chilling investment. These moves interact with transatlantic tensions over tariffs and the portrayal of EU digital regulations as anti-competitive taxation, and face political backlash from voices pressing for deregulation or even departure from the EU framework. On infrastructure, stakeholders call for resilient, sustainable systems and pragmatic transition rules. Proposals range from digitally modernizing core regulatory systems (e.g., emissions trading registries) and compensating telecom operators forced to replace high-risk suppliers, to prioritizing grid-supportive approaches over prescriptive performance mandates for data centers. Industry lobbies contest specific energy provisions (e.g., RED III Article 20a(3)) they see as burdensome to competitiveness, while others link infrastructure modernization to broader housing and industrial strategies. Together, the insights reveal a balancing act: assert regulatory and technological autonomy; keep markets interoperable and investable; and adapt trade, energy, and network infrastructure so sovereignty complements, rather than isolates from, global markets.

> *US President Donald Trump, rather than recom- mitting the transatlantic alliance to its joint defence of human rights and rule of law, has instead imposed unjus- tified tariffs and incorrectly framed the EU's digital regu- lation as a form of arbitrary taxation against successful American companies.* ()
>
> *The EU is running like the Soviet Union at the time.* ()
>
> *I no longer believe in this EU that goes directly into the wall.* ()
>
> **:** Criticizes EU digital regulation and trade actions as unfairly targeting American companies, exacerbating transatlantic tensions over market governance.
>
> *US President Donald Trump, rather than recom- mitting the transatlantic alliance to its joint defence of human rights and rule of law, has instead imposed unjus- tified tariffs and incorrectly framed the EU's digital regu- lation as a form of arbitrary taxation against successful American companies.*
>
> **:** Denounces the EU as over-centralized and failing, urging departure from its regulatory environment to pursue freer markets.
>
> *The EU is running like the Soviet Union at the time.*
>
> **DigitalTrade4.EU:** Promotes digital modernization of EU trade and regulatory systems and positions EU rules as global benchmarks. Streamlines IPR customs processes and links infrastructure planning to housing, bolstering market sovereignty.
>
> **Japan Business Council in Europe (JBCE):** Calls for deleting RED III Article 20a(3) to remove constraints perceived as harmful to investment and competitiveness in energy-related infrastructure.
>
> **Confederation of Industry of the Czech Republic:** Proposes a risk criterion tied to funding participation and a control-based definition of foreign investment to safeguard market sovereignty while enabling investment.
>
> **Plateforme de la filière Automobile:** Seeks repeal of RED III Article 20a(3) to reduce burdens on industrial supply chains and support competitive energy infrastructure and markets.

Google: Urges avoiding CAIDA MPS requirements and strengthening support grids to promote resilient digital and energy infrastructure and competitive markets.

Fastweb S.p.A.: Advocates a compensatory mechanism when replacing suppliers to maintain continuity and fairness in critical infrastructure procurement.

EFCA - European Federation of Engineering Consultancy Associations: Emphasizes prioritizing sustainable, resilient infrastructure as essential for competitive markets and long-term economic sovereignty.

Filiera Italia: Promotes a balanced, ethical approach to digital sovereignty that reinforces domestic control while keeping markets competitive.

European Savings and Retail Banking Group: Opposes EUDIW outsourcing contracts to protect banks' operational autonomy and market sovereignty within digital identity infrastructure.

ECIS, European Committee for Interoperable Systems: Seeks publication of SEP withdrawal decisions to ensure transparency, interoperability, and fair competition in digital markets.

Mistral AI: Supports EU digital sovereignty goals, advocating development of homegrown AI capabilities to strengthen strategic autonomy in digital trade.

1.11.2 Corporate Law, Tax & Business Practices

This category synthesizes EU-facing corporate law and business practice reforms: calls to harmonize company law regimes to reduce fragmentation, enable transparent clean corporate vehicles (e.g., EUTIR), strengthen competition law with clearer procedures, rebalance contract termination remedies by accounting for losses, curb excessive litigation, remove extraterritorial copyright overreach, and avoid burdensome structural separation mandates. On tax and administrative policy, stakeholders aim to boost public revenues while simplifying compliance: modernizing payment policies (e.g., CASD) and clarifying who is economically active help target obligations; shifting liability and responsibility directly onto businesses is proposed to reduce administrative burden and sharpen accountability across digital and traditional value chains. Operational insights show how firms implement these norms: prioritizing product sales over demonstrations, offering ancillary demonstrations free and unpaid, and relying on basic electronic tools to collaborate with freelancers for supporting services. Market adaptation challenges, such as resistance to change in the EV sector, illustrate how corporate culture can hinder policy objectives, while industry associations pledge support and engagement.

Vorwerk's primary purpose is selling its branded products, not merely showcasing them. (Vorwerk SE & Co. KG)

This minor, ancillary service is free for customers and unpaid for agents. (Vorwerk SE & Co. KG)

its lack of success in the electric vehicle market is at least partly due to the vehicle manufacturing sector's unwillingness to accept change. (AI & Partners B.V.)

Vorwerk SE & Co. KG: The company frames in-home demonstrations as ancillary, unpaid activities, emphasizing that its core business is selling branded products. It also notes routine use of basic electronic tools to coordinate with freelancers, reflecting standard business practices.

Vorwerk's primary purpose is selling its branded products, not merely showcasing them.

AI & Partners B.V.: It argues that entrenched industry practices and resistance to change have hampered success in the EV market. This highlights how business culture can impede corporate adaptation.

its lack of success in the electric vehicle market is at least partly due to the vehicle manufacturing sector's unwillingness to accept change.

CECE - Committee for European Construction Equipment: Commits to continued support and stakeholder engagement on relevant regulatory and industry matters. This reflects an organizational stance toward responsible corporate practices.

Halle Institute of Economic research (IWH): Proposes reforming CASD payment policy to enhance payment discipline and clarity in corporate transactions. The reform aims to improve the efficiency of business practices.

DigitalTrade4.EU: Supports a harmonized EU company law regime and endorses EUTIR to enable standardized, clean corporate vehicles. These steps aim to simplify cross-border operations and improve corporate transparency.

Confederation of Industry of the Czech Republic: Calls for a narrow definition of 'economically active' to limit obligations to genuinely active entities. This would reduce compliance burdens under corporate and tax rules.

ITI - Information Technology Industry Council: Opposes structural separation mandates as unnecessary and burdensome. It argues such measures would impose heavy costs without clear benefits to business practices.

European Casino Association (ECA): Advocates policies to boost EU tax revenues. This links sector regulation to broader fiscal outcomes.

Digitalexperte: Proposes reducing administrative burden by reallocating liability responsibilities. This shifts compliance incentives while streamlining corporate processes.

Movement for an Open Web: Urges shifting more responsibility onto businesses for compliance and enforcement. The change is framed as improving accountability within corporate practices.

The Center for Countering Digital Hate: Notes that the law is intended to prevent excessive litigation. This shapes corporate legal risk and dispute strategies.

Computer & Communications Industry Association (CCIA Europe): Calls for removing extraterritorial copyright provisions. The aim is to reduce cross-border legal friction for businesses.

ECIS, European Committee for Interoperable Systems: Recommends including losses when calculating termination penalties. This affects contract design and risk allocation in corporate relationships.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Observes that competition law lacks sufficient procedural mechanisms. This gap undermines predictability and effective enforcement for businesses.

1.11.3 Smart Regulation, Evidence & Compliance

This category aggregates calls for smart regulation: rigorously evidence-based, outcome-oriented, proportionate, and coherent across the EU acquis. Stakeholders emphasize robust ex ante and ex post impact assessments that account for indirect effects, avoidance of scope creep and duplicative obligations, and structural simplification over piecemeal tweaks. Proposals include recalibrating frameworks to the pace of technology, aligning overlapping instruments (e.g., GDPR/DMA/DSA/DORA), clarifying remits, and adopting trust-based, future-proof approaches that reduce burdens while preserving core policy objectives. On compliance and enforcement, the insights stress practicality: feasibility checks for measurements, clear scoping and definitions, flexible illustrative lists, and concrete guidance, examples, and tools. Companies advocate leveraging existing enforcement mechanisms, inserting safeguards (fairness, abuse-of-rights, due process), and using high-quality, trusted data (e.g., for due diligence and nature credits) to improve outcomes. Early gap analysis, comprehensive overviews of obligations, and right-sized reporting (e.g., provide documentation on request) can cut costs and legal uncertainty; mandates should rest on solid evidence, not be extended without justification, and outdated burdens should be removed.

> *The lesson from this example is that the EU digital acquis-including the GDPR, but also asymmetric regulations like the DMA and the DSA-need to be subjected to careful analysis of their negative indirect effects.* (The International Center for Law & Economics)

The impact assessment behind the DMA can serve as a case study of poor analysis of indirect effects, where positive indirect effects were assumed without robust analysis, while negative indirect effects were ignored. (The International Center for Law & Economics)

The impact assessment behind the DMA can serve as a case study of poor analysis of indirect effects, where positive indirect effects were assumed without robust analysis, while negative indirect effects were ignored. (The International Center for Law & Economics)

The lesson from this example is that the EU digital acquis-including the GDPR, but also asymmetric regulations like the DMA and the DSA-need to be subjected to careful analysis of their negative indirect effects. (The International Center for Law & Economics)

The International Center for Law & Economics: Critiques the DMA's impact assessment and urges rigorous analysis of negative indirect effects to ensure evidence-based, proportionate regulation.

The impact assessment behind the DMA can serve as a case study of poor analysis of indirect effects, where positive indirect effects were assumed without robust analysis, while negative indirect effects were ignored.

Adigital (Asociación Española de la Economía Digital): Puts forward constructive, solution-oriented proposals to simplify and improve regulatory compliance while preserving policy goals.

The recommendations in this report provide constructive and solution-oriented proposals for adaptation and improvement

American Chamber of Commerce to the EU: Warns that EU compliance burdens are escalating and calls for streamlined, evidence-based rules to restore predictability.

CECE - Committee for European Construction Equipment: Urges regulators to factor industry priorities and practical feasibility into compliance requirements.

: Welcomes the simplification initiative to reduce red tape without undermining regulatory objectives.

iProov Ltd: Highlights procedural flaws that create legal uncertainty and calls for clearer, more reliable compliance processes.

European Law Institute: Supports an illustrative list approach with flexible updates to keep compliance clear and adaptable.

DigitalTrade4.EU: Advocates trusted data for due diligence, high-integrity nature credits, and integrating advanced frameworks to make compliance efficient and credible.

Bayerische Motoren Werke Aktiengesellschaft: Opposes demonstration obligations absent a recipient's request and argues existing enforcement tools are sufficient.

VDMA - Advancing Europe´s machinery industry: Calls for feasibility checks on measurement obligations and justification for deviations from core legal principles.

Japan Business Council in Europe (JBCE): Flags inconsistencies between Articles 4 and 9 that risk creating compliance uncertainty.

BusinessEurope: Prioritizes structural regulatory fixes over incremental tweaks to achieve clarity and reduce burdens.

Federation of Austrian Industries: Urges removal of outdated regulatory burdens to cut costs and streamline compliance.

U.S. Chamber of Commerce: Says smart-regulation principles are not fully reflected in current rules and seeks alignment with evidence and outcomes.

: Views current regulation as overly strict and calls for proportionate, workable compliance obligations.

Confederation of Norwegian Enterprise (NHO): Calls for structural reforms to simplify compliance rather than piecemeal adjustments.

CENTR - Council of European Top Level Domain Registries: Warns DORA creates unintended consequences and questions the appropriateness of financial oversight in certain domains.

ITI - Information Technology Industry Council: Requests clearer scoping of related services to ensure practical and predictable compliance.

REIF: Commits to applying EU rules and seeks clarity to facilitate effective implementation.

Verband der Automobilindustrie e.V.: Proposes safeguards against abuse of rights to keep enforcement and compliance proportionate.

Association des Constructeurs Européens de Motocycles: Argues existing mechanisms are sufficient and strongly supports deregulation to reduce burdens.

Sdružení pro internetový rozvoj (SPIR): Criticizes unrelated or unreasoned authority orders, urges fairness safeguards, and suggests deleting Article 21.

Google: Advocates a coherent, trust-based regulatory framework that aligns compliance with outcomes.

MVFP Medienverband der freien Presse e.V.: Supports the simplification objectives to ease compliance while maintaining policy intent.

Forvis Mazars: Calls for practical, effective compliance measures and guidance that work in real-world settings.

secunet Security Networks AG: Welcomes the Omnibus Package as a chance to craft balanced, coherent, future-proof regulation.

International Information System Security Certification Consortium, Inc.: Emphasizes improved data quality to strengthen insight and evidence-based regulation.

CSC - IT Centre for Science: Calls for careful impact assessments and better analytical tools to guide smart regulation.

Business Software Alliance: Urges regulation to keep pace with technological change and support adaptive, interoperable compliance.

Bocconi University: Seeks efficiency anchored in constitutional principles, endorsing a dual-basis, rule-of-law approach to compliance.

Seznam.cz, a.s.: Requests safeguards to ensure fairness and prevent arbitrary or excessive compliance demands.

Renault Group: Urges removal of Article 20a's second paragraph to avoid unnecessary administrative burdens.

Cigref: Calls for practical examples and use cases to clarify expectations and support compliance.

RECHARGE - The Advanced Rechargeable & Lithium Batteries Association: Assesses the current framework as not fit for purpose and seeks targeted revisions for workable compliance.

Insurance Europe: Emphasizes clear, proportionate compliance standards tailored to the insurance sector.

CIO Platform Nederland: Requests a comprehensive overview of legislation to manage overlapping obligations efficiently.

European Entrepreneurs CEA-PME: Wants rules written as clear instruction manuals to help SMEs comply without excessive cost.

noyb: Proposes a concrete legal standard and adoption mechanism to harmonize compliance across the EU.

Computer & Communications Industry Association (CCIA Europe): Calls for fundamental structural reforms to fix past mistakes, enhance clarity, and future-proof regulation.

Hugging Face: Urges making the Fitness Check a practical resource that guides implementers and improves compliance.

Palo Alto Networks: Recommends outcome-oriented, risk-based policies to streamline compliance and improve security results.

European Savings and Retail Banking Group: Calls for impact assessments before EU-wide systems, workable rules, early gap analyses, and adequate resourcing.

SAP SE: Advocates a simple-as-possible approach and a recalibrated framework to eliminate overlaps.

Danish Industry: Reports significant burdens on Danish companies and calls for simplification and predictability.

Data & Technology for Compliance Alliance: Highlights unintended regulatory consequences and seeks data-driven, corrective adjustments.

Zentralverband Deutsches Baugewerbe: Offers industry support to the Commission to co-develop pragmatic compliance pathways.

Alliance Digitale: Proposes changes that deliver direct compliance benefits while maintaining policy objectives.

: Prioritizes technical simplifications over policy shifts to reduce risk and complexity.

European DIGITAL SME Alliance: Conditionally supports simplification that protects SMEs and preserves fair competition.

DIGITALEUROPE: Provides practical burden-reduction proposals, questions weak evidence behind some mandates, and urges not extending the final report.

Verband Österreichischer Zeitungen (VÖZ): Backs deregulation goals to lower compliance overhead for publishers.

STM: Encourages practical compliance tools and templates to aid implementation.

Indeed: Emphasizes effective, consistent implementation over adding new rules.

Esomar: Supports an approach that improves legal certainty and data protection through clearer guidance.

Council of European Municipalities and Regions (CEMR): Urges anticipating compliance aspects in future strategies to avoid burdens on municipalities and regions.

Too Good To Go: Suggests providing documentation on request to reduce unnecessary reporting burdens.

APPLiA (Home Appliance Europe): Rejects mischaracterizing opt-out conformity and seeks clarity to prevent compliance confusion.

1.11.4 Advertising, Marketing & Media Pluralism

Advertising, marketing, and audience measurement are foundational to funding digital content and sustaining media pluralism. Publishers increasingly rely on advertising to finance journalism's democratic role; when ad investments fall, publishers' resources shrink and pluralism is threatened. Stakeholders stress that marketing is essential for creating advertising value, and that contextual ads alone are often insufficient—responsible personalization can improve user experience and unlock the higher-yield revenue many publishers need. Robust, fair audience measurement is critical; biases and data gaps skew representativeness and undermine sustainable markets. Affiliate marketing exemplifies a performance-based, attribution-driven model that ties spend to real outcomes. Operating primarily on a cost-per-acquisition basis, it relies on accurate attribution and network infrastructure to reconcile referrals with transactions and pay commissions. Because revenue only occurs after genuine consumer actions, the model incentivizes helpful services and is relatively resistant to misleading tactics. Despite these benefits and its role as post-ad measurement, affiliate marketing is frequently overlooked in discussions dominated by programmatic and contextual advertising.

I am in favour of advertising because it enables sites to generate revenue and thus offer content. ()

Affiliate marketing is often monetised on a cost-per-acquisition, or "CPA", basis. (Sheridans, on behalf of Awin AG)

Despite its name, affiliate marketing is therefore more accurately described as a form of advertising measurement. (Sheridans, on behalf of Awin AG)

It is very difficult to generate CPA revenue by misleading or confusing consumers into acting against their own interests. (Sheridans, on behalf of Awin AG)

Sheridans, on behalf of Awin AG: Explains affiliate marketing's CPA monetisation and attribution-driven commission model, positioning it as a post-ad engagement measurement system that incentivises consumer-beneficial services.

Despite its name, affiliate marketing is therefore more accurately described as a form of advertising measurement.

: Supports advertising as essential for enabling websites to generate revenue and offer content.

I am in favour of advertising because it enables sites to generate revenue and thus offer content.

SIA Tet: Expresses support for media diversity and pluralism.

Fedoweb - Federazione Operatori Web: Warns that reduced advertising investment is shrinking publishers' resources, posing a threat to media pluralism and the quality of information.

Movement for an Open Web: Argues that personalized advertising improves user experience by making content and offers more relevant.

German Newspaper Publishers and Digitalpublishers Association (BDZV): Contends that contextual ads are insufficient and that publishers need personalized advertising revenues to sustain their businesses.

Audience Measurement Coalition (AMC): Promotes audience measurement that upholds media pluralism, fairness, and sustainability, noting that current distortions skew representativeness and impede accurate measurement.

European Publishers Council: Highlights publishers' growing reliance on advertising and the vital role of marketing in creating advertising value, while recognising journalism's democratic role.

DIGITALEUROPE: Calls to maintain copyright exceptions during delays, impacting content availability and monetisation.

1.11.5 AI, Public Health & Safety Standards

AI in public health and safety standards is portrayed as a tool for inclusion, risk reduction, and efficiency across healthcare, occupational safety, disability rights, digital platforms, and biosecurity. Stakeholders highlight AI's capacity to improve accessibility for persons with disabilities, support mental health, foster fairness and inclusion, enhance clinician–patient engagement, and deliver measurable safety benefits in consumer platforms. In health technology, a history of safe AI-enabled devices underscores the importance of safety-by-design and clinical integration, while in plant health regulation AI contributes to modernized, proactive pest monitoring and control. Yet, there is a parallel emphasis on governance and evidence. With limited empirical data on the impacts of the AI Act, stakeholders call for rigorous evaluation, transparency, and standard-setting to ensure AI aligns with public interest, protects vulnerable groups, and upholds occupational and public safety. Cross-sector coordination—linking healthcare, safety professionals, disability advocates, and regulators—is presented as essential to translate AI's promise into trustworthy, equitable practice.

> *These new technologies can be of enormous benefit to persons with disabilities and drive the search for inclusive equality across a broad range of fields such as employment, education and independent living.* (European Disability Forum)

> *These new technologies can be of enormous benefit to persons with disabilities and drive the search for inclusive equality across a broad range of fields such as employment, education and independent living.* (European Disability Forum)

European Disability Forum: The European Disability Forum underscores AI's potential to advance disability inclusion across employment, education, and independent living, reinforcing equitable access as a public interest objective.

These new technologies can be of enormous benefit to persons with disabilities and drive the search for inclusive equality across a broad range of fields such as employment, education and independent living.

ENSHPO - The European Network of Safety and Health Professional Organizations: ENSHPO notes that AI can support mental health and promote inclusion and fairness in occupational safety and health, contributing to safer, more equitable workplaces.

DigitalTrade4.EU: DigitalTrade4.EU advocates modernizing plant pest regulatory frameworks, leveraging contemporary data-driven tools to strengthen biosecurity and public health safeguards.

Meetic Group, a Match Group Company: Meetic reports tangible safety gains from AI-driven safety tools, indicating measurable improvements in user protection and harm prevention.

Siemens Healthineers AG: Siemens Healthineers points to a track record of safe AI-enabled medical devices, aligning with clinical standards and demonstrating reliable, regulated deployment.

BioMed Alliance: BioMed Alliance highlights that AI-enabled solutions can streamline clinician–patient engagement, improving efficiency while supporting care quality and safety.

Ada Lovelace Institute: The Ada Lovelace Institute flags a lack of evidence on the real-world impacts of the AI Act, calling for robust evaluation to ensure public interest and safety outcomes.

2 Criticism of deregulation

The clearest lesson is that blanket deregulation erodes trust, safety, and competitiveness; durable progress needs a rights-first, risk-proportionate, coherent regime with independent enforcement. Enforceable safeguards for AI and data (privacy, non-discrimination, opt-out with human review) and rigorous fundamental-rights impact assessments should be non-regressive. Legal certainty comes from EU-wide alignment of scope, definitions, timelines, and certification, with uniform implementation and predictable transitions. Enforcement must be well resourced and independent, with clear powers, cross-border coordination, transparency, and redress. Privacy-by-default should curb tracking with device-level controls, consent integrity, and limits on profiling-based adtech. Incident reporting should be harmonized, risk-based, and confidential across NIS2, DORA, GDPR, PSD2, and the CRA, reusing standards. AI governance should be lifecycle-based: precise high-risk scoping, transparency and provenance, robustness and human oversight, post-market monitoring, and upstream GPAI accountability. Data sharing needs interoperable access and portability with trade-secret safeguards, trusted data spaces, lawful transfers, and sovereign capacity. Competition and media require disciplining gatekeepers via interoperability, device neutrality, fair data access, and privacy-respecting measurement. SMEs need proportionate duties, single

gateways, upstream liability, and practical support, not carve-outs. Sectors like health, work, accessibility, environment, and critical infrastructure demand safety-by-design, continuous oversight, and inclusion. Policy should be evidence-based, participatory, execution-focused, with targeted simplification that preserves certainty. Digital identity should be tech-neutral, with testable security and interoperability, clear roles and liability, and user-controlled wallets. Across sub-categories, the dominant pattern is harmonization, proportionality, interoperability, and enforceability that reduce friction while preserving rights. The shared trend is simplifying execution without weakening protections, aligning innovation with accountability.

2.1 Protect Fundamental Rights and Safeguards

The strongest insight is that enforceable, participatory rights safeguards—privacy, non-discrimination, opt-out with human review, and robust impact assessment—are prerequisites for trustworthy AI and sustainable innovation. Equality and inclusion mean embedding CRPD standards throughout design, deployment, and oversight, with co-design and representation to prevent proxy bias in hiring and gendered harms like deepfakes. Privacy, data protection, and IP must hold end-to-end: GDPR/ePrivacy alignment, user control, narrowly tailored and transparent state exceptions with notice, proportionate measures that respect confidentiality, and lawful training data with accountability. Fair automated decision-making requires explicit rights to opt out, challenge materially adverse outcomes, receive meaningful explanations, and access complaints and appeals; strengthen worker protections, use disaggregated data, and be cautious in judicial use. Accountability depends on rigorous Fundamental Rights Impact Assessments with standard triggers and templates, alignment with GDPR and EDPB guidance, concrete mitigation and redress, independent oversight, transparency, publication, and participation by NHRIs, civil society, and representative disability groups, kept distinct from safety reviews. A non-regression principle guards against simplification that dilutes obligations; prioritize guidance, interoperability, and enforcement over rollbacks. Across sub-categories, a rights-first, high-risk-focused, non-regressive approach couples transparency, accountability, and participation to build trust and legitimacy. The shared trend is aligning competitiveness with democratic oversight so protections drive reliable innovation.

2.1.1 Rights-Centered Innovation & Democracy

This category contends that fundamental rights, democratic values, and safety-by-design are the foundation—not a brake—on sustainable innovation. The EU's comprehensive digital rulebook (spanning privacy, product safety, cybersecurity, and fair competition) is presented as a rights-centered template that elevates health, security, and wellbeing, builds public trust, and has influenced global standards beyond Europe. Strong accountability and human-centric design are seen as essential to make data-driven innovation reliable, safe, and socially beneficial. Contributors urge maintaining and improving safeguards rather than deregulating: align AI and digital governance with democracy, inclusivity, and European values; target rules to high-risk or overhyped tools with unproven reliability and heavy copyright or privacy implications; and streamline processes within a protected "safe space." They warn that illiberal or monopolistic pressures erode autonomy, resilience, and freedom, arguing for a calibrated balance where competitiveness is advanced by protections and technology is shaped by democratic oversight, not vice versa.

> *Instead of dismantling the EU's digital safeguards, the Commission should recognize that robust protection of fundamental rights and democratic values is not a burden but a foundation for sustainable innovation and public trust.* (Civil Liberties Union for Europe)
>
> *Together with the GDPR, the e-Privacy Regulation shall bring tangible benefits to consumers and help ensure that data- driven innovation and the Digital Single Market thrive in a way that is respectful of citizens' fundamental rights and freedoms.* (BEUC - The European Consumer Organisation)
>
> *Unless Europe creates a regulatory framework that moves away from illiberal influence, there can be no real growth in Europe, as all processes in a globalised economy will ultimately be weakened to comply with the monopolists and autocrats in these illiberal nations.* ()
>
> *Parts of it have thus become a template for other governments in emerging markets, while multinational companies have adopted EU laws on data privacy, cybersecurity, pro- duct safety as their global standard, benefiting countless people who have never set foot on European soil.* ()
>
> **:** Argues EU institutions should prioritize citizens' wellbeing through a comprehensive digital rulebook that protects privacy, safety, and fair competition. Warns against unreliable, overhyped tools with copyright and data privacy risks.
>
> *Its digital rulebook is the most comprehensive effort globally to protect privacy and other human rights, raise product safety standards, and ensure fair competition in the digital economy.*

Civil Liberties Union for Europe: Contends that robust rights and democratic safeguards underpin sustainable innovation, public trust, and societal resilience. Asserts EU's global tech governance credibility depends on upholding these principles over short-term pressures.

Instead of dismantling the EU's digital safeguards, the Commission should recognize that robust protection of fundamental rights and democratic values is not a burden but a foundation for sustainable innovation and public trust.

BEUC - The European Consumer Organisation: Maintains that data-driven innovation can thrive while respecting fundamental rights through instruments like GDPR and e-Privacy. Emphasizes coexistence of consumer protection and the Digital Single Market.

Together with the GDPR, the e-Privacy Regulation shall bring tangible benefits to consumers and help ensure that data- driven innovation and the Digital Single Market thrive in a way that is respectful of citizens' fundamental rights and freedoms.

: Insists the EU must resist illiberal influence to protect liberal democracy and enable genuine growth. Supports simplifying business processes within a rights-safe framework.

Unless Europe creates a regulatory framework that moves away from illiberal influence, there can be no real growth in Europe, as all processes in a globalised economy will ultimately be weakened to comply with the monopolists and autocrats in these illiberal nations.

European Partnership for Democracy: Urges aligning technology regulation with democratic principles and fundamental rights to steer innovation responsibly. Highlights the need for accountability and participation.

Pour Demain Europe: Encourages the EU to continue a human-centric regulatory trajectory that embeds rights into innovation policy. Stresses maintaining momentum toward rights-centered governance.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Notes that democratic governance can shape inclusive AI ethics and innovation rooted in fundamental rights and societal values. Promotes participation and fairness.

IDRS Platform: Emphasizes compliance frameworks that uphold European autonomy and values while enabling responsible innovation. Links adherence to standards with trust and legitimacy.

European Public Service Union: Argues technology should be governed by democratic, rights-based values to serve the public interest and workers. Calls for safeguards in deployment and oversight.

Danish Society of Engineers (IDA): Prioritizes protection of fundamental rights over short-term competitiveness as a basis for sustainable innovation. Advocates for rights-first policy choices in tech.

Digitalexperte: Warns that deregulation and excessive corporate influence threaten democracy and freedom. Calls for rights-centered safeguards to protect society.

Connect Europe: Calls for balanced policies that uphold fundamental rights while fostering innovation across the digital economy. Seeks pragmatic approaches that preserve trust.

: Advocates policymaking that respects EU values, engages stakeholders, and embeds rights-centric considerations in innovation strategies. Supports inclusive, transparent processes.

2.1.2 Non-Regression & Regulatory Safeguards

This category articulates a non-regression principle for EU digital policy: regulatory simplification must neither dilute nor defer existing protections for fundamental rights, privacy, transparency, accountability, and consumer safety. Stakeholders across civil society, human rights bodies, consumer groups, and parts of industry endorse streamlining compliance and clarifying overlaps only if safeguards remain intact, explicitly rejecting deregulation-by-stealth, watered-down definitions, widened exemptions, or reduced checks on high-risk systems and automated decisions. Contributors warn that omnibus simplification initiatives risk reopening recently adopted frameworks (GDPR, DSA, AI Act), undermining hard-won minimum protections, legal certainty, and

public trust. They call for a rights-first approach: preserve core obligations, strengthen enforcement, avoid premature changes before evidence of undue burden, and prioritize guidance and interoperability over legislative rollbacks. Proposed safeguards include embedding non-regression clauses, maintaining transparency and meaningful consent, and ensuring accountability for automated decisions so competitiveness is pursued without eroding EU values or protections.

> *However, we would like to emphasize that any simplification of the regulatory landscape must not impact the individuals' fundamental rights and freedoms.* (Enel SpA)
>
> *Simplification efforts should never lead to deregulation.* (Centre for Democracy and Technology Europe)
>
> *Such an approach risks undoing years of progress achieved through landmark EU legislation such as the GDPR, the DSA, and the AI Act.* (Civil Liberties Union for Europe)
>
> *Given that the AI Acts early stage of implementation, we furthermore call upon the Commission to not simplify obligations of providers and deployers in the absence of clear, verifiable and transparent evidence of the laws negative implications on innovation and the compliance burden for companies.* (Centre for Democracy and Technology Europe)

Enel SpA: Warns that regulatory simplification must not erode individuals' fundamental rights and freedoms. Calls for safeguards to preserve rights while streamlining rules.

> *However, we would like to emphasize that any simplification of the regulatory landscape must not impact the individuals' fundamental rights and freedoms.*

Amazon: Supports reducing administrative burden while insisting that consumer safeguards remain intact. Emphasizes a balanced approach that keeps robust protection alongside efficiency.

> *While reducing administrative burden is essential, it should not come at the cost of consumer safeguards.*

Civil Liberties Union for Europe: Argues that the Digital Omnibus risks turning simplification into deregulation that weakens fundamental rights and EU values. Warns of diluted standards, widened loopholes, and threats to protections in the AI Act and other laws.

> *In short, we worry that the simplification process will instead become a deregulation process.*

Centre for Democracy and Technology Europe: Opposes any simplification of the AI Act that jeopardizes fundamental rights or amounts to deregulation. Stresses obligations are minimal yet essential and must be preserved and enforced rather than watered down.

> *Simplification efforts should never lead to deregulation.*

BEUC - The European Consumer Organisation: Urges against reopening recently adopted digital laws, warning that even targeted changes can undermine fundamental rights and accountability. Notes that many measures are too new to evaluate and weakening them would harm trust and legal certainty.

> *gainst this backdrop, even "targeted changes"9 to the digital rulebook could have counterproductive consequences contrary to the spirit of the legislation, rolling back fundamental rights, sending the wrong signal about Europe's commitment to rights-respecting tech governance, and undermining legal certainty.*

Akava: Advocates preserving core regulatory principles, including consumer, occupational safety, and privacy protections. Rejects ideological deregulation in the name of simplification.

> *the basic principles of the regulations and, for example, consumer and occupational safety and privacy protection should be preserved and it must not be a question of ideological "deregulation",*

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Supports simplification that removes irrelevant provisions without reducing the rights of individuals or transparency of AI systems. Calls for streamlining that does not compromise fundamental rights.

This simplification however cannot be reached by reducing the rights of natural persons or any other rights that could be infringed by using AI but must be achieved by reducing irrelevant regulating parts that do not touch the transparency of AI systems.

: Asserts that simplification should not equate to deregulation and that citizens' rights must be safeguarded. Emphasizes transparency, meaningful consent, and accountability to keep protections strong.

Simplification should not mean deregulation.

Health Action International: Calls for safeguarding fundamental rights and protections in health contexts amid deregulatory pressures. Warns that simplification should not weaken patient safety, privacy, or accountability.

European Law Institute: Notes alignment with consumer contract protections and the need for exceptional tasks to protect rights. Emphasizes that simplification should respect and reinforce these safeguards.

DigitalTrade4.EU: Claims that streamlining through the EUTIR can enhance consumer protection and trust. Stresses that simplification should bolster, not reduce, safeguards.

: Warns that deregulation undermines protections and fundamental rights. Urges maintaining strong non-regression safeguards during reform.

European Public Service Union: Argues the Omnibus risks undermining protections and safety for workers and the public. Calls for maintaining robust rights and safeguards against dilution.

U.Di.Con. APS UNIONE PER LA DIFESA DEI CONSUMATORI: Supports simplification that preserves strong consumer protection. Emphasizes maintaining safeguards while reducing complexity.

Brighten Digital: Urges avoiding any reduction of safeguards during simplification. Calls for rights-preserving reforms.

Federation of German Consumer Organisations (vzbv): States that simplification must not lead to deregulation and should protect fundamental and consumer rights. Warns that some proposed reforms risk undermining these protections.

University of Amsterdam: Cautions that premature simplification can undermine protections and legal coherence. Advocates evidence-based adjustments that preserve rights.

European Casino Association (ECA): Opposes Omnibus measures that would weaken digital rules and protections. Calls for retaining strong safeguards while improving clarity.

Verband der Automobilindustrie e.V.: Supports avoiding any lowering of protection standards in simplification efforts. Emphasizes non-regression in safety and rights.

European Broadcasting Union: Advocates upholding fundamental rights protections throughout digital reforms. Warns against weakening safeguards under the banner of simplification.

ENNHRI - European Network of National Human Rights Institutions: Insists on maintaining fundamental rights safeguards and warns that lowering protections harms EU credibility. Urges non-regression as a core principle of simplification.

WITNESS: Calls for protecting fundamental rights and consumers in digital governance. Opposes simplification that dilutes accountability and safeguards.

Corporate Europe Observatory: Warns that lobby-driven deregulation would erode rights and standards. Urges shielding core protections from industry pressure.

Danish Institute for Human Rights: Stresses the need to maintain critical safeguards for fundamental rights in any simplification. Opposes weakening enforcement or standards.

AlgorithmWatch: Argues that deregulation would undermine EU protections and accountability for algorithmic systems. Supports non-regression and strong oversight.

Homo Digitalis: Warns that digital simplification risks undermining protections and weakening EU safeguards. Criticizes attempts to dilute rights in the name of competitiveness.

Bocconi University: Recommends embedding a non-regression clause and other safeguards to ensure efficiency without harming rights. Advocates rights-proof mechanisms alongside streamlining.

ACT | The App Association: Supports simplification accompanied by clear safeguards to protect users and rights. Encourages balance between reducing burdens and maintaining protections.

Chair in Cyber Policy, University of Luxembourg: Opposes deregulation and weakening of safeguards under the Omnibus. Calls for protecting rights as a prerequisite to any simplification.

European Digital Rights (EDRi): Warns that so-called simplification amounts to deregulation that undermines protections, while highlighting how the AI Act can reinforce rights and compliance. Urges preserving and implementing existing safeguards.

Eurosmart: Emphasizes the need to safeguard fundamental rights within digital policy updates. Supports simplification only if protections remain intact.

AI Accountability Lab (AIAL), Trinity College Dublin: Argues that tech deregulation threatens fundamental rights and that simplification must be rights-first. Warns that repeated deregulatory pushes dilute protections and create cascading risks.

Access Now Europe: States that simplification and cost-cutting measures undermine core rights and protections. Warns the Omnibus deregulation agenda threatens essential safeguards.

2.1.3 Accountability, Oversight & Rights Impact Assessments

This category centers on making accountability real through robust, enforceable Fundamental Rights Impact Assessments (FRIAs) and coordinated oversight across the digital and AI rulebook. It calls for standardized triggers, templates, and crosswalks that align FRIA duties with GDPR practice, EDPB high-risk criteria, Charter proportionality and strict-necessity tests, and Article 27 obligations, supported by coherent European Commission and EDPB guidance. Assessments should evaluate concrete consequences, necessity, and proportionality; plan safeguards, mitigation, and effective redress; and remain distinct from safety and security assessments. Independent oversight, transparency, documentation, and auditability are essential to ensure compliance and remedies. Process integrity and participation are central: FRIAs should be transparent and involve rights expertise from NHRIs, civil society, and affected communities, with specific inclusion and leadership of representative organisations of persons with disabilities in line with the CRPD. Proposals include Human Dignity Impact Assessments and stronger publication and consultation duties. The insights warn against deregulation, exemptions, and rushed, box-ticking consultations that downplay rights impacts, and insist on rights-respecting deployment backed by enforceable safeguards and accountability mechanisms.

> *In order to do so, the Commission needs to not only keep them, but to involve civil society in formalizing a template for FRIAs that is stringent enough to fulfill the objective assessments' objective of protecting fundamental rights.* (Civil Liberties Union for Europe)

> *In this context, the European Commission can and should play a vital role in providing guidance on the interplay between different obligations under the aim of ensuring the protection of fundamental rights.* (Centre for Democracy and Technology Europe)

> *Such a brief period for review strongly suggests that this call for evidence is little more than a box-ticking exercise in the guise of a proper consultation.* (Civil Liberties Union for Europe)

> *It is now just less than two months until the Digital Omnibus proposal is scheduled, giving decision-makers little time to properly consider the arguments and warnings from civil society organizations,*

individual experts and others who flag significant threats to fundamental rights. (Civil Liberties Union for Europe)

Civil Liberties Union for Europe: Criticises a rushed consultation that downplays fundamental rights risks and urges involving civil society to co-design stringent Fundamental Rights Impact Assessments to ensure accountability.

In order to do so, the Commission needs to not only keep them, but to involve civil society in formalizing a template for FRIAs that is stringent enough to fulfill the objective assessments' objective of protecting fundamental rights.

Centre for Democracy and Technology Europe: Calls for the European Commission to provide guidance on how obligations interact to safeguard fundamental rights, referencing EDPB criteria for identifying high-risk processing to structure oversight and assessments.

In this context, the European Commission can and should play a vital role in providing guidance on the interplay between different obligations under the aim of ensuring the protection of fundamental rights.

CERMI: Demands a disability-focused rights check that systematically tests EU digital rules against the CRPD, with direct participation and leadership of representative organisations of persons with disabilities to ensure accountable assessments.

This check-up must explicitly and systematically assess how the EUs digital regulatory framework impacts the rights of pWd as enshrined in the CRPD.

Bündnis F5: AlgorithmWatch, Gesellschaft für Freiheitsrechte, Open Knowledge Foundation, Reporter ohne Grenzen, Wikimedia Deutschland: Advocates prioritising systematic checks and oversight mechanisms to protect fundamental rights in digital governance, embedding accountability through rigorous assessments.

European Law Institute: Urges application of a strict necessity and proportionality test by courts and policymakers, with explicit consideration of consequences and safeguards in rights impact assessments.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Questions the adequacy of current rights assessments and warns that broad exemptions undermine accountability, calling for stronger oversight and clearer limits.

Nordic Financial Unions - the Nordic financial trade unions confederation: Proposes Human Dignity Impact Assessments alongside fundamental rights impact assessments to safeguard workers and consumers, strengthening accountability through social dialogue and oversight.

Inter IKEA Group: Calls for standardized triggers and a crosswalk for fundamental rights impact assessments across legal regimes to streamline compliance while preserving accountability and rights protections.

Federation of German Consumer Organisations (vzbv): Supports mandatory fundamental rights impact assessments for relevant systems, backed by enforceable oversight to ensure consumer protections.

ENNHRI - European Network of National Human Rights Institutions: Urges preservation of Article 27's FRIA requirements and transparent consultations that include human rights expertise and NHRIs to reinforce accountability.

Public Defender of Rights: Advocates robust fundamental rights impact assessments and deployment practices that respect rights, with monitoring and redress mechanisms to ensure accountable use.

Danish Institute for Human Rights: Highlights that human rights risk management differs from safety or security risk approaches and requires tailored oversight, accountability, and assessment methods.

Bocconi University: Calls for enforceable FRIAs with oversight guarantees and explicit Charter-based proportionality and necessity checks to anchor accountability in law.

European Digital Rights (EDRi): Warns that policymakers downplay rights impacts and urges strong safeguards, accountability measures, and binding FRIA obligations.

European Network Against Racism (ENAR): Flags growing rights threats, especially racial discrimination, and calls for accountability and community-centered rights impact assessments.

AI Accountability Lab (AIAL), Trinity College Dublin: Critiques deregulation for lacking rigorous rights impact assessment and independent oversight, increasing risks to fundamental rights.

Access Now Europe: Advocates comprehensive FRIA duties, transparency, and independent oversight to effectively protect fundamental rights.

APPLiA (Home Appliance Europe): Calls to clearly separate safety, security, and fundamental rights obligations to avoid duplicative assessments while maintaining accountability.

2.1.4 Fair Automated Decision-Making & Redress

Fair Automated Decision-Making & Redress centers on tangible, enforceable rights that let people avoid or contest automated outcomes, obtain meaningful explanations, and access effective complaint and appeal pathways. Stakeholders call for an opt-out from automated decision-making (e.g., under GDPR Art. 22), an explicit right to challenge materially adverse automated decisions, and protection of explanation rights, shifting the AI governance model from mere disclosure to outcome-oriented accountability and access to justice. In the workplace, they seek to extend regulation of algorithmic management, empower workers beyond transparency alone, and address gaps in the Platform Work Directive by creating positive rights and remedies. Fairness also requires strong anti-discrimination safeguards, including preventing algorithmic bias—especially against persons with disabilities—through better disaggregated data and an expanded scope of sensitive characteristics. Simplification of rules must not dilute these protections, and the use of AI in the judiciary warrants particular caution to avoid miscarriages of justice. Overall, the category consolidates demands for opt-out and human review, robust challenge and complaint mechanisms, meaningful explanations, worker protections, and proportionate, rights-based redress.

Enable an opt-out model in Article 22 regarding automated decision-making (i.e., data subjects should have the right to refuse automated decisions). (DigiFinland)

Notably, it does not explicitly provide a right to challenge automated decisions with material adverse effects. (Unipol Assicurazioni S.p.A.)

A more outcome-oriented and proportionate approach, focused on tangible rights, would have been preferable for a Level-1 framework, fostering innovation while ensuring accountability. (Unipol Assicurazioni S.p.A.)

The lack of disaggregated data on persons with disabilities renders them invisible to these systems, resulting in exclusionary outcomes. (CERMI)

DigiFinland: Advocates an opt-out right under Article 22 regarding automated decision-making, allowing individuals to refuse automated decisions. Positions this opt-out as a safeguard for fairness and redress in AI-driven outcomes.

Enable an opt-out model in Article 22 regarding automated decision-making (i.e., data subjects should have the right to refuse automated decisions).

Unipol Assicurazioni S.p.A.: Criticizes the AI Act for prioritizing procedural compliance over enforceable, outcome-oriented rights and for lacking an explicit right to challenge harmful automated decisions. Calls for tangible rights that ensure accountability and effective redress.

Notably, it does not explicitly provide a right to challenge automated decisions with material adverse effects.

CERMI: Warns that AI may perpetuate discrimination against persons with disabilities and urges stronger safeguards, including better data practices. Stresses that regulatory simplification must not weaken protections needed to prevent exclusionary automated outcomes.

The lack of disaggregated data on persons with disabilities renders them invisible to these systems, resulting in exclusionary outcomes.

Akava: Supports an AI directive for algorithmic management and full implementation of the Platform Work Directive to protect workers' rights. Seeks mechanisms to ensure fair automated workplace decisions and avenues for redress.

we support the initiative for an artificial intelligence directive in the workplace (algorithmic management in the workplace) and the full implementation of the platform work directive,

European Law Institute: Urges expanding the definition of sensitive characteristics to capture discrimination risks in automated decision-making. Aims to strengthen fairness safeguards and improve access to redress for affected individuals.

Nordic Financial Unions - the Nordic financial trade unions confederation: Calls to extend AI-related workplace rights beyond transparency, empowering workers to contest and remedy automated decisions. Notes that the Platform Work Directive lacks sufficient positive rights and urges stronger protections and redress mechanisms.

Federation of German Consumer Organisations (vzbv): Advocates safeguarding and enforcing explanation rights under GDPR and the AI framework so individuals can understand and challenge automated decisions. Emphasizes these rights as key to fairness and effective redress.

European Digital Rights (EDRi): Emphasizes access to justice for people harmed by AI, including effective complaints, remedies, and the ability to contest automated decisions. Prioritizes practical pathways to redress and accountability.

European network of equality bodies (Equinet): Highlights the importance of complaint mechanisms and explanation rights to detect, challenge, and remedy discriminatory automated decisions. Frames these as essential safeguards for fairness and equality.

Access Now Europe: Warns that AI use in the judiciary risks miscarriages of justice and demands strong safeguards and human oversight. Calls for avenues to challenge AI-assisted decisions to protect fundamental rights and ensure redress.

2.1.5 Equality and Inclusion

Equality and Inclusion in digital and AI governance demands embedding human rights—especially the CRPD—so that accessibility, non-discrimination, participation, and reasonable accommodation are integral to design, deployment, and oversight. Insights highlight that lack of user engagement leads to irrelevant tools and barriers for persons with disabilities, underscoring the need for co-design, meaningful consultation, and human rights impact assessments. Equality must be prioritized over perceived regulatory burdens, and cultural and gender representation in governance processes is essential to ensure diverse voices shape standards, safeguards, and remedies. Across sectors, algorithmic bias and proxy-based differential treatment can reproduce historic exclusion, particularly in employment, where training data and feature proxies may flag disability or penalize deviation from past hiring norms. Digital simplification and deregulatory agendas must not dilute rights or protections; otherwise they risk entrenching barriers and exclusion. The documents call for a focused debate on disability rights in AI, recognition of gendered harms such as deepfakes targeting powerful women, and proactive safeguards to prevent new inequalities while enabling inclusive innovation.

This means that any changes to digital legislation - including the Digital Omnibus and the implementation of the AI Act - must fully respect and implement CRPD rights: equality, non-discrimination, accessibility, independent living, employment, education, health, and privacy. (European Disability Forum)

CERMI welcomes the digital simplification promoted by the Commission, but reminds that it must not entail a reduction of rights or a lack of protection for social groups requiring enhanced safeguards, such as persons with disabilities (PwD). (CERMI)

OECD research (attached, page 9) finds that the most cited barrier to the adoption of AI for people with disabilities is a lack of user engagement in developing solutions, resulting in irrelevant and impractical tools. (European Disability Forum)

This may flag disability and hence a presumed lack of fit with a job. (European Disability Forum)

European Disability Forum: Calls for AI and digital legislation to fully implement CRPD rights, ensuring equality, non-discrimination, accessibility, and meaningful participation of persons with disabilities. Warns that biased training data and proxy signals can entrench discrimination and urges an informed, disability-centered debate.

This means that any changes to digital legislation - including the Digital Omnibus and the implementation of the AI Act - must fully respect and implement CRPD rights: equality, non-discrimination, accessibility, independent living, employment, education, health, and privacy.

CERMI: Supports digital simplification only if it upholds CRPD-based human rights and enhanced safeguards for persons with disabilities. Warns that overlooking disability perspectives will create new digital barriers and consolidate exclusion.

CERMI welcomes the digital simplification promoted by the Commission, but reminds that it must not entail a reduction of rights or a lack of protection for social groups requiring enhanced safeguards, such as persons with disabilities (PwD).

ENSHPO - The European Network of Safety and Health Professional Organizations: Highlights that algorithmic bias can cause discriminatory outcomes that undermine equality and inclusion, especially in safety and health-related decision-making. Calls for robust safeguards to prevent unfair treatment.

European Law Institute: Affirms that equality law should address proxy-based differential treatment by algorithms, capturing discrimination even when based on inferred or indirect characteristics. This helps ensure inclusive, effective protection against modern forms of bias.

The Center for Countering Digital Hate: Notes that deepfakes and online abuse disproportionately target powerful women, reflecting gendered harms that threaten equality and inclusion. Calls for measures to prevent and remedy these rights violations.

European network of equality bodies (Equinet): Stresses that advancing equality must take precedence over easing regulatory burdens, ensuring strong enforcement and protections. Advocates for adequately resourced equality bodies to safeguard rights.

Culture Action Europe: Urges inclusive cultural representation in digital governance so diverse communities are not sidelined. Warns that deregulation without safeguards can exacerbate inequalities and compromise fundamental rights.

2.1.6 Privacy, Data & IP Rights

Stakeholders across this category converge on safeguarding privacy, data protection, and related fundamental rights in AI. They call for systems that prevent harm and discrimination, ensure user control over personal data, and uphold GDPR- and Charter-aligned protections throughout the lifecycle, including contexts beyond model internals and rights against harmful mentions. Building consumer trust requires a robust, enforceable legal framework, fair data processing in sensitive sectors like health, proportionate and workable technical and organisational measures, and safeguards that also respect business confidentiality and trade secrets. At the same time, civil society warns against overbroad state powers that dilute ePrivacy/GDPR guarantees, urging narrow, transparent, necessity-and-proportionality-based exceptions with specific safeguards and notice to users. IP stakeholders stress that AI development must not infringe copyrights and related rights (e.g., via unlawful training data use), and propose obligations that combat such violations while balancing fundamental rights. Overall, the category favors clear limits on restrictions, strong transparency and accountability, and effective remedies to protect privacy, data and IP rights without stifling legitimate innovation.

A robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services. (BEUC - The European Consumer Organisation)

users must be protected from abusive data practices and retain control over their personal information. (Unipol Assicurazioni S.p.A.)

In particular, Article 21.3 (e) of the GDPR allows restrictions to safeguard "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest (..)". (BEUC - The European Consumer Organisation)

Moreover, it must be clear that any legal measure adopted by Member States under this provision should also comply with Article 23.2 of the GDPR and contain specific provisions, among other things, about the purposes of processing, the scope of the restrictions introduced, the safeguards to prevent abuse and the right of end-users to be informed about the restrictions. (BEUC - The European Consumer Organisation)

Unipol Assicurazioni S.p.A.: Highlights a rights-focused approach requiring AI to prevent harm, discrimination, and abusive data practices, with users retaining control over personal information. Emphasizes privacy and fairness safeguards by design and use.

users must be protected from abusive data practices and retain control over their personal information.

BEUC - The European Consumer Organisation: Critiques overly broad Member State powers to restrict users' privacy and communications rights and calls for limits aligned with existing ePrivacy rules and GDPR safeguards. Stresses the need for a robust legal framework to protect consumers' privacy and build trust.

A robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services.

European Law Institute: Advocates upholding privacy and Charter and GDPR rights in AI contexts, including protection when individuals are referenced beyond model outputs. Calls for preserving rights against harmful mentions and ensuring safeguards apply outside AI models.

CPME: Supports safeguards for data rights and fairness in AI to protect individuals from misuse and inequity. Emphasizes maintaining lawful, fair processing and non-discrimination.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Backs safeguards that protect confidential business and personal information while limiting obligations to proportionate, necessary measures. Seeks clarity to avoid excessive compliance burdens.

ICMP - International Confederation of Music Publishers: Urges strong IP and data obligations to uphold fundamental rights and prevent unauthorized AI training on protected works. Calls for enforcement mechanisms to combat infringements and safeguard creators' rights.

noyb: Warns that diluting ePrivacy protections would threaten fundamental rights to privacy and data protection. Calls for maintaining strong safeguards to prevent rights erosion.

APPLiA (Home Appliance Europe): Argues that proposed technical and organizational safeguards for privacy and data protection are ineffective or unworkable in practice. Urges pragmatic, effective measures that protect users without imposing impractical obligations.

2.2 Harmonized Regulation and Legal Certainty

The leading message is that coherence across the EU's digital rulebook is the backbone of legal certainty. Stakeholders call for "clear alignment of definitions, scopes, and risk concepts", lex specialis carve-ins, and early regulator coordination to avoid collisions between horizontal and sectoral regimes. Uniform application matters as much as design: "consistent, EU-wide implementation, supervision, and enforcement" with convergent practices, One-Stop-Shop mechanisms, and shared Level-2 guidance. Compliance should be streamlined via "a single EU reporting gateway/one-stop-shop", aligned thresholds, and practical tooling, while clearer scope, roles, and liability reconcile Data Act/GDPR interfaces and platform functions. Predictability underpins investment: "predictable timelines, stable obligations, and coherent transitions" through aligned applicability dates, phased rollouts, and targeted grandfathering. Harmonised standards and certification—"a unified, EU-wide certification framework" and consistent Notified Body evaluation—must fit existing safety regimes and avoid overreliance on Common Specifications. Cross-border trust needs mutual recognition,

reliable data-transfer mechanisms, and restraint from extraterritorial divergence. Evidence-led simplification should be proportionate and avoid new burdens; high-quality guidance and capacity-building—"regulators should serve as advisors as well as supervisors"—are critical. Europe's rule-of-law tradition supports purpose-built instruments with IP/trade-secret and consumer safeguards. Across sub-categories, the common trend is clarity of scope, uniform enforcement, predictable transitions, and proportionate, risk-based obligations. Coordinated governance and practical tooling reduce duplication, support innovation, and uphold safety, security, and fundamental rights.

2.2.1 Evidence-Based, Proportionate & Innovation-Friendly Simplification

Stakeholders converge that simplification must be evidence-based, proportionate, and innovation-friendly: it should streamline obligations and improve coherence across the EU rulebook without diluting safeguards or legal protections. The emphasis is on quality and clarity over the sheer number of acts, risk-based and balanced requirements, and practical, adaptable common rules that work across Member States. Priorities include reducing overlaps and duplications across instruments, clarifying interplays to avoid fragmented compliance, preventing new convoluted burdens, and delivering legal certainty through horizontal alignment, consistent enforcement, and clear monitoring-and-revision mechanisms that make law future-responsive. Sufficient time for analysis and deliberation is viewed as necessary to get these interdependencies right. An evidence-led approach is urged: claims of duplication or excessive burden should be grounded in cross-cutting analysis, and targeted surgical fixes should address concrete pain points without lowering protection. Some warn that oversimplification or deregulation by stealth could undermine legal certainty or skew the playing field, while others note that existing frameworks are not, in themselves, a major barrier to innovation. Sector signals reinforce these points—calling out patchwork transparency and data-use rules, uneven enforcement, and cases where formal assessments seem disproportionate to risk—underscoring the need for proportionate simplification that supports innovation, fairness, and trust.

> *It is important to ensure a proportionate, balanced and streamlined approach, with a logical and easily compatible interplay of the requirements of these separate legislations.* (DigiFinland)
>
> *Simplification is not deregulation: the goal is coherence, transparency, and efficient implementation, without lowering protections.* (Union of Entreprenuers and Employers)
>
> *If simplification means making it easier for genAI-focused companies to make money, this would be a massive mistake.* ()
>
> *We do not identify the existing regulatory framework as a particularly important hurdle to innovation and investment.* (BEUC - The European Consumer Organisation)
>
> **:** Warns that simplification must not prioritise genAI business interests over safeguards and the public interest, urging evidence-based, proportionate changes that preserve protections.
>
> *If simplification means making it easier for genAI-focused companies to make money, this would be a massive mistake.*
>
> **ZVEI e.V.:** Reports that bureaucracy reduction and legal certainty have not materialised, calling for proportionate simplification that delivers practical clarity without undermining objectives.
>
> *Initial experience with the new regulation has already made it clear that the twin goals of minimising bureaucracy and providing legal certainty have not been achieved.*
>
> **DigiFinland:** Advocates a proportionate, balanced, and streamlined framework with logically compatible requirements across laws to enable coherent, innovation-friendly compliance.
>
> *It is important to ensure a proportionate, balanced and streamlined approach, with a logical and easily compatible interplay of the requirements of these separate legislations.*
>
> **FIGIEFA aisbl:** Supports simplification only insofar as it improves coherence and efficiency without deregulating or weakening protections.
>
> *Simplification, however, must not be confused with deregulation.*
>
> **Encode Europe:** Stresses that simplification must not dilute regulatory safeguards; proportionality should enhance clarity while maintaining protections.
>
> *Simplification should however not lead to weakening of regulatory safeguards that are in place.*

EMMA-ENPA: Urges that simplification remain within its mandate and not be used to push fundamental changes through secondary law.

Simplification efforts should not exceed the simplification mandate and de facto turn into a means of introducing fundamental changes to secondary law.

FEBIS: Calls for prioritising the quality and clarity of rules, not just their number, to achieve meaningful simplification and legal certainty.

FEBIS strongly encourages the Commission to focus not only on the number of regulations but also on their quality and clarity.

Video Games Europe: Warns against simplification that introduces new, convoluted compliance burdens; streamlining should reduce complexity in practice.

Therefore, we caution against such measures when they bring new convoluted compliance challenges.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Highlights harmful overlaps and inconsistencies across frameworks, urging harmonised, proportionate rules and consistent enforcement to support startups and SMEs.

For German and European AI startups and SMEs, todays patchwork of rules, across European digital regulatory frameworks, creates overlapping transparency obligations, restrictive and inconsistent data-use provisions, duplicated documentation and assessments, and uneven enforcement across Member States.

GSMA: Argues that proliferating and poorly coordinated instruments create harmful complexity, underscoring the need for coherent, streamlined, and well-interfaced regulation.

An overly complex regulatory landscape, marked by the proliferation of legislative instruments and their unclear and fragmented interplays, risks undermining the very objectives set out by EU institutions.

Government Office of the Czech Republic: Emphasises evidence-based deliberation, seeking sufficient time for analysis and Council debate given wide-reaching impacts on the digital acquis.

However, given the wide- reaching implications for the digital acquis, sufficient time for analysis and debate at the Council will be necessary.

Telefonica, S.A.: Calls for a more ambitious yet balanced simplification agenda that reduces undue burdens while preserving essential protections.

However, Telefónica urges the European Commission to adopt a more ambitious and balanced approach to regulatory simplification.

Centre for Democracy and Technology Europe: Notes a lack of evidence for claims of duplication or excessive burdens and calls for cross-cutting analysis before pursuing simplification.

As the European Commission's efforts to reduce perceived regulatory burden and simplification conversations gain traction, the evidence behind assertions that the AI Act and other laws may be duplicative of existing legislation or overly burdensome is generally lacking, and cross-cutting analyses of the relationships and relative strengths of the other elements of the EU digital rulebook continue to be missing in the conversation.

Mastercard Europe SA: Supports common rules that are practical and adaptable to national contexts, enabling equal access and fair ecosystem growth through proportionate harmonisation.

Common rules should be both practical and adaptable to national conditions to ensure equal access to digital opportunities and fair growth of the ecosystem.

BEUC - The European Consumer Organisation: Contends the current framework is not a major barrier to innovation, cautioning against deregulation disguised as simplification.

We do not identify the existing regulatory framework as a particularly important hurdle to innovation and investment.

Bolt: Affirms that simplification should improve coherence and usability without equating to deregulation or reduced protections.

Simplification would not mean deregulation.

The International Center for Law & Economics: Criticises superficial procedural tweaks that fail to fix core enforcement issues, urging targeted reforms to improve efficiency and legal certainty.

The Commission's proposed GDPR Procedural Regulation fails to address these fundamental issues, merely tinkering at the margins while leaving the privacy-absolutist enforcement structure intact.

Schneider Electric: Cautions that oversimplification can undermine legal certainty, advocating measured, proportionate adjustments.

An oversimplification of the rules could risk undermining legal certainty in the EU.

Adigital (Asociación Española de la Economía Digital): Endorses a horizontal approach for coherence while retaining necessary sector-specific rules to maintain effectiveness and certainty.

From this perspective, advocating for a more horizontal regulatory approach does not mean eliminating all sector-specific rules.

Vodafone Group: Warns that telecoms simplification is being deprioritised relative to platforms, urging proportionate prioritisation of urgent sector reforms.

Based on the scope of the current call for evidence Vodafone is extremely concerned that urgent and necessary regulatory simplification in the telecoms sector is being de-prioritised relative to efforts to simplify or streamline regulation on digital platforms.

Panasonic Europe B.V.: Backs a surgical simplification package that delivers near-term, high-impact fixes without lowering protection levels.

We support the Digital Omnibus as a surgical simplification package that delivers nearterm, highimpact fixes without lowering protection.

Union of Entreprenuers and Employers: Defines simplification as achieving coherence, transparency, and efficient implementation while keeping protections intact, not deregulation.

Simplification is not deregulation: the goal is coherence, transparency, and efficient implementation, without lowering protections.

: Argues that current debureaucratisation efforts risk sliding into deregulation, which would undermine a rules-based system.

The current call for de-bureaucratisation is the attempt to deregulation, which is not conducive to a rules-based system.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Identifies disproportionate CRA conformity demands for low-risk products, advocating risk-based proportionality to avoid unnecessary burdens.

Even though the CRA will not require any additional cybersecurity protection measures due to the virtually non-existent cybersecurity risks, these products with digital elements will still have to go through the NLF formal conformity assessment to demonstrate CRA compliance with all processes, documents, and labelling requirements.

: Proposes simplifying by adding monitoring and revision mechanisms, shifting from future-proof to future-responsive, adaptive governance.

EU digital regulation can be simplified not simply by reducing the number of rules, but also by introducing clear mechanisms for monitoring and revision, moving from future-proof to future-responsive law.

: Insufficient provided content to extract the document’s position on evidence-based, proportionate simplification and legal certainty.

2.2.2 Clear Scope, Definitions, Roles & Liability

Stakeholders consistently call for clearer scope and definitions to ensure harmonized regulation and legal certainty across digital frameworks. Ambiguities around what constitutes an AI system, products with digital elements, safety components, and the boundary between personal and non-personal data create interpretative uncertainty and compliance risk. Vague transparency provisions and unclear applicability (e.g., combined datasets, SaaS coverage) further complicate obligations and enforcement. A second theme concerns roles and liability. Divergences between the Data Act's "user" and the GDPR's "data subject" raise questions about lawful bases and responsibility allocation. Sectoral competences (e.g., medicines) must remain intact, machine-to-machine communications should stay in scope, and platform functions (like ad space) challenge existing liability categories (e.g., hosting). Exceptions such as the trade secrets "handbrake" need tighter framing to avoid lengthy arbitration, while new initiatives should align liability rules with established regimes to prevent fragmentation. The overarching message is that precise definitions, scoped obligations, and clearly assigned roles build trust and legal certainty, reduce ambiguity for both existing and future systems, and enable proportionate, predictable compliance across sectors.

> *Furthermore, unclear definitions of "products with digital elements" add additional legal uncertainty.* (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))
>
> *Article 4(13) limits use of non-personal data to explicit contracts, yet it is unclear what constitutes "non-personal data of the user," especially when datasets combine personal and non-personal data.* (GSMA)
>
> *Some argue that providing space for online advertisements constitutes hosting.* (Seznam.cz, a.s.)
>
> *While we acknowledge the importance of the "trade secrets handbrake" (which frames the conditions under which a data holder can withhold, suspend or, exceptionally, refuse to share data) we consider useful to further reflect on ways to enhance legal certainty with regards to its scope, considering the risk of lengthy and complex arbitration processes between data subjects and data holders.* (Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique)
>
> **DATEV eG:** The submission flags that the AI Act's core definition of an AI system is too vague, creating interpretative uncertainty and undermining legal certainty.
>
> *One of the core elements of the AI Act the definition of an artificial intelligence system is vague, resulting in significant interpretative uncertainty (e.g., varying levels of autonomy or may exhibit adaptiveness).*
>
> **PHOENIX group:** Cautions that clarifying EU rules for medicines must respect Member State competences on authorization, dispensing and distribution, to avoid scope overreach.
>
> *However, this should be done only in ways that do not alter Member State competences over authorization, dispensing and distribution of medicines.*
>
> **France Digitale:** Seeks clarity on whether the Data Act applies to SaaS offered by cloud providers and third-party startups, to ensure predictable obligations and roles.
>
> *Does the Data Act apply to SaaS offered directly by the cloud providers or also SaaS by third parties (service startups)?*
>
> **Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique:** Calls for clearer boundaries to the trade secrets 'handbrake' to enhance legal certainty and avoid lengthy disputes between data holders and data subjects.
>
> *While we acknowledge the importance of the "trade secrets handbrake" (which frames the conditions under which a data holder can withhold, suspend or, exceptionally, refuse to share data) we consider useful to further reflect on ways to enhance legal certainty with regards to its scope, considering the risk of lengthy and complex arbitration processes between data subjects and data holders.*
>
> **Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association):** Warns that unclear definitions of 'products with digital elements' generate legal uncertainty and complicate compliance responsibilities.
>
> *Furthermore, unclear definitions of "products with digital elements" add additional legal uncertainty.*

GSMA: Highlights ambiguity around what counts as a user's non-personal data, especially in mixed datasets, and urges clearer scope to align data-use obligations.

Article 4(13) limits use of non-personal data to explicit contracts, yet it is unclear what constitutes "non-personal data of the user," especially when datasets combine personal and non-personal data.

Airbus: Notes that a particular provision creates significant legal ambiguity for both legacy and future AI systems, indicating a need for clearer temporal scope and responsibilities.

This provision creates a significant legal ambiguity for past and future AI systems.

Bitkom e.V.: Requests guidance on the legal basis under GDPR when the Data Act's 'user' and GDPR's 'data subject' are different persons, clarifying roles and liability.

Legal Basis under the GDPR when user and data subject roles diverge in the Data Act: Which legal basis under the GDPR is used when the »user« under the Data Act and the »data subject« under the GDPR are not the same person?

Seznam.cz, a.s.: Points to uncertainty over whether providing ad space is 'hosting,' seeking precise definitions to delineate intermediary liability.

Some argue that providing space for online advertisements constitutes hosting.

Mastercard Europe SA: Urges clear, aligned liability rules for the European Digital Identity Wallet to avoid gaps seen in eIDAS2 implementation.

So, when developing the EBW, it is important to thoroughly assess liability implication and ensure those rules are clear and aligned with existing frameworks, as a lack of clarity on this point has been a concern in the implementation of eIDAS2.

BEUC - The European Consumer Organisation: Advocates keeping machine-to-machine communications clearly within scope to ensure consistent protections and obligations.

Ensure that machine-to-machine communications duly remain in the scope of the Regulation.

Schneider Electric: Asks for a sharper definition of 'safety component' to clarify responsibilities and liability boundaries.

What constitutes a "safety component" requires more precision.

Adigital (Asociación Española de la Economía Digital): Recommends excluding unconditional refund obligations for merchant-initiated transactions in PSD3/PSR to avoid misaligned liability allocation.

Concerning PSD3 and the proposed Payment Services Regulation (PSR), it is recommended to exclude the unconditional refund obligation for merchant-initiated transactions (MITs) and transfers with equivalent refund obligations (as proposed in Article 85bis of PSR), in order to avoid equating them with SEPA direct debits.

Entrust SAS: Emphasizes the need for precise definitions of key terms to secure legal certainty and consistent interpretation.

Clarity on key terms is also essential.

: Affirms that well-defined rules foster trust and legal certainty, underscoring the value of clear scope and obligations.

Rules create trust, legal certainty and clarity.

European Advertising Standards Alliance (EASA): Reports that vague transparency provisions create legal uncertainty for advertisers, calling for clearer requirements and roles.

Due to these provisions' vague wording, stakeholders in the advertising sector face significant legal uncertainty regarding the interpretation and practical implementation of this transparency requirement.

2.2.3 Cross-Regulatory Coherence & Conflict Resolution

Stakeholders converge on the need for cross-regulatory coherence to deliver legal certainty: overlapping, duplicative, or inconsistent obligations across EU instruments (AI Act, Data Act, GDPR/ePrivacy, NIS2/CRA, MDR/IVDR, sectoral safety law) create confusion for businesses and authorities, inflate compliance costs, and can chill innovation (e.g., IoT and AI). While the push to harmonise is welcomed, persistent inconsistencies—especially conflicting or outdated definitions and interfaces—mean that new rules must not override or collide with existing horizontal or vertical regimes. Solutions emphasized include consolidation beyond mere red-tape cuts; clear alignment of definitions, scopes, and risk concepts; explicit lex specialis/sectoral carve-ins to avoid double regulation (e.g., medical devices vs. AI Act); and proactive coordination among regulators to detect and resolve conflicts early (e.g., a dedicated Regulatory Consistency Board). Complementary updates to adjacent frameworks (such as copyright for AI-generated content) and careful distinctions between policy domains (e.g., safety vs. cybersecurity) are seen as essential to sustain coherence, predictability, and innovation-friendliness.

> *However, companies across all industry sectors face significant challenges due to several regulatory issues, in particular: an increasing volume of regulatory measures, a lack of coherence between different legislations, overlapping or duplicate regulations and dysfunctionalities in European digital policy.* (ZVEI e.V.)
>
> *Avoids duplicate and potentially conflicting obligations between the Al Act and MDR/IVDR.* (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)
>
> *The Digital Omnibus should establish a Regulatory Consistency Board under DG CONNECT, tasked with resolving such cross-regulatory contradictions before delegated acts are adopted.* (Namirial Spa)
>
> *Art. 11(7) of the CRA provides a different definition of main establishment than Art. 26(2) of the NIS2.* (Ibec)
>
> **DATEV eG:** They welcome simplification but stress the current package will not solve key cross-regulatory problems. Deeper harmonization is needed to resolve conflicts.
>
> *However, we would also like to emphasize that further simplification steps remain necessary, as this package will not resolve the most pressing issues.*
>
> **FERMA - Federation of European Risk Managers Associations:** They urge consolidation of digital rules that goes beyond administrative streamlining. Substantive alignment is needed to ensure coherence and predictability.
>
> *Providing consolidation that is not only limited to cutting red tape is also essential.*
>
> **SIEMENS AG:** They highlight the need to reconcile AI requirements with existing industrial safety regimes. Coherent rules should ensure reliability and robustness without conflicting sectoral standards.
>
> *This example shows that the high safety standards in industrial areas, such as machinery, request AI system to demonstrate reliability and robustness.*
>
> **City of Stockholm:** The city supports EU-level harmonization to reduce conflicting obligations. Clear, consistent legislation aids municipalities in compliance and service delivery.
>
> *From a municipal perspective, the Commission's intention of harmonising EU legislation is positive.*
>
> **ZVEI e.V.:** They describe growing regulatory volume and incoherence across laws, with overlaps and duplications harming digital policy. Coordinated cleanup is needed to restore legal certainty.
>
> *However, companies across all industry sectors face significant challenges due to several regulatory issues, in particular: an increasing volume of regulatory measures, a lack of coherence between different legislations, overlapping or duplicate regulations and dysfunctionalities in European digital policy.*
>
> **Zimmer Biomet:** They warn that multiple instruments can collectively produce overlapping and inconsistent duties. Better coordination is required to prevent duplicative compliance burdens.

While each instrument pursues legitimate and important policy goals, their combined effect can create overlapping, duplicative, and sometimes inconsistent obligations.

Volkswagen Group: They seek safeguards so the Data Act does not override or overlap existing laws. Clear boundaries are needed to avoid legal uncertainty across horizontal and sectoral regimes.

The Data Acts core provisions - such as the definitions governing access to data from connected products, the obligations for manufacturers and service providers, and the rules for data sharing (including financial compensation) - must not lead to legal uncertainty by over- lapping with/overriding existing horizontal or vertical legislation.

eco - Verband der Internetwirtschaft e.V.: They argue the ePrivacy Directive is outdated and overlaps with the GDPR. Updating and aligning these frameworks is necessary to eliminate redundancy.

In general, the ePrivacy Directive is outdated and significantly overlapping with the GDPR.

EMMA-ENPA: They call for coherent AI and digital frameworks that uphold intellectual property rights to secure legal certainty. Alignment ensures innovation while respecting rights.

Only in this way will the objective laid down in the Al Act of helping rightsholders exercise and enforce their rights under Union law be achieved and legal certainty for all stakeholders be secured, while also ensuring that the EU's Al and digital frameworks remain coherent, innovation-friendly, and firmly respectful of intellectual property rights.

FEBIS: They stress that poorly coordinated or unclear rules create confusion for businesses and authorities. Harmonized guidance and enforcement can resolve this.

Poorly coordinated or unclear regulations create confusion for both businesses and competent authorities.

Dun & Bradstreet: They support reducing fragmentation and complexity in data access and reuse rules. Streamlined, consistent standards would improve cross-regulatory clarity.

We strongly support efforts to reduce fragmentation and complexity in the rules governing access to and re-use of such data.

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: They urge avoiding duplicated or conflicting obligations between the AI Act and MDR/IVDR. Clear delineation and alignment across regimes are essential.

Avoids duplicate and potentially conflicting obligations between the Al Act and MDR/IVDR.

German Insurance Association: They note insurers face overlapping but distinct regulatory requirements. Cross-framework clarity is needed to manage compliance coherently.

In addition to this robust regulatory framework insurers are subject to other legal instruments with overlapping, but distinct, requirements.

GSMA: They emphasize that safety and cybersecurity are conceptually different and should not be conflated. Coherent regulation must respect these distinctions.

Cybersecurity and safety differ fundamentally in definitions, threats, risks, objectives, and mitigation measures.

Bitkom e.V.: They criticize inconsistent definitions and interpretations across laws. Harmonizing legal terminology would address root causes of incoherence.

Symptom-based approach instead of addressing root causes: General problem of inconsistent definitions and differing interpretations of legal terms.

German Social Insurance European Representation: They call for adapting the AI Act to avoid contradictions with data security and social data protection frameworks. Coordinated reforms are necessary for legal certainty.

At the same time, it sees a significant need for adaptation to avoid contradictions between the AI Act and other regulatory frameworks such as data security or social data protection.

BEUC - The European Consumer Organisation: They underline ePrivacy's central role in safeguarding confidentiality of communications. Coherence with other instruments is key to preserving fundamental rights and legal clarity.

Currently the e-Privacy Directive is the main legal instrument that crystallises Article 7 of the European Charter of Fundamental Rights4 (the respect for private life) into secondary EU law and specifically protects the confidentiality of communication

Centre for Information Policy Leadership (CIPL): They urge the Commission to fix overlaps and inconsistencies among major digital laws. A coordinated approach is needed to restore coherence.

CIPL urges the Commission to address the growing overlap and inconsistency among major digital instruments.

European Tech Alliance: They identify potential conflicts between NIS2 requirements and GDPR obligations. Guidance and alignment are needed to reconcile duties.

There are concerns about potential conflicts between NIS-2 requirements and GDPR obligations.

Ibec: They point to conflicting definitions of main establishment between the CRA and NIS2. Aligning definitions would reduce uncertainty and enforcement inconsistency.

Art. 11(7) of the CRA provides a different definition of main establishment than Art. 26(2) of the NIS2.

Namirial Spa: They propose a Regulatory Consistency Board under DG CONNECT to preempt cross-regulatory contradictions. Systematic resolution before delegated acts would enhance coherence.

The Digital Omnibus should establish a Regulatory Consistency Board under DG CONNECT, tasked with resolving such cross-regulatory contradictions before delegated acts are adopted.

Meta Platforms Ireland Limited: They argue ePrivacy's cookie and traffic rules misalign with the GDPR and modern technologies, causing legal uncertainty and hindering IoT and AI. Modernization and harmonization are required.

The ePD's cookie and traffic data provisions are misaligned with the GDPR and modern digital realities, creating legal uncertainty and stifling IoT and AI development.

Almega: They urge updating copyright frameworks to clarify the legal status, authorship, and rights for AI-generated content. Cross-regulatory clarity would improve legal certainty and innovation.

The Commission and co-legislators must update copyright frameworks to clarify AI-generated content's legal status and define authorship and rights.

Union of Entreprenuers and Employers: They emphasize the need for flexible, coordinated oversight among regulators. Such coordination balances innovation with accountability across regimes.

complex, flexible coordination among regulators will be critical to maintain both innovation and accountability.

2.2.4 Predictable Timelines, Transitions & Regulatory Stability

This category emphasizes the need for predictable timelines, stable obligations, and coherent transitions to ensure harmonized regulation and legal certainty. Stakeholders caution against stop-and-go policymaking and reopening recently agreed frameworks, urging preservation of the acquis (e.g., GDPR) and a level playing field to sustain investment and competitiveness. Sudden or poorly considered changes are seen as creating uncertainty that deters long-term planning. On implementation, contributors call for aligned applicability dates across interlinked instruments, phased rollouts, grace periods, and where warranted, “stop-the-clock” mechanisms to accommodate incomplete national designations, delayed standards, or missing secondary rules. They stress protecting legitimate expectations for existing systems (via grandfathering or clear exemptions) while resisting blanket postponements that would dilute core objectives, particularly in the AI Act. Without coordination, overlapping or compressed deadlines risk a regulatory limbo and even disruptions to supply chains and product

availability; divergent readings about whether the AI Act effectively grandfathers pre-existing systems illustrate the need for clearer, more consistent transition rules.

Industry needs legal certainty and predictability to plan the significant investments required to enable data-driven services. (European Tyres and Rubber Manufacturers' Association)

At the same time, however, a stable and predictable legal framework is vital for the competitiveness of EU businesses. (Government Office of the Czech Republic)

the Act explicitly excludes from its scope AI systems already in use prior to August 2024, unless substantial changes to the design of those systems or their intended purpose occur after this date. (Centre for Democracy and Technology Europe)

Unlike the MDR, which includes transitional provisions under Article 120, the AI Act does not offer any form of grandfathering for existing AI systems. (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)

: Warns that unpredictable regulatory changes create uncertainty that deters investment and harms the EU's strategic interests.

If anything, unpredic- table and poorly-considered changes to applicable EU laws risk creating an uncertain environment for invest- ment and would weaken the EU's long-term strategic in- terests.

Kaspersky Labs Limited: Supports deregulation only if it preserves the substance of existing laws, ensuring continuity and legal certainty.

At the same time, we note that the adjustments proposed in the Digital Omnibus are not expected to alter or negatively affect the substance of the underlying acts.

eco - Verband der Internetwirtschaft e.V.: Proposes a stop-the-clock mechanism and extended transitions so Member States can complete implementation without causing instability.

Against this background, it seems reasonable - insofar as the procedures and national implementations have not yet been completed - to introduce a so-called "stop-the- clock" mechanism, as is also used in other initiatives.

EMMA-ENPA: Urges maintaining a level playing field and opposes using the Omnibus to dilute or postpone AI Act obligations for GPAI providers.

Against this background, EMMA and ENPA oppose in the strongest terms any potential use of the Digital Omnibus as a means to either dilute, in any manner, delete altogether, or postpone the entry into application of the copyright-relevant obligations incumbent on providers of general- purpose AI models per Art. 53(1)(c) and (d), which represent but an initial, yet still insufficient step that must necessarily be built upon.

FEBIS: Cautions that stop-and-go regulatory approaches create instability instead of simplification, undermining business certainty.

FEBIS members caution against "stop-and-go" regulatory approaches, which generate instability for businesses rather than simplification.

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Calls for protecting legitimate expectations via transitional grandfathering for existing AI medical devices, noting current AI Act gaps.

Unlike the MDR, which includes transitional provisions under Article 120, the AI Act does not offer any form of grandfathering for existing AI systems.

European Tyres and Rubber Manufacturers' Association: Stresses that industry needs legal certainty and predictability to plan and sustain data-driven investment and services.

Industry needs legal certainty and predictability to plan the significant investments required to enable data-driven services.

Government Office of the Czech Republic: Emphasizes a stable, predictable framework for competitiveness and warns against substantive changes beyond simplification.

Therefore, CZ would avoid substantive changes to rules that go beyond simplification, especially those that have been recently endorsed.

Verisure: Advocates aligning implementation dates across related laws since many authorities are not yet operational, to ensure practical rollout.

Given that many of these authorities are not yet designated or operational, Verisure strongly believes that the most efficient and practical way to achieve this is by aligning all relevant implementation dates across the CRA and related legislation.

Centre for Democracy and Technology Europe: Notes that pre-existing AI systems are largely outside scope unless substantially changed, shaping a clear transitional boundary.

the Act explicitly excludes from its scope AI systems already in use prior to August 2024, unless substantial changes to the design of those systems or their intended purpose occur after this date.

BEUC - The European Consumer Organisation: Supports aligning applicability with the GDPR to provide consistency and legal certainty for businesses and consumers.

This would ensure consistency and legal certainty both for businesses and consumers.

Ibec: Urges avoiding a premature overhaul of the EECC during critical implementation, and reducing overlaps while preserving subsidiarity.

Avoid a premature overhaul of the European Electronic Communications Code (EECC), which remains in a critical implementation phasexlix.

Schneider Electric: Warns against drastic regulatory changes and reopening the GDPR, which would undermine predictability and legal certainty.

We believe that reopening the GDPR could introduce significant risks and undermine legal certainty.

Adigital (Asociación Española de la Economía Digital): Highlights overlapping timelines that create a regulatory limbo and disrupt company preparations, increasing complexity.

The entry into force of the CSDDD in July 2024 and CSRD compliance deadlines (e.g., 2026 in many cases) overlap with the publication of the Omnibus proposals, creating a "regulatory limbo."

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Warns that tight implementation timelines could disrupt supply chains and reduce product availability in the EU.

Tight implementation timelines risk negatively impacting existing supply chains.

ANEC: Insists that AI Act timelines be respected and that postponements would undermine the regulation's purpose and credibility.

Postponing the applicability of the AI Act because the development of harmonized standards is delayed or for any other reason, would undermine both the purpose and credibility of the regulation.

Compagnie Nationale des Commissaires aux Comptes (professional organisation for statutory auditors): Calls to preserve the EU regulatory acquis while accelerating AI Act-related standardization for predictable implementation.

European Partnership for Democracy: Recommends prioritizing implementation of adopted rules and avoiding premature reviews that would create uncertainty.

FME: Advocates feasible implementation timelines linked to the availability of standards to enable workable compliance.

Pour Demain Europe: Warns that early changes framed as simplification send the wrong signal and erode regulatory stability.

Deutscher Gewerkschaftsbund: Opposes weakening or renegotiating rules and supports a gradual entry into force to provide planning certainty.

Palombar - Associação de Conservação da Natureza e do Património Rural: Flags that reopening or revising the AI Act would inject uncertainty and hamper effective deployment.

BusinessEurope: Requests grace periods and coordination to handle overlaps, including with NIS2, to ensure predictable transitions.

IDEMIA: Supports aligning compliance timelines with harmonized standards to give businesses clarity and certainty.

Confederation of Norwegian Enterprise (NHO): Proposes grace periods and potential stop-the-clock measures to manage delays and ensure orderly transitions.

Polish Confederation Lewiatan: Points to unclear compliance pathways and delays that create legal uncertainty and complicate planning.

Danish Society of Engineers (IDA): Urges prioritizing the timely rollout of the AI Act rather than reopening it, to maintain predictability.

Ecommerce Europe: Supports phased implementation with transition safeguards and cautions against reopening the GDPR to preserve certainty.

University of Amsterdam: Warns that removing existing protections would increase legal uncertainty and fragment the framework.

Association of Netherlands Municipalities: Calls to preserve and implement the existing digital rulebook and avoid amending the GDPR and AI Act for stability.

AI Standards Lab: Notes that major legislative changes now would heighten confusion and reduce predictability for stakeholders.

IAB Europe: Warns that an unstable regulatory framework hampers long-term projects and investment decisions.

Association des Constructeurs Européens de Motocycles: Requests adjusted timelines to reflect broader sector coverage, enabling manageable compliance.

Advertising Information Group: Highlights regulatory complexity and incompatible timelines across files, urging better alignment for certainty.

EU DisinfoLab: Cautions that perception-driven reopening of laws creates uncertainty and chills compliance efforts.

epicenter.works - for digital rights: Argues that stable, predictable regulatory frameworks build confidence and legal certainty.

ENNHRI - European Network of National Human Rights Institutions: Opposes premature changes to the AI Act and supports focusing on consistent implementation and enforcement.

WITNESS: Rejects deregulation and delays that would undermine protections and legal clarity.

ICMP - International Confederation of Music Publishers: Urges preventing legislative backsliding on the DSA to avoid destabilizing the regulatory environment.

AFME: Seeks clarity on the timeline and thresholds for compute obligations to enable predictable planning.

Forvis Mazars: Calls for legal predictability to guide investment and compliance across the regulatory landscape.

Danish Institute for Human Rights: Advises against premature AI Act changes and for prioritizing implementation to ensure certainty.

AlgorithmWatch: Warns that reopening rules risks fragmentation and undermines legal certainty; stability is essential.

Orgalim - Europe's Technology Industries: Asks to avoid duplicative requirements and ensure an adequate transition phase for industry.

ACT | The App Association: Suggests pausing certain AI Act obligations until guidance and standards provide sufficient clarity and feasibility.

ESYS Foundation: Recommends binding deadlines for institutions and standards bodies to deliver timely guidance and predictability.

InfoCert: Calls to align and clarify compliance timelines across related laws to reduce uncertainty.

Trans Sped: Flags ambiguous terms and contradictory deadlines that cause legal uncertainty and requests harmonization.

Danish Entrepreneurs: Urges implementing existing rules before adding new ones to preserve stability and predictability.

DECATHLON SE: Notes uncertainty due to missing secondary legislation and calls for timely, clear implementing acts.

European Digital Rights (EDRi): Warns that delays and reforms would undermine legal certainty and harmonization and add compliance risk.

Siemens Healthineers AG: Highlights a lack of grandfathering and risks of incoherent retroactivity that create uncertainty for existing systems.

European Publishers Council: Emphasizes the need for legal certainty and predictability, opposing changes that introduce instability.

ACT (Association of Commercial Television and Video on Demand Services in Europe): Calls to avoid weakening or reopening the AI Act to maintain predictability and legal certainty.

Open-Xchange AG: Urges rapid, clear regulatory guidance and timely standards to support predictable compliance.

Middle Tech Europe: Notes that framework inflexibility and frequent shifts create legal uncertainty for mid-sized tech firms.

Österreichische Notariatskammer: Insists that legal certainty and foreseeable transitions should guide any reforms.

OpenMined: Highlights a gap between policy vision and legislation and calls for clearer, more predictable rules.

European network of equality bodies (Equinet): Warns that amendments risk legal uncertainty and argues for consistent application of existing rules.

DIGITALEUROPE: Opposes reopening core GDPR provisions to protect legal certainty and predictability.

STM: Advises against revisiting established rules and prioritizes consistent, harmonized application.

Enedis: Requests clarity on whether smart meter obligations apply retroactively to ensure predictable compliance.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Argues that frequent legal changes erode trust and jeopardize SMEs' investments; stability is needed.

Esomar: Supports an approach that enhances legal certainty while maintaining protections and aligned timelines.

: Opposes reopening the AI Act and supports a clear transitional regime for existing systems.

European Games Developer Federation (EGDF): Prefers minimal, targeted adjustments over reopening to preserve stable timelines.

Access Now Europe: Warns that Digital Omnibus changes to the AI Act could create uncertainty and weaken protections.

Adyen: Notes that short publication-to-enforcement windows are challenging and asks for more predictable lead times.

Logitech: Highlights uncertainty in transition timelines and seeks clear, harmonized schedules across files.

2.2.5 International Alignment & Mutual Recognition

This category captures the drive for predictable, interoperable cross-border rules that enable mutual recognition, legal equivalence, and alignment with international standards while ensuring legal certainty. Stakeholders call for reliable mechanisms for international data flows (e.g., SCC-based transfers and BCRs) and streamlined approvals, as well as clearer intra-group legal bases, to reduce duplicative paperwork and service delays. Mutual recognition and harmonized conformity approaches are seen as key to cutting friction and enabling trust across jurisdictions. At the same time, contributors warn that unilateral or extraterritorial approaches risk fragmenting markets, creating conflicting obligations, and triggering retaliatory policies abroad. Concerns include EU common specifications that diverge from established standardization processes and create barriers with international markets, and copyright provisions that extend EU rules beyond its territory, undermining territoriality and legal certainty. There is a parallel emphasis on safeguarding EU strategic trade interests while pursuing coordinated solutions to prevent disputes and strengthen multilateral positioning. Alignment should be collaborative and sequenced: some regions advocate internal harmonization before external compliance, prioritizing policy learning, cooperation, and technology transfer over dependency. Others stress that EU regulatory choices should not be settled via trade disputes. Overall, the goal is harmonized regulation that supports mutual recognition and cross-border trust without sacrificing sovereignty or competitiveness.

For data transfers outside the EU, full legal certainty is required, in particular where these depend on standard contractual clauses (Video Games Europe)

The proposal to extend the use of Common Specifications represents a departure from traditional European Standardisation System practices, potentially creating barriers between the EU and international markets. (Amazon)

This shift could also prompt third countries to implement similarly restrictive or divergent policies. (Amazon)

This approach creates legal uncertainty and compliance challenges for AI developers, as it forces companies to address European copyright standards even when they lawfully trained models in countries with different copyright frameworks, potentially exposing them to conflicting legal obligations. (Meta Platforms Ireland Limited)

German Insurance Association: Argues that expanded GDPR BCR requirements and slow approvals overburden intra-group transfers, undermining international data flows. Calls for accelerating BCR approvals and creating a specific legal basis for intra-group processing, including special-category data.

Above all, the lengthy approval process makes BCRs increasingly unattractive in practice as a tool for data transfers to third countries within corporate groups.

Video Games Europe: Calls for full legal certainty for transfers outside the EU, noting reliance on SCCs entails added safeguards, impact assessments, and information obligations. Emphasizes the need to reduce complexity and ambiguity for cross-border data flows.

For data transfers outside the EU, full legal certainty is required, in particular where these depend on standard contractual clauses

Amazon: Warns that extending EU Common Specifications departs from established standardization practices, risking market fragmentation and barriers with global markets. Notes this shift could spur restrictive or divergent policies in third countries.

The proposal to extend the use of Common Specifications represents a departure from traditional European Standardisation System practices, potentially creating barriers between the EU and international markets.

Meta Platforms Ireland Limited: Criticizes the extraterritorial reach of EU copyright rules for AI training as inconsistent with international principles, creating uncertainty and conflicting obligations across jurisdictions. Recommends removing such provisions to realign with territoriality and legal clarity.

This approach creates legal uncertainty and compliance challenges for AI developers, as it forces companies to address European copyright standards even when they lawfully trained models in countries with different copyright frameworks, potentially exposing them to conflicting legal obligations.

Adigital (Asociación Española de la Economía Digital): Urges simplification that safeguards the EU's strategic trade interests and addresses fragmented tax structures that burden foreign players. Advocates coordinated, fair solutions to prevent disputes and strengthen the EU's multilateral position.

A coordinated and fair solution would help prevent trade disputes and strengthen the EU's position in multilateral negotiations.

: Argues for prioritizing internal harmonization across African RECs before aligning with external regimes. Favors collaborative, learning-based engagement with EU rules through cooperation and technology transfer over dependency.

Collaboration before convergence: Africa seeks constructive alignment with EU rules through cooperation, pilot projects, and technology transfer - not through regulatory dependency.

Akava: Asserts EU sectoral regulation should be determined internally rather than through trade disputes. Emphasizes regulatory autonomy amid international pressures.

the regulation in the sector is an internal matter of the EU and should not be decided in trade disputes.

American Chamber of Commerce to the EU: Rejects the Country of Origin principle, signaling caution about cross-border recognition frameworks. Highlights the need for approaches that ensure fairness and legal certainty in international operations.

DigitalTrade4.EU: Advocates using mutual recognition agreements, contractual tools, and legal equivalence to ease compliance and enable cross-border digital trade. Emphasizes predictable frameworks to support international interoperability.

VDMA - Advancing Europe´s machinery industry: Identifies gaps in oversight for non-EU surveillance and chemical imports, underscoring uneven playing fields. Suggests better alignment with third-country regimes to close compliance and safety gaps.

Verband der Automobilindustrie e.V.: Describes international registration hurdles and regulatory barriers that impede cross-border activity. Calls for streamlined recognition and harmonized procedures across markets.

ICMP - International Confederation of Music Publishers: Notes that international constraints on AI-related copyright exceptions limit unilateral policy choices. Encourages alignment with global norms to avoid conflicts and ensure legal certainty for innovation.

Brunel University of London: Argues that alignment with global standards enhances trust, interoperability, and competitiveness. Supports harmonized approaches to unlock international market access.

The Center for Countering Digital Hate: Observes EU, UK, and Australia as regulatory frontrunners, implying coordination opportunities. Suggests alignment to reduce divergence and enable mutual recognition.

Charter of Trust: Calls for alignment with international standards to bolster security, interoperability, and consistency. Aims to minimize fragmentation across jurisdictions.

SPMS – Shared Services of the Ministry of Health: Promotes a principle of normative equivalence to recognize functionally similar rules across countries. Seeks mutual recognition that delivers predictability and legal certainty.

DIGITALEUROPE: Supports mutual recognition of NIS2 audits to prevent duplicative assessments. Aims to streamline cross-border compliance and reduce burden on organizations.

: Urges mutual recognition mechanisms to provide legal certainty for cross-border services. Seeks predictable, interoperable compliance across jurisdictions.

Adyen: Warns that extraterritorial inconsistencies can advantage competitors abroad. Calls for international alignment to ensure fairness and legal clarity for EU and non-EU actors.

2.2.6 Standards, Certification & Technical Interoperability

This category captures how harmonised technical standards and certification schemes underpin legal certainty and technical interoperability across the EU. Stakeholders call for coherent, sector-aware standardisation that aligns conformity assessment with existing safety frameworks and ensures uniform evaluation of Notified Bodies to prevent market fragmentation. A unified, EU-wide certification framework and full coherence among evolving standards are seen as key to simplifying implementation, reducing ambiguity, and supporting cross-border procurement and compliance. At the same time, progress and governance challenges persist: standardisation is slower than anticipated; horizontal and sectoral rules (e.g., CRA, NIS 2, CSA) overlap; and national add-ons create duplicative documentation and unclear evidence requirements. Many warn against replacing consensus-based harmonised standards with Commission-driven Common Specifications, while emphasizing that standards are voluntary and should not delay compliance. Practical gaps—such as missing product-series concepts and limited operational guidance for complex, multi-stakeholder systems—risk interoperability and consistent conformity assessments; transparent, balanced participation in standard-setting is seen as essential to trust and effectiveness.

Regarding the definition of standards, we call for setting up a unified certification framework in order to simplify implementation by all entities. (GSMA)

Chair of CEN-CENELEC JTC 21, where Euro- pean AI standards to underpin EU regulation are being developed, and Co-chair of the AI risk and accountability work at OECD. ()

It is worth noting that tech industry representatives and consultancy firms linked to them reportedly make up around 55% of the members of the CEN-CENELEC committee drafting the hENs . (Democracy Reporting International (DRI))

CRA does not recognize the concept of a product series. (ANIE Federazione - ANIE ASSIFER)

: Advocates transparent procurement and using reform to require harmonised technical standards, cyber resilience, and vendor diversity, noting European AI standards are being developed to underpin regulation.

The upcoming reform of the Public Procurement Directives should be used to introduce ambitious timelines, effective monitoring me- chanisms, require commitments to adopt harmonised technical

standards, and to ensure a high level of cyber resilience as well as sufficient supply chain and vendor diversity.

Technology Industries of Finland: Opposes Commission-led common specifications, arguing they sideline industry input and should be removed in favor of consensus-based standardisation.

Common specifications are usually solely driven by the Commission, without much opportunity for the industry to contribute to their development.

Volkswagen Group: Warns that standardization of high-risk AI requirements is moving too slowly and seeks clarity on the applicability of AI Act-related standards to certain systems.

The standardization of the high-risk requirements is progressing much more slowly than originally planned.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Highlights overlapping horizontal AI rules with sectoral frameworks that drive duplicative documentation and divergent technical pathways, increasing compliance burdens for startups.

Secondly, applying horizontal AI rules in sectors with already existing legal frameworks (e.g., automotive, medical, machinery, aviation) risks duplicative documentation, strained notified bodies, and divergent technical pathways.

GSMA: Calls for a unified certification framework and coherent standards to reduce ambiguity and simplify implementation across entities.

Regarding the definition of standards, we call for setting up a unified certification framework in order to simplify implementation by all entities.

ANIE Federazione - ANIE ASSIFER: Flags gaps in horizontal guidance that create inconsistent interpretations in complex rail supply chains and notes the absence of a product-series concept undermines interoperability over time.

As a horizontal regulation, CRA does not provide sector-specific or operational guidance for addressing the flexibility expressed through phrases such as "where applicable", "where technically feasible", "unless otherwise agreed", etc.

Bitkom e.V.: Requests clarity on evidence or certifications under NIS-2 and warns that additional national schemes elevate cross-border compliance overhead.

NIS-2 does not clarify which evidence or certification must be provided by Important and Essential Entities, while some member states introduce additional schemes, such as Germany's C5, complicating EU-wide compliance.

BEUC - The European Consumer Organisation: Affirms harmonised standards are voluntary tools and stresses that legal obligations are actionable without waiting for standards.

Harmonised Standards are important tools for operationalising compliance, but they are not a precondition for legal obligations as they are voluntary tools.

Democracy Reporting International (DRI): Cautions that industry-linked members dominate the committee drafting harmonised standards, raising concerns about balance in standard setting.

It is worth noting that tech industry representatives and consultancy firms linked to them reportedly make up around 55% of the members of the CEN-CENELEC committee drafting the hENs .

TEAM-NB: Urges uniform assessment of Notified Bodies to ensure consistency and fairness, warning that shortages risk exacerbating regulatory fragmentation.

To maintain consistency, credibility, and trust in the European regulatory system, it is important to ensure a uniform assessment of Notified Bodies by Member States' Competent Authorities.

Namirial Spa: Criticizes overlapping cybersecurity obligations from CRA, NIS 2, and CSA, calling for consolidation and repeal of obsolete CSA certification provisions.

Repeal obsolete certification provisions of the Cybersecurity Act (CSA) and consolidate cybersecurity compliance within CRA and NIS 2.

The Danish Consumer Council: Reiterates that harmonised standards are voluntary and points to sandboxes and service desks as complementary guidance for compliance.

While harmonised standards are important tools for operationalising compliance, they are not a precondition for legal obligations as they are voluntary.

: Advocates coupling policy with clear technical standards to avoid fragmented implementation, citing prior consent window issues as a cautionary example.

The EU just needs to collaborate on the policy decisions with technical experts, so that we avoid another "consent window flood" due to leaving the "how to implement it" to individual website publishers instead of giving a clear standard along with the policy.

Union of Entreprenuers and Employers: Supports modernising conformity assessment and documentation in a digital-by-default approach while maintaining high safety and consumer protection.

The European Commission's "digital-by-default" approach, reflected in the Omnibus IV and related simplification measures, seeks to modernise conformity assessment and product documentation while maintaining the high safety and consumer protection standards that define the Single Market.

Anitec-Assinform: Critiques shifting from harmonised standards to Commission-driven common specifications that bypass ESO consensus and reduce stakeholder participation.

This bypasses the European Standardization System's consensus-based processes and reduces stakeholder participation.

UNIFE: Calls for mandated sector-specific harmonised AI standards for rail, aligned with existing safety and certification frameworks to avoid duplication.

The European Commission must mandate standardisation organisations to develop sector-specific harmonized standards for AI in rail, in collaboration with other agencies like ERA (European Union Agency for Railways).

American Chamber of Commerce to the EU: Encourages adherence to established EU certification framework processes to preserve coherence and trust.

ANEC: Attributes AI standardisation delays to mismanagement and lack of clarity on drafting, beyond mere technical complexity.

In addition to the technical complexity of the matter, we witness a lack of understanding and awareness as well as obfuscation about what and how standards have to be drafted, coupled to an inefficient management system.

: Urges development of enforceable, architecture-level technical standards to ensure interoperable and reliable implementations.

SEC4AI4SEC: Emphasizes that assurance mechanisms and regulation together strengthen trust in AI systems and their interoperability.

DigitalTrade4.EU: Stresses that the latest versions govern legal validity and that EUTIR strengthens NLF and Digital Product Passport compliance via standardized sector rules and governance.

VDMA - Advancing Europe´s machinery industry: Notes uncertainty caused by missing harmonised standards, impeding consistent conformity and interoperability across machinery.

TÜV-Verband e. V.: Rejects a standards-first approach and argues delays in standardisation are not a valid reason to postpone regulatory compliance.

Confederation of Norwegian Enterprise (NHO): Highlights overlapping certification requirements and mandatory burdens that complicate compliance and cross-border interoperability.

Federation of German Consumer Organisations (vzbv): Promotes the use of codes of conduct and certification schemes to enhance consumer protection and market trust.

Ecommerce Europe: Warns that fragmented standards harm accessibility and interoperability in ecommerce, urging coherent EU-wide approaches.

Association of Netherlands Municipalities: Identifies a certification gap that hinders public procurement of compliant digital solutions by municipalities.

Association of Finnish Cities and Municipalities: Calls for GDPR-related updates including guidance, sandboxes, and certification to improve clarity and interoperability.

Comitato Elettrotecnico Italiano - CEI: Argues common specifications undermine standardisation, risk fragmentation and duplication, and calls to strengthen ESOs' role while addressing delays across both the Commission and ESOs.

Forvis Mazars: Advocates standardizing EU audit methodologies to ensure consistent, interoperable assurance across jurisdictions.

The Center for Countering Digital Hate: Proposes an integrated STAR regulatory framework to unify standards, testing, assurance, and reporting for better interoperability.

Danish Institute for Human Rights: Urges alignment of AI Act requirements with standards while reiterating that harmonised standards remain voluntary tools.

Trans Sped: Seeks review and update of standards that hinder automation, fostering technical interoperability and efficiency.

Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA): Opposes introducing harmonised AI occupational safety and health standards, cautioning against overregulation.

Eurosmart: Calls for a legal framework for common and technical specifications and mandates ISO/IEC 17025 and 17065 for testing and certification.

DIGITALEUROPE: Opposes Commission-imposed uniform standards, favoring industry-led, consensus-based standardisation for interoperability.

AMETIC: Critiques the shift toward common specifications at the expense of harmonised standards and inclusive stakeholder processes.

AI Accountability Lab (AIAL), Trinity College Dublin: Advocates harmonised and approved GDPR consent signals to standardize interoperability across services.

Mistral AI: Supports unified, tiered sustainability standards to enable comparable metrics and interoperable reporting.

Access Now Europe: Argues that delays in standards development justify postponing certain obligations to avoid incoherent implementation.

2.2.7 Consistent Guidance, Transparency & Capacity Building

Stakeholders emphasize the need for consistent, timely, and transparent regulatory guidance paired with capacity-building in competent authorities to deliver legal certainty across the digital rulebook. Regulators should serve as advisors as well as supervisors, issuing high-quality methodological support and practical guides that clarify overlaps among frameworks and align obligations into coherent procedures. Unclear scoping of consultations, vague or delayed guidance, and imprecise reporting expectations create implementation uncertainty, drive up compliance costs, and erode trust. Respondents call for clearer publication standards and

transparency for guidance, precise instructions for reporting, and concrete clarifications on specific requirements (for example, where CE marking information should appear for software). They also encourage standardized, EU-wide approaches that make exceptional access regimes predictable and accountable, reinforcing harmonized application across Member States.

> *They should not only act as supervisory and sanctioning authorities but should also have sufficient capacity to perform an advisory function-that is, to provide methodological support, issue practical guides, and explain the overlaps between individual regulations.* (Seznam.cz, a.s.)
>
> *Our analysis finds again that, as above, the AI Act explicitly acknowledges the existence of these regulations and provides legal mechanisms to efficiently integrate new and old obligations into a single procedure and documentation output, and any uncertainty generated by overlapping systems can be resolved or clarified by guidelines published by competent authorities.* (Centre for Democracy and Technology Europe)
>
> *As stated in Article 30 CRA, "for products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 28 or on the website accompanying the software product".* (Video Games Europe)
>
> *Telefónica also warns against vague exceptional need provisions for government access to commercial data, and advocates for the creation of a clear, transparent and mandatory EU-wide compensation scheme to underpin emergency access requests.* (Telefonica, S.A.)

Video Games Europe: Requests clear, consistent guidance on how CE marking should appear on websites accompanying software, including criteria for what constitutes an 'accompanying' page. Seeks Commission clarification to ensure harmonized implementation.

All these questions should be answered by future guidance, and Video Games Europe stands ready to support in the creation of such guidance.

Telefonica, S.A.: Warns that vague 'exceptional need' provisions for government data access undermine legal certainty. Calls for a clear, transparent, EU-wide compensation scheme to standardize emergency access.

Telefónica also warns against vague exceptional need provisions for government access to commercial data, and advocates for the creation of a clear, transparent and mandatory EU-wide compensation scheme to underpin emergency access requests.

Seznam.cz, a.s.: Stresses the need for well-resourced regulators to provide methodological guidance, practical tools, and interpretative clarity. Notes that delayed or missing materials increase uncertainty and hinder compliance.

They should not only act as supervisory and sanctioning authorities but should also have sufficient capacity to perform an advisory function-that is, to provide methodological support, issue practical guides, and explain the overlaps between individual regulations.

Centre for Democracy and Technology Europe: Finds that overlaps between the AI Act and existing regimes can be efficiently integrated and any uncertainties resolved through competent authorities' guidelines. Emphasizes that concrete guidance can address minor implementation details and enable single procedures.

Our analysis finds again that, as above, the AI Act explicitly acknowledges the existence of these regulations and provides legal mechanisms to efficiently integrate new and old obligations into a single procedure and documentation output, and any uncertainty generated by overlapping systems can be resolved or clarified by guidelines published by competent authorities.

Bolt: Calls for more precise reporting guidance specifying what data points must be shown. Notes that implementation rules lacked clarity on expected disclosures.

Also more precise guidance would be needed in that part what exactly is expected to be reported under those data points, implementation regulation didn't give any guidance on that part what exactly needs to be shown.

Centre for Information Policy Leadership (CIPL): Urges greater transparency in the drafting and publication of regulatory guidance and opinions. Seeks clearer expectations and standards for GDPR-related guidance.

Enhance transparency in the drafting of guidance and opinions.

Democracy Reporting International (DRI): Criticizes the AI Act Call for Evidence as overly broad and lacking specificity about identified implementation challenges. Advocates clearer scoping and disclosure to guide stakeholders effectively.

It also notes that implementation challenges were identified through consultations with stakeholders and Member States but does not specify the nature or extent of these challenges.

Schneider Electric: Highlights that late-issued guidance hampers compliance and legal certainty. Notes that key guidelines were released only when the corresponding requirements took effect.

Guidelines on the definition of AI systems and prohibited AI practices were released the same week the corresponding Al Act requirements became applicable.

Entrust SAS: Argues that regulatory uncertainty leads to inconsistent application, higher compliance costs, and reduced trust. Calls for clearer, consistent guidance to stabilize expectations.

This uncertainty creates inconsistent application, higher compliance costs, and reduced trust.

: Points to a lack of transparency and comparability in financing structures within the digital agenda. Urges more coherent, transparent approaches to reduce burdens and uncertainty.

These structures are fragmented, non-transparent and difficult to compare, both within the EU and between regions.

American Chamber of Commerce to the EU: Notes that current implementation guidance can create uncertainty for businesses. Calls for coherent, timely, and harmonized guidance to support compliance.

European Law Institute: Emphasizes the role of the Commission and delegated acts in specifying database and obligation details. Clear secondary rules are needed to ensure harmonized interpretation and legal certainty.

Bundesministerium für Inneres: Raises concerns about insufficient Member State consultation in developing guidance. Advocates more inclusive processes to improve clarity and buy-in.

Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs (VÖWG): Advocates for clear rules, realistic timelines, and accessible guidance to support public and municipal operators. Predictable processes strengthen capacity and legal certainty.

Confederation of Norwegian Enterprise (NHO): Warns that limited familiarity with the New Legislative Framework among drafters undermines consistent guidance. Calls for capacity building within institutions to improve regulatory quality.

Ecommerce Europe: Flags deadlines set without adequate guidance as a source of uncertainty. Recommends centralized EU guidance and regular consultations to harmonize implementation.

DOT Europe: Supports using guidance to preserve GDPR coherence and avoid regulatory conflicts. Also urges refining DSA transparency templates to clarify expectations.

AI Standards Lab: Advocates prioritizing clear guidance over deregulation to reassure stakeholders. Identifies guidance gaps that drive legal uncertainty and need to be addressed.

The Guild of European Research-Instensive Universities: Warns that legal uncertainty and unclear guidance adversely affect university research. Calls for consistent interpretative support tailored to research contexts.

Association des Constructeurs Européens de Motocycles: Notes that national bodies may seek Commission advice to ensure consistent interpretation. Encourages consultative mechanisms to align guidance across jurisdictions.

European Broadcasting Union: Supports coordinated implementation of the EU digital rulebook with clear, harmonized guidance. Emphasizes transparency and capacity-building for public broadcasters and platforms.

WITNESS: Calls for concrete implementation commitments and compliance tools from regulators to aid adherence. Practical resources and templates can build capacity and consistency.

CSC - IT Centre for Science: Recommends providing tools for regulatory analysis to help organizations understand overlapping obligations. Such resources enhance capacity and consistent compliance.

The Center for Countering Digital Hate: Urges stronger transparency mandates and standards in regulation to improve accountability. Clear disclosure requirements and public reporting support consistent enforcement.

Bocconi University: Warns that regulatory simplification without transparency generates uncertainty. Calls for open processes and explanatory guidance to maintain legal certainty.

Orgalim - Europe's Technology Industries: Asks that guidance and rules explicitly safeguard trade secrets while promoting transparency. Clear limits help companies share information confidently and consistently.

BVMed - Bundesverband Medizintechnologie e.V.: Finds Commission guidance insufficient on the interplay between regulatory frameworks. Requests more detailed, coordinated guidance to prevent contradictions and uncertainty.

Chair in Cyber Policy, University of Luxembourg: Promotes transparent republication and consolidation of legislative reforms for clarity. Accessible legal texts strengthen certainty and ease compliance.

SPMS – Shared Services of the Ministry of Health: Seeks clear, practical guidance to comply with the AI Act in healthcare contexts. Early clarity enables safe deployment and consistent practices.

noyb: Notes a lack of experience with the EU digital acquis among authorities and organizations. Calls for capacity building and consistent guidance to close the expertise gap.

INVERCO: Highlights the absence of harmonized AI guidance across the EU. Calls for coordinated, EU-wide interpretative materials to ensure consistent application.

Ada Lovelace Institute: Supports clear, comprehensible digital rules and guidance to protect rights while enabling innovation. Emphasizes transparent, accountable implementation.

SaferAI: Advocates for accessible resources, standards, and guidance to help organizations comply. Resourcing standards development and outreach builds capacity and certainty.

2.2.8 Harmonized Implementation, Supervision & Enforcement

Stakeholders converge on the need for consistent, EU-wide implementation, supervision, and enforcement of digital regulations to avoid fragmentation, legal uncertainty, and duplicative burdens. Across files such as NIS2, eIDAS, DORA, and the CRA, they report divergent national transpositions, varied supervisory practices, differing reporting thresholds, and overlapping obligations that delay deployment, raise costs, and create an uneven Single Market. To restore legal certainty and interoperability, they call for uniform timelines and scope, convergent supervisory practices, shared Level 2 standards and guidance, and mechanisms like One-Stop-Shop or country-of-origin that are applied consistently. Proposals include centralizing the development of concrete use cases, defining minimum contractual terms, coordinating NCAs, simplifying sectoral frameworks, and

avoiding asymmetric regulation. At the same time, several caution that harmonization must balance central coordination with local agility and should not be postponed, given the risks of delay and further divergence.

> *Divergent implementation and enforcement across EU Member States further compound legal uncertainty, delay deployment, and divert resources from innovation and patient care.* (Zimmer Biomet)
>
> *The transposition and application of NIS-2 across EU member states lacks uniformity in timelines, scope and requirements, creating legal uncertainty and additional burdens for companies.* (Bitkom e.V.)
>
> *The One Stop Shop Principle included in NIS2 risks not delivering expected outcomes for the Digital Single Market, due to different interpretations applied by Member States.* (Amazon)
>
> *Mandatory adoption across Member States to avoid fragmentation; voluntary adoption would leave Europe with fragmented systems and undermine cross-border interoperability.* (Entrust SAS)

TIC Council: Warns against delaying CRA implementation, urging timely, uniform rollout to safeguard legal certainty and consistent enforcement.

> *TIC Council warns against the risks of postponing the implementation of the Cyber Resilience Act (CRA).*

Zimmer Biomet: Highlights how divergent national implementation and enforcement create legal uncertainty, delay deployment, and divert resources, calling for harmonized rules.

> *Divergent implementation and enforcement across EU Member States further compound legal uncertainty, delay deployment, and divert resources from innovation and patient care.*

Volkswagen Group: Warns that a directive could result in 27 divergent national regimes, stressing the need for harmonized transposition and consistent obligations.

> *Moreover, since this is a directive, a worst-case scenario could be 27 different national implementations, each with varying obligations.*

eco - Verband der Internetwirtschaft e.V.: Notes that relevant EU measures are adopted and pending or nearing national implementation, underscoring the need for coordinated, timely and coherent transposition to ensure consistency.

> *However, it should be noted that the measures concerned are EU legal acts that have already been adopted and are either still pending implementation in the Member States or are nearing completion.*

ALFI - Association of the Luxembourg Fund Industry: Recommends defining a minimum set of contractual conditions alongside DORA Level 2 to drive convergence and consistent application across Member States.

> *Such a minimum set of contractual conditions should be set alongside with DORA Level 2 regulatory elements, to ensure convergence and consistency across the board.*

Dun & Bradstreet: Highlights how a national data protection decision introduced divergent limits, pointing to the need for EU-wide harmonization and predictable enforcement.

> *For example, the recent decision by the Spanish Data Protection Authority (AEPD) has introduced significant limitations on the processing of sole trader information.*

Intesi Group: Points out divergent national interpretations of eIDAS that fragment the trust services market, calling for harmonized implementation and supervision.

> *National authorities interpret and apply the eIDAS Regulation differently, leading to a fragmented and uneven European trust services market.*

European Tyres and Rubber Manufacturers' Association: Stresses the need for consistent application of horizontal data laws across Member States to ensure legal certainty and a level playing field.

ETRMA stresses the importance of ensuring consistent application of existing horizontal data legislation across Member States.

GSMA: Warns that NIS2's flexible classifications enable inconsistent interpretations, urging clearer, harmonized guidance and enforcement.

NIS2's flexibility in sector and entity classification leads to inconsistent interpretations.

Bitkom e.V.: Reports non-uniform NIS2 transposition and application across the EU, creating legal uncertainty and extra burdens for companies.

The transposition and application of NIS-2 across EU member states lacks uniformity in timelines, scope and requirements, creating legal uncertainty and additional burdens for companies.

Amazon: Cautions that NIS2's One-Stop-Shop may fail without harmonized Member State interpretations, risking fragmentation of the Single Market.

The One Stop Shop Principle included in NIS2 risks not delivering expected outcomes for the Digital Single Market, due to different interpretations applied by Member States.

ENGIE: Describes costly, complex implementation due to overlapping legislation, unclear definitions, inconsistent processes across Member States, and complex national governance, urging streamlined, harmonized approaches.

Nevertheless, its implementation is proving increasingly challenging and costly as a result of the proliferation and overlap of legislation and consequent reporting obligations; unclear and generic definitions not suited for the specific energy use-cases; lack of process consistency across pieces of legislation and Member States; and complex governance at national level.

Leading Baltic tech and other businesses and professional associations listed in the submission: Argues that limited adjustments do not resolve structural and interpretative divergences, undermining consistent application of data protection rules and competitiveness.

The adjustment remains limited in scope and does not yet address the broader structural and interpretative challenges that continue to affect innovation, competitiveness, and the consistent application of data protection rules across the EU.

Evotrust: Emphasizes that divergent eIDAS interpretations by national authorities fragment the trust services market, calling for harmonized implementation and oversight.

National authorities interpret and apply the eIDAS Regulation differently, leading to a fragmented and uneven European trust services market.

Meta Platforms Ireland Limited: Critiques a fragmented enforcement setup with varying regulators and no OSS or country-of-origin principle, calling for coherent supervision to reduce compliance complexity.

The fragmented enforcement landscape, where either both DPAs or telecom regulators are involved depending on the Member State and without any OSS mechanism or country-of-origin principle, further complicates compliance and increases cost

Adigital (Asociación Española de la Economía Digital): Welcomes EU-wide harmonisation paired with substantial simplification of sectoral rules to improve coherence, enforceability and legal certainty.

European-wide rule harmonisation is welcome, but should be accompanied by significant simplification of the sectoral framework.

Entrust SAS: Advocates mandatory, EU-wide adoption to prevent fragmentation and ensure cross-border interoperability and consistent implementation.

Mandatory adoption across Member States to avoid fragmentation; voluntary adoption would leave Europe with fragmented systems and undermine cross-border interoperability.

FiCom ry: Urges the Commission to avoid asymmetric regulation that fragments the digital market and undermines consistent enforcement.

The European Commission must avoid creating asymmetric regulation, as it fragments the digital market.

Union of Entreprenuers and Employers: Notes differing reporting thresholds lead to inconsistent application across Member States, calling for harmonized criteria and oversight.

In addition, different reporting thresholds based on service type, number of users affected, or perceived impact have resulted in inconsistent application across Member States.

WKÖ - Austrian Federal Economic Chamber: Calls for centralized development of specific use cases with national authority involvement and stakeholder input to ensure coherent implementation.

The development of these specific use cases should be centralized, with close involvement of the relevant national authorities and repeated stakeholder consultations.

European Associations of Co-operative Banks (EACB): Highlights divergent interpretations of reporting requirements among NCAs, urging harmonized guidance and supervisory convergence.

There are currently varied interpretations of reporting requirements among NCAs.

ACEA (European Automobile Manufacturers' Association): Calls to reform the fragmented supervisory structure to reduce legal uncertainty and ensure consistent enforcement across Member States.

Finally, this framework should bring about a reform of the fragmented supervisory structure that has led to legal uncertainty and inconsistent enforcement across Member States.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Advocates balancing centralization for harmonization and economies of scale with local agility to adapt to innovation and market conditions.

However, there is a delicate balance to be struck between a more central- ized approach, which could limit local ability to respond quickly to changing market conditions or tech- nological innovation, and the need to achieve large economies of scale, which are important for the introduction of new technologies.

: Finds that while progress is being made, it remains fragmented, indicating a need for stronger harmonization in implementation and oversight.

Benchmark 2025 shows that progress is real, but fragmented.

2.2.9 Streamlined Compliance, Reporting & Contracting

This category captures a broad call to make compliance, reporting, and contracting across the EU's digital rulebook more coherent and predictable without weakening protections. Stakeholders highlight that the proliferation and fragmentation of frameworks (e.g., GDPR, NIS2, DORA, CRA, AI Act) creates overlapping, duplicative, and sometimes conflicting obligations—divergent formats, thresholds, templates, and timelines—that shift resources from real risk mitigation to administrative overhead. Duplication between assessments (such as DPIA and FRIA) and inconsistent national registration/notification practices further undermine the one-stop-shop principle and slow incident response. Proposed remedies focus on harmonization and practical tooling: a single EU reporting gateway/one-stop-shop with aligned thresholds, templates, and timelines; clear guidance to avoid duplicated assessments; and use of instruments like a Digital Omnibus to streamline implementation while preserving safety, security, and fundamental rights. In contracting, stakeholders seek enforceable standard clauses and model licenses to rebalance negotiations with ICT providers, improve legal certainty, and clarify obligations under the Data Act (including avoiding destabilizing termination rights). Centralized, up-to-date compliance information on third-party providers would further reduce burdens and foster adoption, delivering streamlined compliance with high standards of trust and security.

Indeed, the proliferation of EU cybersecurity regulations has resulted in substantial complexity and overlapping requirements, often diverting organizational resources from genuine security enhancement toward compliance administration. (FERMA - Federation of European Risk Managers Associations)

prime example is inci- dent reporting: DORA, the General Data Protection Regulation (GDPR), the Cyber Resilience Act (CRA), and the AI Act each impose reporting obligations, but differ in format, scope, and content. (German Insurance Association)

For example, NIS2 (Article 23) requires an initial report within 24 hours, eIDAS2 (Article 19) mandates a detailed report in the same timeframe, and GDPR (Article 33) calls for an initial report within 72 hours. (Evotrust)

This would threaten the sustainability of these business models, particularly for AI companies, which could lead to losses due to high upfront investments in areas such as development and training. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

: Calls for strong oversight coupled with streamlined national frameworks and removal of bureaucratic bottlenecks to speed digital sector deployment.

Introducing strong regulatory over- sight, streamlining national frameworks and eliminating bureaucratic bottlenecks, such as permit delays, is es- sential for the electrification of key digital sectors.

FERMA - Federation of European Risk Managers Associations: Warns that proliferating and overlapping EU cyber rules create administrative complexity that shifts resources from real security to compliance tasks, urging simplification.

Indeed, the proliferation of EU cybersecurity regulations has resulted in substantial complexity and overlapping requirements, often diverting organizational resources from genuine security enhancement toward compliance administration.

TIC Council: Urges using a Digital Omnibus to streamline reporting and implementation across laws, cutting admin burdens while preserving safety and security.

By following the recommendations outlined in this paper-streamlining reporting, accelerating CRA and Al Act compliance, designating notifying authorities and supporting them, and ensuring secure and compliant digital identification-the EU can simplify processes while maintaining high standards for safety, security, and trust in the digital economy.

: Highlights how non-harmonized incident thresholds force duplicative assessments and slow, multi-rule notifications, calling for aligned criteria.

The lack of clear and harmonized thresholds across different regulations forces teams to examine each incident from multiple angles, which makes the qualification phase more cumbersome.

ALFI - Association of the Luxembourg Fund Industry: Advocates enforceable minimum ICT contractual clauses to level bargaining power and provide legal certainty in negotiations with third-party providers.

With regards to contractual conditions between financial entities and ICT third-party providers, we would see merit in the Guidelines providing a set of minimum standard clauses, applicable to ICT TPSPs (and ICT TPSPs supporting CIFs specifically), so that such clauses would set a common ground for contractual conditions (re-)negotiations with ICT TPSPs and clarify the respective responsibilities and duties.

Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique: Seeks clear guidance to avoid duplicative GDPR DPIA and AI Act FRIA processes, simplifying compliance without deregulating.

The overlapping scopes of fundamental rights impact assessments (FRIA) under the GDPR and the fundamental Rights Assessment (FRAs) under the AI Act can result in duplicative processes and conflicting compliance obligations.

German Insurance Association: Notes fragmented, inconsistent reporting and governance obligations across DORA, GDPR, CRA and the AI Act, urging alignment to reduce burden.

prime example is inci- dent reporting: DORA, the General Data Protection Regulation (GDPR), the Cyber Resilience Act (CRA), and the AI Act each impose reporting obligations, but differ in format, scope, and content.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Raises contracting concerns that Data Act termination rights could destabilize long-term SaaS agreements and undermine sustainable AI business models.

Due to the lack of a clear definition in Art. 2 of the Data Act, the short-term termination rights granted regardless of contract length could undermine long-term SaaS contracts.

Siinda: Recommends standard contractual clauses for balanced, legally certain data exchanges covering liability, re-use, trade secrets, and termination.

Provide standard contractual clauses covering liability, permitted re-use, trade-secret protection, and termination rights to ensure balanced and legally certain exchanges.

Bitkom e.V.: Requests clearer, more flexible Data Act contractual requirements and compatibility with other clauses to ease compliance.

Regarding the contractual requirement under Article 4(13) DA, the language and scope are unclear.

ENGIE: Proposes an EU one-stop-shop portal consolidating provider compliance information to cut deployer burden and increase certainty under the AI Act.

In cases when companies rely on third-party providers, the creation of a "one-stop-shop" at EU level serving as a single portal regularly updated collecting relevant information regarding the providers' compliance with the Al Act would greatly reduce the administrative burden for deployers, foster certainty in compliance and eventually support AI adoption.

European Tech Alliance: Asks for pan-EU clarity so marketplaces register/notify only their main country of establishment, avoiding multi-state duplication.

It would be good to have clarity in the regulation that for online marketplaces, both registration and notification would always only be to the competent authority of the main domicile / country of establishment.

Ibec: Calls to rationalize overlapping transparency and risk reporting duties, noting some companies face eight duplicative submissions.

Certain companies must submit 8 different overlapping reporting obligations.

Evotrust: Points to conflicting cross-regime incident timelines that complicate compliance for QTSPs, recommending alignment.

For example, NIS2 (Article 23) requires an initial report within 24 hours, eIDAS2 (Article 19) mandates a detailed report in the same timeframe, and GDPR (Article 33) calls for an initial report within 72 hours.

Adigital (Asociación Española de la Economía Digital): Supports making compliance more efficient by eliminating redundancies, contradictions, and disproportionate requirements across sectoral digital laws.

On the contrary, it is about making regulatory compliance more efficient, eliminating redundancies, contradictions, and disproportionate requirements that do not add real value to the objectives pursued.

Union of Entreprenuers and Employers: Promotes rationalization of digital rules via a single reporting gateway with harmonized templates and timelines that cut burden while maintaining effectiveness.

A single digital reporting gateway coordinated through ENISA, supported by harmonised templates and timelines such as an initial notice within 24 hours and a final report within 72 hours, would make incident management more efficient while maintaining security standards.

Anitec-Assinform: Seeks to restore a one-stop-shop approach and remove fragmentation and cliff-edge effects that raise administrative burdens, especially for SMEs.

This undermines the One Stop Shop principle and creates unnecessary administrative burden.

American Chamber of Commerce to the EU: Encourages streamlining and clarifying EU data rules to reduce overlaps and provide predictable, efficient compliance pathways.

Swisscom IT Services Finance S.E.: Highlights burdens from fragmented reporting obligations and advocates consolidation and harmonization to ease compliance.

Uber B.V.: Notes overlapping and duplicative reporting across EU, national and sector levels, urging alignment to avoid double reporting.

German Property Federation: Urges standardized data processing agreement templates to increase legal certainty and reduce negotiation burdens.

Bundesministerium für Inneres: Observes that separate regimes and frameworks impede timely incident reporting; calls for better coordination and simplification.

Test and Measurement Coalition: Flags overlapping obligations that generate redundant reports, advocating streamlined, interoperable requirements.

VDMA - Advancing Europe´s machinery industry: Calls to streamline and better align Articles 4 and 5 obligations to reduce complexity and ensure consistent application.

SOK: Warns that multi-authority reporting creates inefficiency and confusion; recommends single-channel or coordinated reporting.

BusinessEurope: Advocates harmonized templates, definitions and reporting channels to minimize duplication and compliance costs.

Confederation of Norwegian Enterprise (NHO): Reports fragmented supervisory questionnaires leading to duplicative reporting; calls for consolidation and reuse of information.

CENTR - Council of European Top Level Domain Registries: Opposes duplicative oversight and reporting layers that burden registries, urging reliance on existing mechanisms.

: Expresses cautious support for streamlining measures that cut red tape while safeguarding core objectives.

ENTSO-E: Supports harmonized reporting across instruments while preserving effective sectoral frameworks and avoiding double obligations.

DOT Europe: Urges harmonized thresholds and reduced reporting frequency to lessen administrative load without undermining oversight.

Association des Constructeurs Européens de Motocycles: Calls for EU-wide, sector-tailored reporting criteria with implementing acts that specify obligations to avoid duplication.

secunet Security Networks AG: Notes cross-border fragmentation in reporting that burdens operators; seeks coherent EU-level processes.

European Fund and Asset Management Association (EFAMA): Warns of overlapping obligations and duplication risks, and proposes enforceable standard ICT contract terms to boost legal certainty.

E.ON SE: Advocates streamlined incident reporting and uniform regulation to simplify compliance across jurisdictions.

Chair in Cyber Policy, University of Luxembourg: Recommends clear guidance and aligned reporting requirements to make compliance feasible and consistent.

Association of German Cities: Calls for more feasible, simplified obligations and the avoidance of duplicative processes for municipalities and public services.

CIO Platform Nederland: Urges regulators to prevent overlapping rules and excessive burden by aligning requirements across frameworks.

SPMS – Shared Services of the Ministry of Health: Argues that overlapping regulations hamper operational efficiency; seeks coherent, simplified compliance pathways.

OpenSSF: Calls for a single EU reporting pathway for security incidents to reduce fragmentation and speed coordinated response.

INVERCO: Supports enforceable standard contractual conditions to streamline third-party ICT agreements and ensure clarity of responsibilities.

European Savings and Retail Banking Group: Highlights overlaps between sectoral and horizontal reporting and notes ongoing review of ECB requirements; calls for harmonization.

Danish Industry: Points to overlapping obligations and misaligned notification timelines that complicate compliance, urging alignment.

Wolt: Warns that fragmented compliance regimes degrade user experience and slow innovation; advocates harmonized, predictable rules.

AMETIC: Recommends harmonizing NIS2 and CRA reporting to avoid duplication and conflicting requirements.

OpenAI: Supports harmonizing duplicate reporting burdens across EU instruments to enable efficient, non-redundant compliance.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Endorses a one-stop principle for overlapping digital laws to streamline compliance and enforcement.

Ada Lovelace Institute: Urges caution in removing duplications to ensure necessary safeguards remain while still simplifying compliance.

Council of European Municipalities and Regions (CEMR): Asks for clear, simplified legislation for local services with minimized duplication and straightforward reporting.

2.2.10 Miscellaneous

This “Miscellaneous” set under Harmonized Regulation and Legal Certainty underscores Europe’s regulatory tradition and rule-of-law as strategic assets for competitiveness and trust. It converges on the need for coherent, harmonized frameworks that deliver predictability and accountability, including strict adherence to GDPR, AI, and DLT regimes, while anticipating targeted legislative updates to sustain legal certainty across sectors. Contributors caution against rushed or omnibus approaches that risk incoherence, favoring purpose-built instruments and, where consensus is lacking, withdrawal or redesign of proposals to avoid undermining original objectives. They call for robust safeguards for intellectual property and trade secrets, stronger consumer protections where current rules fall short, and comprehensive regulatory options for harmful digital content. The throughline is that trust, innovation, and digitalisation are enabled by clear, enforceable rules—whereas deregulation threatens both industry resilience and public interest.

> *Yet the EU has within its grasp all the key ingredients to reverse this trajectory: a vast internal market, a highly skilled workforce, world-class research institutions, and a strong regulatory tradition.* ()

> *Considering that co-legislators have not yet agreed on appropriate solutions to overcome contentious key provisions, we recommend withdrawing FIDA's proposal.* (Unipol Assicurazioni S.p.A.)

We believe that without significant amendments, the regulation could hinder the achievement of its original objectives. (Unipol Assicurazioni S.p.A.)

: The document frames the EU's strong regulatory tradition as a strategic asset that can underpin harmonized rules and legal certainty to reverse decline.

Yet the EU has within its grasp all the key ingredients to reverse this trajectory: a vast internal market, a highly skilled workforce, world-class research institutions, and a strong regulatory tradition.

Unipol Assicurazioni S.p.A.: The submission urges withdrawing the FIDA proposal unless significantly amended, arguing current provisions risk missing objectives and undermining a coherent, workable framework.

Considering that co-legislators have not yet agreed on appropriate solutions to overcome contentious key provisions, we recommend withdrawing FIDA's proposal.

Government Office of the Czech Republic: It recommends addressing contentious issues via the forthcoming Digital Networks Act rather than an omnibus process to enable deeper debate and clearer, more legally certain outcomes.

Nonetheless, we believe that certain aspects of this directive will be revisited within the framework of the proposed Digital Networks Act (DNA), where there will be greater room for in-depth discussion than within the scope of the digital omnibus.

FEDIL, the Voice of the Luxembourg's Industry: Industry advocates stronger trade secret protections within regulatory initiatives to safeguard competitiveness while enabling compliant data use and legal certainty.

DigitalTrade4.EU: The group stresses strict adherence to GDPR, AI, and DLT rules and overall EU regulatory compliance to ensure harmonization and predictable legal environments.

Bundesministerium für Inneres: The ministry anticipates that implementing proposals will require legislative changes and calls for early clarity to support legal certainty and effective enforcement.

European Banking Federation: Banks call for safeguarding intellectual property in any deregulatory moves to maintain innovation incentives and legal certainty across the single market.

Federation of German Consumer Organisations (vzbv): Consumer advocates argue existing laws are insufficient and urge stronger limitations and clearer, harmonized rules to protect consumers and provide certainty.

epicenter.works - for digital rights: It argues that trust—and thus successful digitalization—rests on clear, enforceable regulation that delivers legal certainty for users and providers.

The Center for Countering Digital Hate: The organization proposes comprehensive regulatory options to tackle online harms, emphasizing robust, harmonized rules that provide clarity and certainty.

Bocconi University: Scholarly input stresses preserving the rule of law in AI governance through clear frameworks that ensure accountability and legal certainty.

Access Now Europe: The NGO warns that deregulation would harm European industry and competitiveness, advocating strong, predictable regulation to anchor legal certainty.

2.3 Enforcement, Oversight and Accountability

Effective, harmonised, and timely enforcement—anchored by well-resourced, technically competent, and independent authorities—delivers legal certainty and deters persistent non-compliance. Stakeholders prioritise uniform guidance, EU-level coordination, and market surveillance, with standards developed in parallel to implementation rather than delaying action. Regulators need deep AI and cybersecurity expertise, structured training, and strong, well-defined powers (audits, interim measures, exceptional access to technical artifacts) while safeguarding independence and avoiding burden shifts to under-resourced public bodies. Clear governance and role clarity enable joint investigations, information-sharing, and consumer redress across

domains; avoiding over-centralisation and using machine-readable reporting and feedback loops prevents bottlenecks. Trust depends on independent, conflict-free oversight, proportionate safeguards, and tamper-proof traceability insulated from political interference and subject to judicial review. Accountability is reinforced by inclusive participation of local authorities and civil society, registers and comparable reporting, immutable audit trails, and proportionate, risk-based continuous monitoring. Enforcement architecture should close exemptions and blind spots, assign responsibilities across the value chain, empower cessation orders and deterrent fines, and provide accessible whistleblowing and collective redress. Cross-border coherence requires stronger EU27 networks, fixes to one-stop-shop weaknesses, adapted customs/product safety for direct-to-consumer imports, and scrutiny of non-EU platforms without geopolitical misuse. Across sub-categories, coordinated, evidence-based supervision with clear mandates, interoperable reporting, and proportionate checks dominates. Building capacity, independence, and transparency aligns enforcement with fairness, rights protection, and competitiveness.

2.3.1 Governance, Coordination, Jurisdiction & Role Clarity

Governance, Coordination, Jurisdiction & Role Clarity synthesizes calls for clear mandates and harmonized enforcement across the EU's digital and AI rulebook. Stakeholders urge early, structured engagement among EU-level bodies and a lead coordinating role to align supervision across Member States, backed by formal cooperation channels among data protection, competition, consumer, telecom, and new AI regulators. Joint investigations and information-sharing are emphasized to handle cross-domain issues and deliver deterrent enforcement and easier consumer redress, mirroring GDPR's enforcement model and DPA competencies. At the same time, fragmentation and ambiguous oversight show the difficulty of assigning a single regulator to multi-chapter, multi-domain regulations, making role clarity and sector-specific expertise essential. Several insights caution against over-centralization of adaptive capacity in the European Commission: reliance on Commission discretion without real-time monitoring, machine-readable reporting, and structured feedback loops creates bottlenecks and slows responsiveness. Remedies proposed include clearer allocation of responsibilities between EU and Member State authorities, hybrid oversight arrangements, and practical guidelines that define reporting lines and cooperation triggers to ensure efficient, accountable enforcement.

> *As regards the AI Act, the EU's new AI Office should take a lead role in harmonising the Regulation's enforcement across Member States, akin to how the European Data Protection Board (EDPB) coordinates the GDPR supervision.* (Technology Industries of Finland)
>
> *As the regulation is structured in chapters that each address very different domains, assigning a single regulator with the expertise and authority to oversee the entire regulation proves challenging.* (Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique)
>
> *This centralization breeds bottlenecks and delays; without structured feedback loops, rules risk obsolescence within months.* ()
>
> *Second, adaptive capacity sits almost entirely in the Commission.* ()
>
> **CNIL (French Data Protection Authority):** Urges the Commission to engage the EDPB/EDPS early to clarify scope and ensure coordinated oversight for rules affecting privacy and rights. This upstream coordination would strengthen governance and role clarity.
>
> *We encourage the Commission to engage in upstream, informal exchanges with the EDPB on the scope and content of the text and, when appropriate, ask for a joint EDPB/EDPS opinion on it, given its implications on privacy and rights (art. 42.2 EUDPR).*
>
> **Technology Industries of Finland:** Calls for a cohesive, harmonised AI enforcement architecture led by the EU AI Office. Stresses formal cooperation, joint investigations and information-sharing among data, competition and consumer regulators.
>
> *As regards the AI Act, the EU's new AI Office should take a lead role in harmonising the Regulation's enforcement across Member States, akin to how the European Data Protection Board (EDPB) coordinates the GDPR supervision.*
>
> **Luxembourg, Ministère d'État, Service des médias, de la connectivité et de la politique numérique:** Notes that the regulation spans disparate domains, making it difficult to assign a single regulator with sufficient expertise and authority. Points to a need for multi-competent or coordinated oversight.

As the regulation is structured in chapters that each address very different domains, assigning a single regulator with the expertise and authority to oversee the entire regulation proves challenging.

BEUC - The European Consumer Organisation: Supports aligning enforcement with the GDPR by empowering DPAs for e-Privacy and ensuring strong redress. Urges deeper cooperation and information-sharing among DPAs and other sectoral authorities.

BEUC welcomes that Chapters IV and V of the proposed Regulation mirror the enforcement and redress system under the GDPR and that competence for the enforcement of the e- Privacy Regulation is allocated to the Data Protection Authorities (DPAs).

: Criticises excessive reliance on Commission discretion and centralised adaptive capacity that creates governance bottlenecks. Calls for structured, real-time feedback loops to keep oversight responsive.

This centralization breeds bottlenecks and delays; without structured feedback loops, rules risk obsolescence within months.

Bündnis F5: AlgorithmWatch, Gesellschaft für Freiheitsrechte, Open Knowledge Foundation, Reporter ohne Grenzen, Wikimedia Deutschland: Emphasises the need to define clear responsibilities and lines of authority among regulators to enable effective enforcement. Clarity on mandates would reduce overlap and gaps.

ENSHPO - The European Network of Safety and Health Professional Organizations: Warns that ambiguous oversight roles create uncertainty and heighten liability risks for actors subject to enforcement. Calls for clearer allocation of duties and accountability.

European Law Institute: Highlights that enforcement powers remain primarily with Member States, requiring clear jurisdictional boundaries and coordination with EU-level bodies. Consistent cooperation mechanisms are needed.

DigitalTrade4.EU: Advocates a hybrid, ESMA-like coordination model to align national and EU supervision. This would strengthen cross-border consistency and reduce fragmentation.

Polish Confederation Lewiatan: Flags fragmented enforcement due to overlapping EU groups and committees. Recommends streamlining governance structures and clarifying mandates to avoid duplication.

ITI - Information Technology Industry Council: Identifies administration, oversight and guidance gaps that hinder consistent application. Seeks clearer role definitions and practical guidance for authorities and regulated entities.

DOT Europe: Calls for more flexible VLOP/VLOSE designation with transparent role allocation among authorities. Better coordination would improve predictability and oversight effectiveness.

Verband der Automobilindustrie e.V.: Warns that fragmented, multi-level enforcement undermines consistency and compliance. Urges stronger coordination and clearer division of responsibilities.

Association des Constructeurs Européens de Motocycles: Notes that dispersed oversight responsibilities impede coherent enforcement. Recommends well-defined coordination channels and jurisdictional clarity.

WITNESS: Stresses the importance of clearly assigned oversight responsibilities and accountability lines. This prevents enforcement gaps and strengthens governance.

Computer & Communications Industry Association (CCIA Europe): Highlights fragmented oversight and uneven enforcement across jurisdictions. Calls for harmonised governance and enhanced inter-agency cooperation.

ECIS, European Committee for Interoperable Systems: Argues that fragmented oversight mandates reduce efficiency and legal certainty. Urges consolidation or tightly coordinated mechanisms across competent authorities.

: Proposes guidelines to clarify authority roles, cooperation procedures and reporting obligations. Such guidance would enhance coordination and accountability.

2.3.2 Regulatory Capacity, Powers & Resources

This category highlights that effective enforcement of the AI framework hinges on regulators' capacity, powers, and resources. Authorities require deep technical expertise in AI, cybersecurity, and full product lifecycles, supported by clear, harmonised guidance and structured, ongoing training—potentially via EU-wide certification—to keep pace with fast-evolving technologies. EU-level coordination (e.g., ENISA guidance, EDIB subgroups) and evidence-based oversight tools are needed to ensure consistent supervision across Member States. Cooperation and access arrangements among data protection, equality, and human rights authorities—as well as clear designation and readiness of notified bodies—are critical to closing gaps and preventing regulatory elusion. Resourcing is a persistent concern: both national authorities and the EU AI Office need sufficient staffing and funding, and current plans are viewed as inadequate. Policymakers should prioritise enforcement while avoiding administrative burden shifts onto already under-resourced public and local authorities, and they must safeguard the independence of regulators. Strong, well-defined powers—spanning audit rulemaking, interim measures, and, in exceptional circumstances, access to sensitive technical artifacts like source code—are seen as necessary to deter bad actors, ensure accountability, and avoid underregulation stemming from overly permissive guidance.

> *Market surveillance authorities, which will monitor compliance with the AI Act, will need to have staff with in-depth technical knowledge, not only of AI but also of cybersecurity in general.* (FERMA - Federation of European Risk Managers Associations)
>
> *National authorities should be provided clearer guidance and expert assistance to oversee compliance.* (Technology Industries of Finland)
>
> *Articles 74(13) and 92(3) grant market surveillance authorities or the Commission the right to access the source code of AI systems.* (Ibec)
>
> *The planned staffing level of 140 employees, of which only 30 are to monitor the implementation of the law from December 2024, appears insufficient for this and must be increased to 200 by 2025.* (WKÖ - Austrian Federal Economic Chamber)

FERMA - Federation of European Risk Managers Associations: Calls for regulators to be equipped with deep technical expertise in AI and cybersecurity and harmonized guidance to enable efficient, consistent supervision.

> *Market surveillance authorities, which will monitor compliance with the AI Act, will need to have staff with in-depth technical knowledge, not only of AI but also of cybersecurity in general.*

City of Stockholm: Warns that an industry-centric approach shifts administrative complexity and costs onto public sector authorities, straining local regulatory capacity.

> *It should also be noted that the Commission's primarily focus on the needs of industry may unintentionally shift administrative complexity and workload onto public sector organisations.*

Technology Industries of Finland: Urges clearer guidance, thematic cooperation structures, and joint training to build regulators' capacity to oversee compliance amid fast-evolving technologies.

> *Additionally, invest in joint training programmes to equip regulators with required knowledge, allowing them to keep up with fast-evolving technologies.*

Ibec: Raises concern about broad powers granting authorities or the Commission access to AI source code, highlighting implications for oversight scope and confidentiality.

> *Articles 74(13) and 92(3) grant market surveillance authorities or the Commission the right to access the source code of AI systems.*

Schneider Electric: Advocates staffing market surveillance bodies with skilled regulators and establishing EU-wide certification to strengthen consistent enforcement maturity.

> *Market surveillance bodies should be staffed with skilled and mature regulators with industry and product/system level expertise covering the whole lifecycle of a high-risk AI systems (including a*

practical understanding of complete product architecture (AI and non-AI interactions), design and development, as well as prelaunch phases).

WKÖ - Austrian Federal Economic Chamber: Argues the EU AI Office needs significantly more staff to provide appropriate oversight, with planned levels deemed insufficient and specific increases proposed.

The planned staffing level of 140 employees, of which only 30 are to monitor the implementation of the law from December 2024, appears insufficient for this and must be increased to 200 by 2025.

SEC4AI4SEC: Calls for evidence-based oversight tools to enhance regulators' capacity to assess and enforce AI risks effectively.

European Law Institute: Supports empowering the Commission to set audit rules to standardize and strengthen oversight mechanisms across the EU.

Bundesministerium für Inneres: Warns against shifting burdens to authorities without adequate resourcing, emphasizing balanced responsibilities in enforcement.

European Public Service Union: Notes regulators are underfunded and lack resources, urging investment to enable effective enforcement and accountability.

Federation of German Consumer Organisations (vzbv): Emphasizes prioritising enforcement, closing regulatory gaps, and properly resourcing data protection authorities to protect consumers.

AI Standards Lab: Critiques under-regulation in guidelines that may embolden bad actors and calls to enhance the AI Office's rights and resources for robust enforcement.

ENNHRI - European Network of National Human Rights Institutions: Urges safeguarding the powers and roles of human rights authorities to ensure effective oversight of AI impacts on rights.

WITNESS: Calls for robust expert enforcement capacity, ensuring regulators have the skills and resources to act effectively.

AK Wien: Demands adequate funding for data protection authorities to handle new AI oversight responsibilities.

The Center for Countering Digital Hate: Advocates empowered, independent regulatory enforcement to curb AI harms, stressing strong mandates and resources.

European Digital Rights (EDRi): Warns that simplification measures risk overloading already under-resourced authorities, undermining effective oversight.

Clever Cloud: Urges preserving regulators' capacity to impose interim measures, maintaining swift protective enforcement powers.

Open-Xchange AG: Calls to empower institutions with sufficient authority and tools to prevent elusion and ensure compliance.

European network of equality bodies (Equinet): Seeks strong access to information and cooperation mechanisms for equality bodies to enforce AI-related obligations.

DIGITALEUROPE: Highlights gaps in notified body designation under the AI Act, urging clarity and capacity to support conformity assessment.

AI Accountability Lab (AIAL), Trinity College Dublin: Warns that under-resourced authorities face new burdens and calls for EU-level resourcing and empowerment to meet enforcement demands.

: Stresses the need to resource enforcement functions to oversee the AI Act effectively.

2.3.3 Enforcement Strategy, Timeliness & Uniformity

This category foregrounds enforcement as a strategy: prioritising consistent, harmonised, and timely application of existing rules over reopening or diluting them. Stakeholders call for clear, uniform guidance and stronger EU-level coordination to prevent fragmentation, alongside robust oversight and market surveillance (including for self-certified Class I devices and notified bodies). Aligning enforcement regimes and updating interpretative guidance are seen as crucial to deliver legal certainty and fair competition across Member States. Timeliness is critical: postponements to the AI Act or enforcement windows are framed as harmful—exposing people to risks, creating legal uncertainty, and weakening the EU's credibility as a rule-setter. Standards and guidelines should be developed in parallel with implementation, not used to "stop the clock." Practical experience shows that deprioritised areas (e.g., cookie rules) foster persistent non-compliance that is only corrected after inspections, underscoring the need for credible, well-resourced, and coordinated enforcement.

> *Focus first on the consistent and harmonised enforcement of the Data Act;* (European Tyres and Rubber Manufacturers' Association)
>
> *We therefore urge the Commission to maintain its firm commitment to the timely and uninterrupted implementation and enforcement of the Act, on schedule with what is elaborated in the Act itself.* (Civil Liberties Union for Europe)
>
> *Some business-sector groups are even calling for a 24-month pause.* (Civil Liberties Union for Europe)
>
> *In Denmark, complying with the rules regarding cookies used for simple statistical purposes are explicitly not prioritized by the authorities* . (The Danish Consumer Council)

DigiFinland: Calls for stronger EU-level oversight of notified bodies and uniform market surveillance, clarifying self-certification so Class I device makers meet conformity beyond mere CE marking.

> *Clarify self-certification requirements and ensure sufficient and uniform market surveillance by competent authorities so that manufacturers of Class I devices fully meet conformity requirements, not just affix the CE mark without adequate compliance.*

Technology Industries of Finland: Advocates uniform, EU-wide enforcement of the Data Act via a strengthened European Data Innovation Board to balance data protection and use.

> *The European Data Innovation Board should similarly ensure the uniform enforcement of the Data Act and evolve into a credible counterpart to the EDPB, thereby enabling a better balance between data protection and usage.*

European Tyres and Rubber Manufacturers' Association: Urges prioritising consistent, harmonised enforcement and guidance of the Data Act before any simplification to prevent fragmentation.

> *The Data Act has only recently entered into force, and its effective and harmonised enforcement must be prioritised before embarking on any legislative simplification exercises.*

Civil Liberties Union for Europe: Demands timely, uninterrupted AI Act implementation and stronger GDPR enforcement, warning that delays undermine rights and legal certainty.

> *We therefore urge the Commission to maintain its firm commitment to the timely and uninterrupted implementation and enforcement of the Act, on schedule with what is elaborated in the Act itself.*

BEUC - The European Consumer Organisation: Supports simplification only to bolster effective enforcement and opposes deregulation, urging focus on implementing and enforcing the AI Act and digital rulebook.

> *Any simplification exercise must not undermine the protection of consumers rights but ensure more effective enforcement.*

Democracy Reporting International (DRI): Rejects delaying the AI Act and calls for strong, timely implementation and enforcement, noting ongoing progress that guides compliance.

> *Rather than introducing delays, the focus should be on strong and timely implementation and enforcement.*

The Danish Consumer Council: Insists simplification must enhance enforcement and shows that deprioritising cookie oversight leads to persistent non-compliance remedied only after inspections.

Despite this, reports show the same issues and indicate that companies almost never fully comply and only do so after they have been visited by the authorities .

ANEC: Warns that delaying enforcement erodes the EU's credibility as a leader in AI governance.

Delaying enforcement would undermine the credibility of the EU as a global leader in AI governance by signalling that regulatory ambitions can be stalled by technical and standardisation processes.

: Argues that weak legislation is ineffective against hostile international actors and calls for strict enforcement of rules.

Not by diluting regulation, but by strict enforcement on international players.

: Notes that without consistent enforcement, compliance deteriorates and risks multiply.

European Law Institute: Cautions that reducing obligations may weaken enforcement standards and uniformity across the EU.

: Urges focusing on enforcing existing rules rather than dismantling regulatory protections.

Pour Demain Europe: Recommends centralized, proportionate enforcement for general-purpose AI to ensure uniform accountability.

Nordic Financial Unions - the Nordic financial trade unions confederation: Warns that a purely risk-based supervisory approach can leave violations unaddressed, calling for more comprehensive enforcement.

The European Lotteries Association: Calls for strong enforcement and clear accountability to curb illegality and protect consumers.

European Public Service Union: Urges timely enforcement and coherent alignment of the AI Act across authorities to ensure consistent protections.

TÜV-Verband e. V.: Opposes postponements because deadlines drive oversight, while acknowledging delays in setting up competent authorities and notified bodies.

Federation of German Consumer Organisations (vzbv): Seeks stronger enforcement capacities paired with support for SMEs to ensure uniform compliance.

DOT Europe: Supports streamlining DSA notice-and-action processes to improve enforcement efficiency and uniformity.

European Casino Association (ECA): Highlights consumer harm from illegal markets and urges strict, uniform cross-border enforcement and cooperation.

Confederation of European Security Services (CoESS): Criticizes ineffective enforcement and fragmented reporting, advocating standardized, efficient oversight mechanisms.

EU DisinfoLab: Warns that enforcement failures harm democracy and innovation, urging robust implementation of rules.

epicenter.works - for digital rights: Opposes deregulation and calls for firm enforcement of existing digital rights frameworks.

ICMP - International Confederation of Music Publishers: Backs proportionate DSA enforcement architecture and maintaining robust AI Act enforcement to safeguard rights.

The Center for Countering Digital Hate: Cautions that deregulation before enforcing existing laws undermines protections and accountability.

AlgorithmWatch: Argues that law credibility depends on consistent enforcement rather than deregulation.

European Digital Rights (EDRi): Calls for stronger enforcement and practical guidance over deregulation to ensure uniform rights protections.

noyb: Notes that lax enforcement inflates consent rates and undermines GDPR effectiveness, requiring stricter oversight.

European DIGITAL SME Alliance: Advocates fair, calibrated enforcement and implementation that supports SMEs while ensuring uniform compliance.

AI Accountability Lab (AIAL), Trinity College Dublin: Urges investment in compliance support and strong enforcement, including strict GDPR application and safeguards.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Observes that limited enforcement capacity fuels non-compliance and calls for strengthening authorities.

Ada Lovelace Institute: Emphasizes responsive institutions and robust enforcement to keep digital governance effective and uniform.

BUGLAS e.V.: Asserts that strong law enforcement remains necessary to ensure compliance and user protection.

Access Now Europe: Argues that delaying AI Act enforcement weakens rights and that enforcement failures—not strict standards—are the real problem.

2.3.4 Cross-Border & Sectoral Enforcement

Cross-border enforcement in the EU requires stronger application of existing frameworks for international data flows and digital markets, alongside tighter coordination among authorities. Priorities include improving enforcement of GDPR transfer rules, addressing weaknesses in the main-establishment/one-stop-shop model, building EU27 enforcement networks with greater Commission support, and using the DSA to tackle cross-border IP infringement. Oversight should extend to third-country infrastructure nodes, with a preference for EU-supervised trust services and enhanced scrutiny of consent management platforms and related vendors. Sectorally, product safety and customs enforcement must adapt to direct-to-consumer imports where the consumer effectively acts as the importer, creating compliance gaps and distorting competition. Solutions highlighted include requiring an EU-based responsible person or importer of record for all products, revising the Customs Code to strengthen inspections, and deploying AI at borders. In finance, stakeholders flag cross-border enforcement risks and the need to detect insolvency fraud. Across the digital sphere, there is a call to ensure large non-EU tech firms comply with GDPR, DSA, DMA, and the AI Act—and meet tax obligations—while avoiding the use of these rules as geopolitical bargaining tools.

One of the biggest challenges today is the growing entry of products into the EU under a B2C model in which the consumer assumes the role of importer, as the goods are delivered directly to their home. (Adigital (Asociación Española de la Economía Digital))

In what concerns the international dimensions of data, we highlight that while EU rules on personal data transfers provide an adequate balance, their enforcement should be improved as the CJEU itself infers in its case law. (BEUC - The European Consumer Organisation)

Comply with the GDPR and implement the other regulations (DSA, DMA,AIAct, etc.) STRENG and do not use them as a bargaining power with the US. ()

Make sure that US tech monopolies comply with the U.S. Acts and pay taxes in the EU! ()

BEUC - The European Consumer Organisation: Calls for stronger enforcement of EU personal data transfer rules in line with CJEU case law while relying on existing tools like adequacy decisions to ensure safe cross-border flows.

In what concerns the international dimensions of data, we highlight that while EU rules on personal data transfers provide an adequate balance, their enforcement should be improved as the CJEU itself infers in its case law.

Adigital (Asociación Española de la Economía Digital): Highlights enforcement gaps from direct B2C imports that bypass EU importers and proposes designating an EU-responsible person, creating an importer of record, and using AI at customs to police compliance.

This effectively prevents the enforcement of European compliance standards for those products, posing risks for consumers and distorting competition with EU-based operators.

American Chamber of Commerce to the EU: Warns that certain enforcement approaches pose risks for cross-border financial services and need careful calibration to avoid unintended market impacts.

: Urges firm, non-political enforcement of EU digital rules on US tech firms to ensure consistent cross-border compliance across GDPR, DSA, DMA, and the AI Act.

Comply with the GDPR and implement the other regulations (DSA, DMA,AIAct, etc.) STRENG and do not use them as a bargaining power with the US.

DigitalTrade4.EU: Advocates stronger EU oversight of third-country infrastructure nodes in digital services to safeguard compliance and security across borders.

European Signature Dialog: Favors EU-supervised trust and signature services to keep oversight within EU jurisdiction and ensure enforceability across borders.

ASNEF: Calls for enhanced detection and enforcement against insolvency-related fraud through improved cross-sector cooperation and data use.

ICMP - International Confederation of Music Publishers: Seeks robust, coordinated EU-wide enforcement against copyright infringement facilitated by GPAI, leveraging the DSA and empowering an EU27 enforcement network and the Commission.

Connect Europe: Notes that ambiguity around main establishment and underuse of the one-stop-shop impede consistent cross-border enforcement under EU digital rules.

Zentralverband der deutschen Werbewirtschaft (ZAW): Stresses the need for better coordination among EU authorities to achieve effective, consistent cross-border enforcement.

DIGITALEUROPE: Argues the GDPR main establishment rule alone is insufficient for effective cross-border enforcement and calls for improvements.

AI Accountability Lab (AIAL), Trinity College Dublin: Calls for stronger oversight and accountability of consent management platforms and their vendors to address cross-border compliance gaps in adtech.

2.3.5 Transparency, Participation, Audits & Monitoring

This category assembles calls to make enforcement legitimate and effective by pairing transparency with inclusive participation. Stakeholders urge systematic involvement of local and regional authorities that shoulder implementation burdens, and continuous engagement of civil society, unions, researchers and consumers through open, public hearings rather than invitation-only consultations. Multiple inputs flag consultation and impact-assessment gaps, the sidelining of NGOs, and risks from deregulation or private standard-setting without democratic control. At the same time, transparency should remain effective yet proportionate: align disclosure across laws, protect commercially sensitive information, and preserve traceability, registration (e.g., ROPA) and notification obligations essential for oversight and anti-discrimination enforcement. Audits and monitoring are framed as the backbone of accountability. Proposals include mandating regular independent audits with comprehensive reports, ensuring cooperation and non-interference by auditees, and reinforcing market surveillance. Digital oversight should rely on long-term, immutable audit trails and contract metadata, end-to-end verification, dual LEI/vLEI identifiers, and AML reporting; supervisory models can replace burdensome consent-logging with random checks and complaint analysis. Registers and comparable reporting enhance

fairness and compliance, while robust authentication, transparent version control and long-term accessibility underpin trustworthy records. Finally, stakeholders warn that burdensome on-site audits and over-simplification can create new risks, advocating proportionate, risk-based checks and continuous monitoring (including trusted flaggers) to reveal misleading metrics and unintended consequences.

> *The City of Stockholm therefore urges the Commission to systematically involve local and regional authorities throughout the legislative process.* (City of Stockholm)
>
> *In addition, future "omnibus" or simplification packages should be discussed through open, public hearings rather than invitation-only consultations.* (FEBIS)
>
> *Regarding redirection to market-specific websites: rather than requiring platforms to store every individual consent, it would be more efficient to establish a supervisory system that verifies companies' methodologies via random checks and customer complaint analysis.* (Adigital (Asociación Española de la Economía Digital))
>
> *Any transition to digital systems must include robust authentication tools, transparent version control, and guarantees of long-term accessibility.* (Union of Entreprenuers and Employers)

City of Stockholm: Calls for systematic inclusion of local and regional authorities in lawmaking to improve transparency and oversight, noting local administrations bear major implementation burdens.

> *The City of Stockholm therefore urges the Commission to systematically involve local and regional authorities throughout the legislative process.*

FEBIS: Advocates open, public hearings for simplification packages instead of invitation-only consultations to enhance transparency and accountability.

> *In addition, future "omnibus" or simplification packages should be discussed through open, public hearings rather than invitation-only consultations.*

Democracy Reporting International (DRI): Urges continuous involvement of civil society, consumer groups, unions, and researchers in relevant discussions to uphold democratic oversight.

> *Civil society organisations, consumer groups, trade unions, and researchers must be continuously involved in all relevant discussions, in line with the European Commission's Better Regulation principles.*

Adigital (Asociación Española de la Economía Digital): Proposes supervisory oversight via random checks and complaint analysis instead of storing individual consents, maintaining effective monitoring with less burden.

> *Regarding redirection to market-specific websites: rather than requiring platforms to store every individual consent, it would be more efficient to establish a supervisory system that verifies companies' methodologies via random checks and customer complaint analysis.*

Union of Entreprenuers and Employers: Supports simplification that preserves proportionate transparency, traceability, and accountability, with aligned disclosures and robust digital audit features.

> *Simplification should nonetheless preserve the principles of traceability and accountability.*

Bündnis F5: AlgorithmWatch, Gesellschaft für Freiheitsrechte, Open Knowledge Foundation, Reporter ohne Grenzen, Wikimedia Deutschland: Calls for inclusive stakeholder participation in evaluations to ensure transparent oversight and accountable policy reviews.

European Law Institute: Recommends comprehensive audit report requirements, cooperative non-interference during audits, and justification when not implementing recommendations to strengthen accountability.

DigitalTrade4.EU: Advocates technology-enabled oversight: immutable long-term audit logs, dual LEI/vLEI, end-to-end verification, AML reporting, and contract metadata for effective surveillance and audits.

: Warns that limited civil society participation undermines transparency and democratic accountability in oversight processes.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Encourages inclusive stakeholder engagement with feedback loops to improve transparency and ongoing monitoring of impacts.

Nordic Financial Unions - the Nordic financial trade unions confederation: Stresses the need for transparency and sufficient oversight competence to ensure accountable enforcement in finance.

Palombar - Associação de Conservação da Natureza e do Património Rural: Highlights transparency and consultation shortcomings that weaken participatory oversight and accountability.

European Public Service Union: Emphasizes mobilizing civil society to reinforce enforcement and public oversight of EU rules.

Intesa Sanpaolo: Supports establishing registers to aid compliance, improving transparency and auditability for authorities.

University of Amsterdam: Criticizes the lack of impact assessments and meaningful consultation, reducing transparency and legitimacy of oversight reforms.

REIF: Notes missing analyses of public sector impacts, hindering transparent decision-making and accountable implementation.

Comitato Elettrotecnico Italiano - CEI: Calls to preserve transparency and stakeholder participation even during urgent interventions to safeguard accountability.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Opposes deregulation that removes notification and reporting duties, asserting these are vital for transparent oversight and fair enforcement.

Fedoweb - Federazione Operatori Web: Argues that strong oversight and comparable reporting are needed to ensure fairness and accountability in digital markets.

Forvis Mazars: Proposes mandating regular independent audits to ensure effective monitoring and accountability.

Corporate Europe Observatory: Reports civil society has been sidelined in consultations, undermining transparency and democratic scrutiny.

The Center for Countering Digital Hate: Warns that misleading moderation metrics obscure accountability and calls for robust transparency reporting and empowered trusted flaggers.

Homo Digitalis: Flags insufficient consultation time for civil society, weakening participatory transparency and scrutiny.

Bocconi University: Recommends stronger consultation and Digital Rights oversight, with independent monitoring of simplification effects to protect accountability.

Orgalim - Europe's Technology Industries: Supports separate registration and reporting obligations to preserve transparency and traceability for regulators.

: Calls to mandate clear transparency and accountability standards across legislation to support effective oversight.

Insurance Europe: Warns that burdensome on-site audits can raise operational risks and urges proportionate oversight mechanisms.

European Digital Rights (EDRi): Highlights risks to democratic legitimacy and scrutiny from deregulation and urges preserving registration obligations to maintain transparency.

Middle Tech Europe: Advocates monitoring simplification for unintended consequences to ensure transparency and corrective oversight.

European network of equality bodies (Equinet): Argues that thorough impact assessments and maintained transparency are essential for effective anti-discrimination enforcement.

AI Accountability Lab (AIAL), Trinity College Dublin: Warns that removing records-of-processing obligations would undermine oversight, accountability, and compliance monitoring.

Access Now Europe: Critiques shifting standard-setting outside democratic control, reducing transparency and accountability in enforcement.

2.3.6 Independent Oversight, Integrity & Safeguards

Independent Oversight, Integrity & Safeguards centers on building public trust through independent, law-based supervision that protects democratic norms and European values. Stakeholders stress that self-regulation is insufficient: regulators should reinforce ethical AI, GDPR compliance, and platform accountability; require independent audits for large-scale processing; and deploy technical safeguards such as authority-controlled locks and tamper-proof chain-of-custody traceability. Civil society calls for strong, conflict-free oversight, reflected in scrutiny of the EU AI Office, while unions and watchdogs demand strict oversight of powerful platforms and tech giants. Integrity requires insulating investigations and supervisory actions from political or national interference, ensuring clear judicial review, and preventing abuse of exemptions or science-washing. Oversight should be proportionate and streamlined (e.g., third-party risk oversight), recognize the limits of relying on certifications over time, and avoid captured or burdensome, reversed-presumption regimes. While some industry actors claim existing mechanisms suffice, the throughline is that independent, conflict-free supervision with enforceable checks and transparency embeds trust, accountability, and competitiveness in the EU technology stack.

The EU's digital policy must not only be shaped by but also effectively safeguard democratic norms and European values. ()

Regulatory frameworks must, for instance, reinforce ethical AI development, GDPR compliance, and platform accountability. ()

3 Lobby watchdogs file complaint against AI Office over conflict of interest | Corporate Europe
(BEUC - The European Consumer Organisation)

o maintain citizens' confidence and buy-in but also to crea- te a globally competitive ‚made in the EU' commercial brand, European digital products and services must - on top of being sustainable - be secure, transparent, and accountable. ()

: Advocates democratic oversight to embed trust, accountability, and European values in digital policy through strong regulatory frameworks and political leadership. Calls for institutional safeguards to prevent political or national interests from derailing investigations.

While the adjustments should enable the Com- mission's DG Competition to intervene faster and more effectively in all cases with a Union dimension, new insti- tutional safeguards should make sure that investigations cannot be stopped anymore because of political or nati- onal interests.

BEUC - The European Consumer Organisation: Highlights conflict-of-interest concerns regarding the AI Office and urges strong, independent oversight informed by civil society recommendations. Emphasizes the need for transparent governance and accountability mechanisms.

3 Lobby watchdogs file complaint against AI Office over conflict of interest | Corporate Europe

Compagnie Nationale des Commissaires aux Comptes (professional organisation for statutory auditors): Argues that independent public authorities and professional standards, not multinationals, should shape regulation and oversight. Emphasizes safeguarding integrity through impartial rule-setting.

European Law Institute: Proposes mandatory independent audits for large-scale processors to ensure accountability and robust safeguards. Stresses external verification as a core oversight tool.

DigitalTrade4.EU: Calls for law-based oversight by competent authorities with technical access controls and tamper-proof chain-of-custody to ensure integrity and traceability. Emphasizes enforceable, verifiable safeguards.

European Public Service Union: Demands strict public oversight and enforcement over tech giants to protect the public interest and workers/users. Urges robust accountability for powerful platforms.

AI Standards Lab: Warns regulators to curb abuse of exemptions and science-washing that undermine oversight. Calls for tighter safeguards and transparency to preserve integrity.

Association des Constructeurs Européens de Motocycles: Argues for case-specific decisions aligned with EU interests and subject to judicial review, while asserting existing oversight mechanisms are sufficient. Seeks proportionate, legally grounded enforcement.

: Asserts that self-regulation is ineffective without robust external oversight and enforceable safeguards. Calls for independent accountability mechanisms.

The Center for Countering Digital Hate: Criticizes platform self-oversight as ineffective and supports stronger regulator-led digital services oversight. Emphasizes independent enforcement to ensure accountability.

European Fund and Asset Management Association (EFAMA): Urges streamlining and clarifying third-party oversight to ensure consistent accountability across service providers. Seeks proportional, efficient supervisory frameworks.

Insurance Europe: Cautions against long-term reliance on certifications for assurance, emphasizing ongoing supervision and reassessment. Advocates dynamic oversight to maintain compliance over time.

DIGITALEUROPE: Warns against burdensome presumptions and reversed oversight obligations that distort enforcement. Calls for proportionate, predictable supervision focused on risk.

AI Accountability Lab (AIAL), Trinity College Dublin: Recommends banning interference with audits and rejecting excuses for noncompliance to safeguard independent accountability. Supports strong, enforceable integrity safeguards.

2.3.7 Accountability, Liability, Sanctions & Redress

This category consolidates how accountability, liability, sanctions, and redress should operate across AI governance. Stakeholders warn that size-based and scope-based exemptions (e.g., loosening record-keeping or narrowing "material influence" in risk classifications) can dilute oversight and transparency, while internal-only conformity assessments (often not reviewed or approved and disclosed only on a reasoned request) risk making infringements harder to detect. Additional obstacles include downstream shielding, complex complaint pathways, and broad third-party exemptions that complicate enforcement. At the same time, the interplay between sectoral regimes (e.g., CRA and the AI Act) demands clarity so that essential cybersecurity and AI obligations are consistently applied without creating blind spots. A robust enforcement architecture is urged: proactive supervision with the ability to act on adverse audit findings; cross-authority coordination (including fundamental rights bodies) with adequate resourcing; and clear allocation of responsibilities across the value chain (producers, deployers/employers, marketplaces, and controllers). Calls include maintaining accountability during regulatory simplification, strengthening marketplace and platform responsibility (countering immunity overreach), and ensuring context-specific oversight such as clinician roles in medical AI. Regulators must be able to investigate, order cessation of unlawful processing, and impose effective, proportionate, and deterrent fines; overlapping prohibitions may legitimately trigger multiple sanctions. Whistleblowing and accessible complaint channels are essential to surface harms. Redress is central: individuals need actionable remedies (including guidance on the right to an explanation), and collective pathways should mirror GDPR-style representation by not-for-profit organizations. Empowering NGOs to act on behalf of users—and, where appropriate, in their own right—bolsters collective interests, especially where harms are diffuse. Overall,

consequences must be real and predictable so that providers and platforms “own” their decisions and incentives align with responsible behavior.

We highlight the need to ensure the effective and consistent application and enforcement of the AI Act that enables individuals to seek redress in case of fundamental rights infringements, especially in the absence of the AI Liability Directive. (Centre for Democracy and Technology Europe)

Finally, we request that Datatilsynet imposes an effective, proportionate and deterrent fine against Google for the infringements of the GDPR, considering: (BEUC - The European Consumer Organisation)

Moreover, the assessment is not subject to review or approval. (Centre for Democracy and Technology Europe)

If exemptions to the 'high-risk' classification are expanded through the simplification process and the idea of "material influence" is weakened, systems that indirectly shape decisions, such as ranking, recommendation, or scoring tools-could avoid proper oversight. (Civil Liberties Union for Europe)

Civil Liberties Union for Europe: Warns that size-based exemptions and weakened high-risk criteria would erode record-keeping, transparency, and accountability, letting influential AI tools evade oversight. Endorses EDPB/EDPS calls to avoid broad exemptions that undermine legal certainty.

Further simplification that removes or weakens the need to justify exemptions would also make the process less transparent and reduce accountability.

Centre for Democracy and Technology Europe: Notes that most high-risk AI conformity assessments rely on unchecked internal control, undermining accountability and preventing timely scrutiny. Calls to strengthen enforcement, enable individual redress, and resource cross-authority cooperation, including guidance on explanation rights.

This is already problematic from an accountability perspective as there is no possibility to check providers' assessments and hold them accountable in cases where infringements go unnoticed or are not acted upon by relevant authorities.

BEUC - The European Consumer Organisation: Calls for explicit NGO representation and collective redress mechanisms, mirroring GDPR Article 80, to ensure comprehensive enforcement for users. Also urges authorities to investigate violations, halt unlawful processing, and impose effective, proportionate, and deterrent fines.

The proposal also lacks a provision on the representation of users by NGOs and collective redress.

: Highlights risks of penalties, litigation, and reputational exposure tied to AI use, emphasizing the need for clear liability frameworks and sanction regimes.

Ingka Group IKEA: Raises concerns that regulatory simplification could dilute accountability for AI actors, advocating balanced rules that ensure responsibility without undue burden.

European Law Institute: Notes that overlapping prohibitions may trigger multiple sanctions and stresses acting on negative audit findings so that compliance failures lead to enforceable consequences.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Advocates robust complaint channels, individual redress, and whistleblower protections to surface harms and ensure accountability across the AI lifecycle.

Nordic Financial Unions - the Nordic financial trade unions confederation: Supports a deployer definition that clearly assigns employer accountability for workplace AI, ensuring duties and liability for impacts on workers.

: Examines limits of AI rights and calls for mechanisms that translate principles into enforceable accountability and redress for affected individuals.

Federation of German Consumer Organisations (vzbv): Urges stronger accountability and liability for AI marketplaces and intermediaries, ensuring they bear responsibility for unsafe or non-compliant systems offered to consumers.

AI Standards Lab: Warns that shielding downstream users hampers enforcement and accountability, recommending calibrated liability to incentivize due diligence along the value chain.

Digitalexperte: Argues that clear producer liability can shift compliance burdens upstream to drive safer AI design while avoiding unfair exposure for end users.

Movement for an Open Web: Calls for strong controller accountability and procedural safeguards to ensure transparent, auditable AI practices and meaningful remedies for violations.

The Center for Countering Digital Hate: Criticizes broad liability shields like Section 230 for weakening platform accountability and urges rules that impose consequences for harmful inaction. Highlights EU approaches, including DSA fines and market restrictions, to drive platform responsibility and enable redress.

Bocconi University: Emphasizes that legality should be remedy-capable, enabling contestation and effective redress when AI decisions harm rights.

Hugging Face: Urges that regulatory simplification must preserve core accountability requirements and avoid loopholes that erode transparency and oversight.

BioMed Alliance: Stresses clear allocation of roles, clinician oversight, and liability in medical AI to ensure patient safety and enforceable responsibility for failures.

Free ICT Europe Foundation: Warns that a fragmented regulatory landscape impedes effective complaints and redress, calling for streamlined pathways and provider accountability.

The Finnish Media Federation, Finnmedia: Argues against broad exemptions for third parties that would dilute accountability, insisting on enforceable obligations and liability across actors.

2.4 Data Governance, Interoperability and Sovereignty

The unifying priority is a coherent, risk-based governance stack that reconciles privacy-by-design with access-by-design, backed by enforceable interoperability and clear roles. Legal clarity on the GDPR–Data Act interface, standardised data classification, and certification would cut liability and implementation risk while aligning access, portability, and trade secret protection. Interoperability and portability need open standards, machine-readable purpose labels, clear cloud switching (including intermediaries), and integrated public infrastructures so passports, customs, and safety systems work as one. Access and reuse should be purpose-based and tiered, using trusted data spaces, robust anonymisation, and compensation models, with safeguards for B2G access and tactics that commingle personal and other data. Open data must be high quality, metadata-rich, harmonised, sustainably funded, and expanded to legal and research domains to power AI and public value, with candid documentation of limits. Security, confidentiality, IP, and cybersecurity alignment demand pre-disclosure risk controls, workable exceptions, automated classification, TDM boundaries, and care for sensitive geospatial detail. Digital sovereignty calls for trusted partnerships, selective localisation, sovereign cloud capacity, and risk-based international transfers, while ensuring EU data availability (including language coverage). Sector rules should ensure role-based access (e.g., vehicles), once-only public services, and viable geospatial cores. Platform governance should rebalance power via quasi-controller duties, responsibility registries, and coherent intermediary regimes. Across areas, the direction is harmonised, interoperable, and proportionate governance that enables competitive data sharing without eroding rights or secrets. The common thread is implementation realism: standardisation, accountability, and sustainable funding to avoid fragmentation.

2.4.1 Regulatory Coherence & Legal Clarity

Regulatory Coherence & Legal Clarity in EU data policy hinges on resolving foundational ambiguities and aligning overlapping regimes. Stakeholders highlight that the distinction between personal and non-personal data remains unsettled and difficult in practice, even as the Data Act introduces broad access rights that intersect with GDPR's access and portability provisions. The resulting tension—Privacy-by-Design under the GDPR

versus Access-by-Design under the Data Act—creates uncertainty in product development, raises liability risks from misclassification (including inadvertent disclosure of personal data), and complicates the protection and sharing of trade secrets that may also trigger competition law concerns. To restore legal clarity, respondents call for authoritative guidance on the GDPR–Data Act interplay, standardized technical procedures for data classification, and certification schemes that evidence compliance. They urge reconsideration of GDPR portability in light of new access rights, clearer minimum disclosure and data holder obligations, and better mapping of the relationships across the EU's data acquis (including DGA, Data Act, sectoral rules). Several caution that piecemeal or narrow reviews will not deliver the necessary coherence and that, beyond new rules, faster learning from proven practices is essential to reduce burdens, avoid perverse incentives (e.g., data-minimizing designs that undercut data-sharing goals), and ensure proportionate, implementable obligations.

> *There is no reliable information on the interplay between the GDPR and the Data Act.* (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)
>
> *However, the central question, whether data is personal or non-personal has yet to be resolved.* (eco - Verband der Internetwirtschaft e.V.)
>
> *While the GDPR (e.g. Art. 5, 6 and 7) with its "Privacy-by-Design"-approach sets out strict requirements for the processing of personal data, the Data Act with its "Access-by-Design"-approach aims to facili- tate access to and sharing of data - often from connected devices.* (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)
>
> *There are great concerns that companies may be incentiv- ized to design their products in a more data-efficient manner, thereby undermining the very objectives the Data Act aims to achieve.* (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)
>
> **eco - Verband der Internetwirtschaft e.V.:** Calls for clearer distinctions between personal and non-personal data, and for a workable definition of non-personal data within the EU data acquis to enable legally secure transfers.
>
> *However, the central question, whether data is personal or non-personal has yet to be resolved.*
>
> **Bitkom e.V.:** Highlights overlap between GDPR access and portability rights and the Data Act's broader data access, urging clarification of their interplay and the added value of new rights.
>
> *This raises the question of what specific benefits this new data access right provides over the existing right of access under the GDPR.*
>
> **Leading Baltic tech and other businesses and professional associations listed in the submission:** Argues the limited Omnibus GDPR review will not deliver the necessary coherence, indicating broader reforms are needed to address practical legal clarity.
>
> *The recent GDPR review initiated by the European Commission earlier this year under the IV Omnibus proposal - which focused primarily on simplifying data processing records for smaller organisations (Article 30 GDPR) - will not deliver the necessary change.*
>
> **Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries:** Warns of unresolved interplay and conflicting objectives between GDPR's privacy-by-design and the Data Act's access-by-design, creating classification and liability risks. Calls for guidance, technical standards, and certification to ensure compliance.
>
> *There is no reliable information on the interplay between the GDPR and the Data Act.*
>
> **:** Contends that more regulation alone will not fix daily administrative burdens, advocating learning from proven practices to achieve practical coherence.
>
> *The solution is not more regulation but faster learning from what already works.*
>
> **American Chamber of Commerce to the EU:** Seeks clear minimum requirements for data disclosure to ensure predictable, coherent obligations for data holders and users.
>
> **Japan Business Council in Europe (JBCE):** Requests clarification of the Data Act's design choices and obligations to provide legal certainty for implementers.

Kompetenznetzwerk Datentreuhandmodelle (DatNet): Urges clearer definitions around legal persons in data trust models and a more precise articulation of DGA objectives and exemptions to avoid uncertainty.

Association of Finnish Cities and Municipalities: Calls for a coherent mapping of relationships among EU data laws to prevent overlap and conflicting obligations for municipalities.

CPME: Supports preserving existing sectoral rules while maintaining the Data Act's ambition, seeking guidance that avoids undermining established protections.

The Guild of European Research-Instensive Universities: Warns that excluding cultural data without clear boundaries breeds uncertainty and requests guidance to delineate scope.

Association des Constructeurs Européens de Motocycles: Asks the EDIB to issue practical assessment guidelines to harmonize data governance and reduce interpretive uncertainty.

AK Wien: Proposes using processing registers to strengthen compliance and AI accountability, contributing to clearer documentation and oversight.

EFCA - European Federation of Engineering Consultancy Associations: Seeks clarity on liability allocation and data access conditions under the Data Act to provide predictable frameworks for engineering consultancies.

Digital Currencies Governance Group (DCGG): Requests clearer definitions of system boundaries in cross-device contexts and emphasizes regulating data-sharing agreements rather than smart contracts to avoid confusion.

CIO Platform Nederland: Notes that the Data Act's impact differs across roles and asks for guidance clarifying responsibilities and rights for each actor.

European Savings and Retail Banking Group: Raises deep concerns about FiDA's burdens, scope, and costs, urging withdrawal or major revision until strategy reviews conclude to restore legal certainty.

Zentralverband Deutsches Baugewerbe: Advocates preserving the Data Act's balanced principles and user protections to maintain clarity and trust in data sharing.

: Emphasizes that legal obligations extend beyond mere data collection and asks for coherent alignment of duties across instruments.

Enedis: Calls for precise clarification of data holder obligations and scope to ensure predictable compliance under the Data Act.

Chamber of Commerce and Industry for Munich and Upper Bavaria: Highlights overlapping roles between the DGA and the Data Act and seeks clear delineation to avoid duplicative requirements.

APPLiA (Home Appliance Europe): Requests a clearer definition of the data holder in connected device contexts to establish predictable responsibilities and legal certainty.

2.4.2 Digital Sovereignty & Cross-Border Transfers

Digital Sovereignty & Cross-Border Transfers centers on reducing strategic dependencies while enabling secure, interoperable data flows. Stakeholders call for trusted partnerships with like-minded democracies, targeted industrial policy, and sovereign cloud capacities (e.g., GAIA-X, IPCEI) to strengthen Europe’s autonomy amid US cloud dominance. Policy proposals include joint ventures, local storage and code escrow in the EU, and using market leverage to require fall-backs and assurances against the weaponisation of dependencies—paired with clear identification of the sovereignty threats being addressed. For cross-border transfers, a risk-based approach anchored in the GDPR is advocated to streamline international data flows and align with open data goals, while guaranteeing security and preventing misuse. Several positions urge reconsidering obligations to share device data outside the EEA, limiting data-holder duties to EU-only contexts to protect competitiveness in

strategic sectors (e.g., rail), and keeping highly sensitive (e.g., military) data within EU jurisdiction. There is debate over how far to go: some support relying on existing GDPR transfer tools and avoiding non-technical sovereignty requirements, while others push stronger localization. Trade-offs are explicit: full onshoring is not feasible, so selective European alternatives in the most sensitive parts of the tech stack are proposed, even as complex supply chains leave residual vulnerabilities. A diffusion-led competitiveness strategy may suit the short term but risks eroding long-term sovereignty if foreign technologies (e.g., foundation models) do not align with EU values; mitigation includes ensuring EU data availability, especially for less-common European languages. More protectionist voices argue for local growth through ending dependencies on illiberal regimes and establishing European cloud, data, and AI regimes that embed democratic norms.

> *It is incomprehensible why the risk-based approach established in the GDPR (Ar- ticles 24 and 32 GDPR) should not be applied to measures taken for data transfers to third countries.* (German Insurance Association)
>
> *Data protection must be guaranteed in cross-border data exchange and appropriate security precautions against misuse must be taken.* (WKÖ - Austrian Federal Economic Chamber)
>
> *A final option is for Europe to use its market leverage to mitigate sovereignty risks - by requiring firms to provide assurances and options that either (i) reduce Europeans' exposure to 'weaponisation' of dependencies; and/or (ii) ensure workable fall-back options if such weaponisation occurred.* (AI & Partners B.V.)
>
> *Growth can now only be achieved locally, by creating a more protectionist environment.* ()
>
> **:** Advocates partnering with like-minded democracies, industrial policy to build strategic capabilities, and keeping sensitive military data under EU jurisdiction to reduce external dependencies.
>
> *timately, the strengthening of the EU's defence capabi- lities will require deeper collaboration between Member States: military data must remain within European juris- diction and be protected from external influenc*
>
> **German Insurance Association:** Calls to anchor a GDPR-style risk-based approach to third-country transfers to streamline flows while maintaining protections and coherence with EU strategy.
>
> *It is incomprehensible why the risk-based approach established in the GDPR (Ar- ticles 24 and 32 GDPR) should not be applied to measures taken for data transfers to third countries.*
>
> **Finnish Food and Drink Industries´ Federation (ETL):** Urges reconsideration of obligations to share device data outside the EEA under the Data Act in light of a changed security environment.
>
> *The obligation to share device data outside the EEA under the Data Act should be reconsidered due to the changed security landscape.*
>
> **WKÖ - Austrian Federal Economic Chamber:** Promotes European sovereign cloud initiatives (GAIA-X, IPCEI Cloud) to strengthen digital independence and secure data ecosystems, while ensuring protection in cross-border exchanges.
>
> *We strongly support the ongoing initiatives to develop a European framework for sovereign clouds in the context of GAIA-X and call for these efforts to be vigorously pursued in order to strengthen Europe's digital independence.*
>
> **AI & Partners B.V.:** Proposes using EU market leverage and regulatory safeguards to mitigate dependency weaponisation, complementing selective onshoring and local storage while acknowledging trade-offs with diffusion and competitiveness.
>
> *Finally, Europe may use its market strength to mitigate sovereignty risks - by requiring firms to provide services which reduce Europeans' exposure to 'weaponisation' of dependencies; and/or ensure workable fall-back options if such weaponisation occurred.*
>
> **UNIFE:** Seeks to confine certain data-sharing obligations to EU-only parties to protect strategic industries, warning that external disclosures could erode competitiveness.
>
> *This could undermine Europe's industrial competitiveness by forcing the disclosure of valuable product data to third-country competitors, potentially weakening the EU's industrial base.*

American Chamber of Commerce to the EU: Urges reliance on GDPR mechanisms for international transfers and cautions against non-technical sovereignty mandates that could hinder data flows.

: Advocates a protectionist pivot to localise cloud, data and AI, ending dependencies on illiberal regimes and fostering European-controlled digital markets.

To create a new market niche, any new regulation must end dependency on these illiberal nations and establish a European cloud, data-protection and AI regime that ensures growth through localisation.

European Law Institute: Treats transfers to third countries as high-risk, implying stronger safeguards and oversight for cross-border data movements.

DigitalTrade4.EU: Supports accreditation and restrictions for cloud service providers to bolster sovereignty while positioning EU rules as global benchmarks.

Pour Demain Europe: Endorses advancing EU technological sovereignty as a strategic goal in digital infrastructure and services.

Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs (VÖWG): Calls for public digital policies aligned with European digital sovereignty to reduce external dependencies.

: Argues for stricter EU data sovereignty measures to better control and secure cross-border data handling.

European Public Service Union: Prioritises European public cloud options and robust enforcement to uphold digital sovereignty in public services.

Federation of German Consumer Organisations (vzbv): Maintains that strong, enforceable rules are essential to reinforce EU digital sovereignty and consumer protection in data transfers.

ITI - Information Technology Industry Council: Warns that overly rigid adequacy regimes and agency overreach could complicate third-country transfers and undermine workable compliance.

ENTSO-E: Requests clear, predictable safeguards for international data transfers to protect critical operations while enabling necessary flows.

CPME: Advocates preserving EU digital sovereignty in health data governance and cross-border processing.

Association des Constructeurs Européens de Motocycles: Raises concerns that divergent national opinions could lead to arbitrary rejection of data transfers, fragmenting the single market.

ICMP - International Confederation of Music Publishers: Asserts that coherent regulation is foundational to EU digital sovereignty and fair cross-border data practices.

Digitalexperte: Recommends measures to boost EU competitiveness alongside digital sovereignty in cloud and data ecosystems.

Google: Highlights that Schrems II has created a burdensome, uncertain compliance regime for transfers, urging more workable solutions.

Fastweb S.p.A.: Supports strategic autonomy by hosting and processing sensitive data within the EU and favouring European providers.

secunet Security Networks AG: Calls for an EU sovereign cloud to ensure autonomy, security, and control over critical data and workloads.

CLEPA: Flags feasibility challenges for cloud compliance obligations tied to sovereignty requirements, especially for SMEs and complex chains.

Chamber of Commerce and Industry for Munich and Upper Bavaria: Notes uncertainty around rules for transferring non-personal data internationally, seeking clarity to avoid barriers.

2.4.3 Interoperability, Standards & Portability

Interoperability, standards and portability are framed as prerequisites for a truly integrated European data economy. Stakeholders call for EU-level mandates and funding that promote digital interoperability, adoption of open standards and open-source components, and vendor diversity, alongside a standardized framework for secure, trustworthy cross-border data exchange to counter market fragmentation and enable the Digital Single Market. At the implementation layer, clarity on cloud and data processing service switching obligations is essential, especially when services are resold through intermediaries; roles, responsibilities and technical capabilities across the value chain must be defined to make portability practical. Interoperability gaps—unstandardised APIs, lack of unified consent repositories, and OEM-specific data formats—create heterogeneity and cost, so minimum datasets, machine-readable information and purpose labels, and transparent ICT interconnections are recommended to streamline data sharing and compliance while preserving innovation. Sector initiatives highlight the need for interoperable public infrastructures: the Customs Data Hub should work seamlessly with the Digital Product Passport and Safety Gate, and duplicative obligations around the Passport (e.g., third-party backups, parallel hazardous substances reporting) should be eliminated by integrating reporting into a single standardized, machine-readable passport, including SDS formats. Across policies, the preference is for interoperable solutions over deregulation, with portability requirements calibrated to technical feasibility and business models, and timelines that enable a smooth, competitive transition.

Policymakers must prioritise legislation and funding that promotes digital interoperability. ()

Use of open source and open standards will help to ensure interaction between services and platforms, opening up choices and foste- ring competition and innovation across Europe. ()

The implementation costs are estimated to exceed €10 billion in the first five years, with analysis from consulting firms like Oliver Wyman suggesting compliance costs could consume up to 40% of revenue in certain product categories. (Unipol Assicurazioni S.p.A.)

The absence of specific provisions or guidance in such cases creates legal uncertainty on roles and responsibilities and how switching obligations apply in practice, and where responsibilities lie across the value chain. (GSMA)

: Advocates EU-wide interoperability through open standards and open source, aligning public and private sector standards to build an integrated Digital Single Market and diversify vendors.

Use of open source and open standards will help to ensure interaction between services and platforms, opening up choices and foste- ring competition and innovation across Europe.

Unipol Assicurazioni S.p.A.: Warns that absent standardization—such as no minimum data set and OEM-defined formats—creates technological heterogeneity and high operational burdens, with costly API and FDSS overhauls diverting resources from innovation.

The absence of a minimum data set and the freedom of each OEM to define the format and technology for accessing vehicle data for every production line creates technological heterogeneity in the market.

GSMA: Calls for clarity on cloud service switching in reseller and intermediary scenarios to reduce legal uncertainty over roles and responsibilities across the value chain.

The absence of specific provisions or guidance in such cases creates legal uncertainty on roles and responsibilities and how switching obligations apply in practice, and where responsibilities lie across the value chain.

Adigital (Asociación Española de la Economía Digital): Highlights that technical and legal interoperability gaps, like unstandardised APIs and fragmented consent management, hinder voluntary data sharing and portability. Urges an interoperable Customs Data Hub linked with the Digital Product Passport and Safety Gate while streamlining duplicative reporting into standardized formats.

Likewise, the lack of technical interoperability (e.g., unstandardised APIs, absence of unified consent repositories) and legal uncertainty hinder the effective implementation of models based on voluntary data sharing and the portability of financial histories.

WKÖ - Austrian Federal Economic Chamber: Calls for a standardized, interoperable EU framework for secure cross-border data exchange to counter market fragmentation, considering open source from hardware to cloud and platforms.

A standardized and improved framework for the cross-border exchange of data between European companies must be created immediately in order to ensure the secure, trustworthy and efficient handling of data in the EU and to enable innovation across locations.

AI & Partners B.V.: Proposes mandating interoperable standards so firms can offer services that expand business customer choice and reduce lock-in.

The EU could also mandate that firms develop their services based on interoperable standards to ensure business customers have a wider range of choices.

European Law Institute: Advocates automated notifications and clear, machine-readable information to strengthen interoperability and transparency in data sharing.

DigitalTrade4.EU: Emphasizes achieving interoperability while preserving regulatory integrity to maintain trust and compliance in data flows.

Bayerische Motoren Werke Aktiengesellschaft: Seeks increased transparency of ICT interconnections to manage dependencies and ensure interoperable, secure integrations across suppliers.

Ecommerce Europe: Notes that incompatible devices and ecosystems hinder adoption, underscoring the need for common standards to achieve interoperability and portability.

ITI - Information Technology Industry Council: Requests clearer data access and switching obligations to enable practical portability and interoperability without excessive burden.

Comitato Elettrotecnico Italiano - CEI: Urges support and adoption of European information exchange standards to deliver interoperability across sectors and borders.

European Digital Rights (EDRi): Prefers policy solutions that enhance interoperability while avoiding deregulatory measures that could erode rights and safeguards.

European Savings and Retail Banking Group: Warns that FiDA risks isolation and incompatibility with existing frameworks, calling for alignment to ensure interoperability and effective portability.

OpenMined: Argues that bilateral data-sharing rules isolate cities and advocates interoperable, standardized frameworks that scale and support portability.

DIGITALEUROPE: Stresses that cloud portability and switching need clear scope, technical limits, and flexible timelines, cautioning that rigid obligations could undermine SaaS and PaaS models.

Mistral AI: Cautions that stringent portability rules may be infeasible or excessively costly for AI providers and should reflect technical constraints and proportionality.

INRIA and Utrecht University: Recommends clarifying and standardizing purpose labels to support machine-readable, interoperable data governance across systems.

2.4.4 Access & Reuse Governance

Access & Reuse Governance focuses on clear, purpose-based rules that distinguish data access from data reuse. Stakeholders call for tiered and purpose-limited regimes that can grant access for legitimate functions (e.g., KYC, fraud, ID verification) without permitting downstream reuse, and for explicit policies on which datasets can be reused, for which purposes, and under what AI-specific conditions. Concerns about overly permissive open-data frameworks enabling gatekeepers to extract and reuse at scale highlight sovereignty, competition, and user-control risks, motivating tighter purpose specification and oversight. Operationally, the EU Data Act's fair, non-discriminatory access principles set the baseline, yet gaps persist—such as the "designed to be retrieved" scope and tactics that commingle personal with other data to evade sharing obligations. To enable lawful,

scalable reuse, actors seek legal certainty on GDPR-compliant reuse and robust anonymisation (with standards like k-anonymity thresholds and differential privacy), alongside trade-secret safeguards and guidance for lawful bulk access to non-personal or properly anonymised data. Many advocate trusted data spaces and tiered access, strong safeguards for B2G access (limited to emergencies or clearly justified cases), demand-led and gradual sharing focused on raw, structured data, practical low-threshold tools, and cost-recovery/compensation models that sustain quality services. The governance balance aims to unlock collective intelligence and innovation while avoiding lock-ins and anti-competitive advantages: pull-only models and limits on real-time or sandbox reuse can hinder innovation; overly voluntary schemes may underdeliver; and restrictive recipient rules can reduce downstream value creation. Conversely, defending a coherent EU access framework, clarifying rights and obligations, and enabling collaborative, compensated sharing can foster interoperability, competition, and resilience without compromising privacy, IP, or sovereignty.

> *FEBIS members would like to stress the importance of distinguishing between the access to data and the possibility to re-use the data, which should both be based on clear purposes.* (FEBIS)
>
> *A balanced approach must enable lawful, non-discriminatory access to non-personal or anonymised datasets for business and information providers, while ensuring personal data protections and trade-secret safeguards.* (Siinda)
>
> *Companies that are not interested in data sharing might attempt to mix generated data with personal data in order to circumvent the scope of the Data Act.* (Bitkom e.V.)
>
> *The manufacturer maintains an advantageous position not only in the data sharing methods, but also in determining the type of data to be made available: the Data Act only mandates the provision of data "designed to be retrieved."* (Unipol Assicurazioni S.p.A.)

FEBIS: Advocates stricter governance of open data access and reuse, especially for AI, by tying datasets to specific purposes and distinguishing access from reuse. Supports cost-recovery fees to sustain high-quality services.

> *FEBIS members would like to stress the importance of distinguishing between the access to data and the possibility to re-use the data, which should both be based on clear purposes.*

Unipol Assicurazioni S.p.A.: Acknowledges the Data Act's push for fair, non-discriminatory access while highlighting practical limits where manufacturers decide which retrievable data are shared. Notes the imbalance this creates in access and reuse.

> *The manufacturer maintains an advantageous position not only in the data sharing methods, but also in determining the type of data to be made available: the Data Act only mandates the provision of data "designed to be retrieved."*

Siinda: Calls for lawful, non-discriminatory bulk access to non-personal or anonymised data with strong privacy protections and trade-secret safeguards. Urges EU guidance on anonymisation standards to give legal certainty for compliant reuse.

> *A balanced approach must enable lawful, non-discriminatory access to non-personal or anonymised datasets for business and information providers, while ensuring personal data protections and trade-secret safeguards.*

Bitkom e.V.: Warns that firms may mix personal and generated data to evade sharing obligations, undermining transparency and access. Stresses guarding against such tactics to preserve effective reuse.

> *Companies that are not interested in data sharing might attempt to mix generated data with personal data in order to circumvent the scope of the Data Act.*

WKÖ - Austrian Federal Economic Chamber: Argues simplification should pair rules with practical examples, use cases, and low-threshold tools that facilitate access and sharing. Emphasizes usability in governance frameworks.

> *Should not only be focused on rules and admin, but also provide examples and Use cases, as well as low-threshold tools and methods for data access and data sharing*

EuroGeographics: Promotes tiered access models to balance protection with usability, aligning sensitivity levels with permissions. Suggests graduated rights to enable responsible reuse.

DigitalTrade4.EU: Notes pull-based access can restrict broader data sharing and reuse. Recommends more proactive mechanisms to improve availability and interoperability.

Elia Group: Supports defending and clarifying the EU data access framework to ensure fair, secure, and interoperable reuse. Emphasizes consistency across sectors.

Irish Farmers' Association: Seeks a fair balance between public and private data interests, protecting farmers while enabling beneficial reuse. Advocates equitable access rules and transparent governance.

Japan Business Council in Europe (JBCE): Calls for allowing compensation or cost recovery when data are shared to ensure sustainability and fairness. Ties remuneration to the value and effort of data provision.

Milestone Systems: Highlights collaborative data strategies and governance as key to enabling secure access and driving innovation. Encourages cross-sector cooperation and standards.

ITI - Information Technology Industry Council: Identifies access risks under the Data Act, including IP and trade-secret exposure, and calls for robust safeguards. Urges clarity to balance innovation with privacy and security.

Association of Finnish Cities and Municipalities: Prefers trusted sharing arrangements over broad openness to protect municipal data and service quality. Supports controlled access with clear responsibilities.

Zentralverband des Deutschen Handwerks (ZDH)- Europaabteilung Brüssel: Opposes voluntary data sharing schemes that may burden SMEs, favoring clear, enforceable rules and protections. Emphasizes certainty in access and reuse obligations.

CLEPA: Warns that restrictions on eligible recipients and limited real-time access impede innovation, particularly in automotive ecosystems. Calls for broader, timely access with appropriate safeguards.

Siemens Healthineers AG: Advocates strong safeguards and the ability for data holders to object to inappropriate requests. Supports limiting vague B2G access to emergency contexts with clear governance.

European Savings and Retail Banking Group: Proposes demand-led, gradual sharing limited to raw, structured data to reduce complexity and risk. Seeks clear scoping for permissible reuse.

Data & Technology for Compliance Alliance: Urges easing administrative and technical burdens in data transfers while maintaining compliance. Promotes streamlined governance to facilitate access and reuse.

Zentralverband Deutsches Baugewerbe: Rejects voluntary data sharing, citing risks and burdens for construction SMEs. Calls for predictable frameworks with protections.

OpenMined: Argues that collective intelligence and research depend on privacy-preserving data sharing. Encourages governance that enables access through techniques like federated analysis.

DIGITALEUROPE: Warns that strict data reuse limits in regulatory sandboxes can hinder innovation. Calls for more flexible experimentation frameworks.

Enedis: Supports limiting and thoroughly evaluating B2G sharing requests to protect operational and security interests. Emphasizes proportionality and accountability in access.

2.4.5 Security, Confidentiality & IP

Security, Confidentiality & IP focuses on safeguarding trade secrets, intellectual property, and sensitive business information in data-sharing regimes. Stakeholders warn that expansive data-access mandates and broad definitions of “customer data” risk exposing derived or inferred insights, proprietary analytics, and pricing models—core competitive assets. They call for pre-disclosure assessments, robust exceptions (“handbrakes”)

that provide genuine protection beyond governance processes, and explicit alignment with cybersecurity, to prevent sensitive disclosures and market distortions. Compliance risk is amplified by uncertain distinctions between personal and non-personal data and trade secrets; misclassification can create liability and competitive harm. To mitigate this, proposals include standardized, automated classification methods and certification for data management systems, while acknowledging that anonymisation remains costly and difficult and that data sharing can inadvertently create personal data. Safeguards should also respect copyright, including limits around text and data mining (TDM). Sector- and security-specific considerations emphasize calibrating openness with national security needs, especially for geospatial data where location detail can be misused (e.g., critical infrastructure). Overall, a balanced framework is sought that enables interoperability and responsible data use while preserving confidentiality, cybersecurity, trade secrets, and IP.

> *These models, which rely on sophisticated algorithms and risk assessments, are trade secrets developed through years of investment and are a cornerstone of competitive differentiation.* (Unipol Assicurazioni S.p.A.)
>
> *The obligation to differentiate between personal and non-personal data and trade secrets poses significant risk potential for data holders.* (Bitkom e.V.)
>
> *This would expose proprietary insights developed through internal analytics, effectively mandating the transfer of intellectual capital.* (Unipol Assicurazioni S.p.A.)
>
> *It is essential consider the requirements for the level of detail thoroughly by the opening geospatial data (especially in relation to critical infrastructure and issues of national security and defense).* ()

Unipol Assicurazioni S.p.A.: Warns that the proposal endangers intellectual property and trade secrets in insurance by extending customer data to derived insights and exposing proprietary pricing and risk models, undermining competitive differentiation.

> *This would expose proprietary insights developed through internal analytics, effectively mandating the transfer of intellectual capital.*

Bitkom e.V.: Highlights high compliance and liability risks from distinguishing personal/non-personal data and trade secrets due to uncertain classifications. Recommends standardized automated classification procedures and certification to mitigate risks and build trust.

> *This distinction is often uncertain and leads to major compliance risks.*

Ibec: Urges reinforcing DA/DGA safeguards so trade-secret protections are substantive and security controls explicitly cover cybersecurity.

> *Reinforce the security and trade secrets handbrakes in DA/DGA by (i) not limiting the trade secrets handbrake to a governance process but to a genuine protection; and (ii) expanding the security hand brake to include cybersecurity issues.*

: Advises limiting the level of detail in open geospatial data because location information is easily misused, particularly regarding critical infrastructure and national security.

> *It is essential consider the requirements for the level of detail thoroughly by the opening geospatial data (especially in relation to critical infrastructure and issues of national security and defense).*

Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg: Calls for rules in the Data Act to prevent disclosure of sensitive industrial information in order to avoid competitive distortions.

> *Secondly: In order to protect the industry, the Data Act would require rules to prevent the disclosure of sensitive information and thus potential distortions of competition.*

EuroGeographics: Notes that achieving effective anonymisation remains difficult and costly, posing ongoing challenges to secure, compliant data sharing.

BusinessEurope: Calls for stronger and clearer protection of trade secrets within data sharing frameworks to prevent leakage of competitive know-how.

Federation of Austrian Industries: Advocates robust, enforceable safeguards to protect trade secrets and proprietary information when data access is mandated.

IBM: Stresses that data sharing must safeguard intellectual property and incorporate strong security measures.

Confederation of Norwegian Enterprise (NHO): Emphasizes the need to protect trade secrets and ensure cybersecurity when sharing data across ecosystems.

Polish Confederation Lewiatan: Warns that forced data sharing can jeopardize confidentiality, intellectual property, and competitiveness without adequate safeguards.

International Federation of Reproduction Rights Organisations (IFRRO): Urges safeguarding copyright in data use and setting clear limits on text and data mining to prevent rights infringements.

Association des Constructeurs Européens de Motocycles: Highlights risks that data access obligations expose trade secrets and intellectual property of manufacturers.

CECIMO - European Association of Manufacturing Technologies: Calls for tailored protections for industrial know-how and sensitive manufacturing data within data governance rules.

Broadcom: Warns that holding and sharing sensitive data entails security and competitive risks that require strong protections.

CIO Platform Nederland: Cautions that the Data Act could inadvertently create or reveal personal data, increasing privacy and compliance risks.

Österreichische Notariatskammer: Argues that data sharing must include strong security, confidentiality, and professional secrecy safeguards to protect stakeholders.

LA POSTE: Proposes adjustments to the Data Act to better protect trade secrets and confidential business information.

APPLiA (Home Appliance Europe): Warns that the Data Act risks exposing trade secrets and analytical insights; calls for pre-disclosure safeguards and binding secrecy obligations on third-party recipients.

2.4.6 Data Intermediaries, Platforms & Market Governance

This category frames platform and market governance around data intermediaries by assigning clearer accountability to powerful service providers. Proposals introduce a quasi-controller status for large platforms and cloud suites that design processing defaults and leave controllers little room to instruct, and that have their own commercial interest in data use. Addressing concentration in ad tech and platform dominance is seen as essential to restoring data sovereignty and fair bargaining power. Market-facing safeguards include pre-market verification via a public EU register of responsible persons and a Unique Operator Identifier aligned with Digital Product Passport standards, so platforms can check responsibility before products are listed. At EU level, a Commission-controlled, public, user-friendly database would define data trading and its risks, register large and very large data traders and processors assisting data trading, and flag unfair, non-negotiated data terms. Cooperation frameworks with data intermediaries are encouraged while clarifying that cooperation should not be mandatory. Policy coherence is stressed to avoid duplications between sectoral proposals such as FIDA and existing DGA intermediary regimes, and to clarify nonprofit requirements for data altruism models so data trusts are credible. Real-world imbalances, such as farmers facing impossible choices under current platform arrangements, illustrate why interoperable governance, accountability, and registries are needed to make data sharing trustworthy and equitable.

> *The concept of a quasi-controller should be introduced to better reflect the role and responsibilities of platform providers, especially large cloud service providers.* (Technology Industries of Finland)

> *For example, in services like Microsoft 365, the customer acting as the controller may have little to no ability to influence how the provider delivers the service.* (Technology Industries of Finland)

A quasi-controller would have responsibilities similar to those of a data controller, recognising that these providers often determine how personal data is processed through the design of their products or services, without leaving meaningful room for the actual controller to give instructions. (Technology Industries of Finland)

A quasi- controller also has its own commercial interest in the data processing, such as using the data to improve or develop services. (Technology Industries of Finland)

Technology Industries of Finland: Proposes creating a 'quasi-controller' accountability category for platform and cloud providers that effectively determine data processing through service design and have their own commercial interests, aligning their duties more closely with data controllers. This would better reflect platform roles and close accountability gaps in platform governance.

A quasi-controller would have responsibilities similar to those of a data controller, recognising that these providers often determine how personal data is processed through the design of their products or services, without leaving meaningful room for the actual controller to give instructions.

Adigital (Asociación Española de la Economía Digital): Calls for a public EU register of responsible persons and a Unique Operator Identifier so platforms can verify compliance before admitting products to their systems. This would strengthen market oversight and traceability in platform governance.

A public register of responsible persons in the EU should be established so platforms can verify before allowing a product on their systems, ensuring no product can enter the EU market without a responsible person.

European Law Institute: Outlines an EU-level governance framework for data trading, including a Commission-controlled, user-friendly database, clear definitions, and mandatory registration for large data traders and assisting processors. It stresses cooperation with data intermediaries, flags unfair non-negotiated data terms, and avoids imposing blanket obligations to cooperate.

Kompetenznetzwerk Datentreuhandmodelle (DatNet): Urges clarification of non-profit requirements for data altruism organizations to ensure trustworthy, workable data intermediary models. This aims to reduce legal uncertainty and support effective data sharing governance.

AK Wien: Warns that dominant ad tech platforms erode data sovereignty and fair market governance. Advocates stronger measures to curb concentration and protect users and competitors.

European Savings and Retail Banking Group: Argues that the proposed FIDA regime duplicates data intermediary provisions under the DGA, risking overlap and regulatory fragmentation. Calls for alignment to prevent conflicting governance for intermediaries.

OpenMined: Highlights that farmers face an untenable choice between participating in dominant data platforms and losing control over their data, or staying out and foregoing benefits. Suggests governance and intermediary solutions to rebalance power and protect agricultural data rights.

2.4.7 Sectoral Governance & Public Data Infrastructure

Sectoral governance is essential to ensure fair data access and interoperability within domain-specific ecosystems, especially for software-defined and connected vehicles. Stakeholders call for aligning the EU acquis with technological realities and adopting dedicated legislation—building on horizontal instruments like the Data Act—to guarantee equal, secure, and innovation-friendly access to in-vehicle data across a multi-brand aftermarket. Interoperability, standardized interfaces, and role-based access are recurring themes to prevent gatekeeping and sustain competition. Public data infrastructures face sustainability and governance challenges. EU-level open core geospatial data requires stable financing and clear governance to support continuous, high-quality releases, yet providers (e.g., national mapping and cadastre agencies) bear most costs while downstream actors capture the value; shrinking budgets compound this. Cross-administrative data sharing still lags: the once-only principle is not implemented, so citizens and SMEs must re-enter data already held by administrations, undermining efficiency and trust. Policymaking must balance openness with security and sector competitiveness. Some actors urge withdrawing broad financial data-sharing proposals amid cybersecurity risks and operational burdens, while others advocate expanding data spaces and labs to incentivize voluntary data exchange and strengthen interoperability. Across sectors, the lesson is to pair horizontal frameworks with tailored, implementable rules and adequately funded public data infrastructure.

ETRMA therefore reiterates its call for dedicated sectoral legislation on access to in- vehicle data, building on the Data Act but tailored to the needs of the automotive and mobility ecosystem. (European Tyres and Rubber Manufacturers' Association)

The acquis should be aligned with technological realities such as connected and software-defined vehicles, where data access and interoperability are key to innovation and competitio (FIGIEFA aisbl)

Once-Only principle (OOTS): not yet implemented anywhere in the EU. ()

PIU calls for the withdrawal of the draft FIDA Regulation, emphasizing that, in light of the current geopolitical and cybersecurity challenges, the European Union should focus its efforts on strengthening the protection of highly sensitive data, particularly citizens financial information. (Polish Chamber of Insurance (PIU))

FIGIEFA aisbl: Calls for EU rules to align with connected and software-defined vehicles, ensuring fair, interoperable access to in-vehicle data, especially for multi-brand aftermarket operators.

The acquis should be aligned with technological realities such as connected and software-defined vehicles, where data access and interoperability are key to innovation and competitio

European Tyres and Rubber Manufacturers' Association: Argues that horizontal rules are insufficient and urges dedicated sectoral legislation on in-vehicle data, tailored to automotive needs to secure fair access and support innovation and circularity.

ETRMA therefore reiterates its call for dedicated sectoral legislation on access to in- vehicle data, building on the Data Act but tailored to the needs of the automotive and mobility ecosystem.

National Land Survey of Finland: Warns that sustaining open core geospatial data requires EU-level financing and governance as providers bear ongoing costs amid rising demand and shrinking public budgets.

While the open data concept yields considerable benefits across the EU, financing and governance the provision of EU level open core geospatial data shall be addressed.

Polish Chamber of Insurance (PIU): Urges withdrawal of FiDA due to high costs, security risks, unclear consumer benefits, and competitiveness concerns, prioritizing protection of sensitive financial data over broad data-sharing mandates.

PIU calls for the withdrawal of the draft FIDA Regulation, emphasizing that, in light of the current geopolitical and cybersecurity challenges, the European Union should focus its efforts on strengthening the protection of highly sensitive data, particularly citizens financial information.

WKÖ - Austrian Federal Economic Chamber: Supports expanding and long-term funding of data spaces and data labs to incentivize voluntary corporate data sharing aligned with European initiatives, strengthening interoperable data infrastructure.

Data spaces and the data labs mentioned in the AI Continent Action Plan should be expanded and developed and promoted in the long term in order to incentivize the voluntary exchange of data by companies and, in coordination with European initiatives, the use and provision of data by companies.

: Notes the Once-Only principle remains unrealized, forcing citizens and SMEs to repeatedly re-enter data and exposing gaps in cross-administration interoperability and public data infrastructure.

Once-Only principle (OOTS): not yet implemented anywhere in the EU.

European Public Service Union: Advocates grounding public data governance in strong public ownership and trust to ensure accountable, citizen-centered data infrastructures.

Association of Finnish Cities and Municipalities: Calls for recognizing the public sector as an active co-creator and operator of data infrastructures and governance frameworks, not merely a data source.

Charter of Trust: Recommends leveraging existing registries such as BRIS for entity verification to streamline cross-border processes and reinforce interoperable public data infrastructure.

European Savings and Retail Banking Group: States payment service providers need access to official evidence data for services, while cautioning that FiDA is not suitable for the SIU approach, pointing to the need for fit-for-purpose sectoral governance.

OpenMined: Highlights that hospitals face barriers to pooling data, underscoring the need for governance and privacy-preserving tools that enable compliant, interoperable health data collaboration.

DIGITALEUROPE: Warns that EHDS could weaken protections and give data holders too much discretion, risking inconsistent access and undermining trustworthy, harmonized health data governance.

Enedis: Argues DSOs must retain control of the IoT data chain to ensure secure, interoperable energy operations and dependable public data infrastructure.

2.4.8 Open Data, Quality & Metadata

This category emphasizes making open data reliable, interoperable, and metadata-rich. Stakeholders call for EU-wide harmonized technical standards, common data models, shared vocabularies, and APIs for high-value datasets (e.g., skills, education, employment, geospatial, legal). Enforceable quality criteria should ensure granularity, timeliness, and reusability, supported by clear metadata, defined stewardship roles, transparent refresh cadences, and crosswalks that create synergies across compliance domains (e.g., ESG). Core datasets must be up-to-date, harmonized, easily accessible, and documented for fitness for purpose. Governance proposals stress a coherent, binding EU framework that goes beyond uneven national practices: impose common open data requirements similar to the Data Act, harmonize reuse rules, protect security while avoiding exclusive reuse arrangements, and ensure sustainable funding for core datasets. Expanding High-Value Datasets to justice/legal data and including research outputs, while improving international uptake, are seen as levers to unlock innovation and equitable access to information. Open data underpins AI and labor-market intelligence; higher standards and rich metadata enable robust, sovereign AI models and sectoral tools. At the same time, known limits (e.g., accident data representativeness) demand candid documentation, provenance, and quality controls so users can assess readiness and risks when reusing data.

The revised Open Data Directive should consider harmonized technical standards and data models for key high-value datasets, specifically concerning skills, education, and employment data. (Workday)

Therefore, enforceable quality standards should be established so that open data becomes reliable, reusable and fit for purpose. (ACEA (European Automobile Manufacturers' Association))

Too often, free data translates into incomplete, outdated, or poorly structured datasets, which severely compromise their reusability. (ACEA (European Automobile Manufacturers' Association))

By establishing binding obligations, expanding High-Value Datasets to include legal data, and harmonising reuse rules, Europe can unlock innovation, strengthen democracy, and ensure that citizens, businesses, and professionals benefit equally from access to the law. (Doctrine)

Workday: Calls for harmonised technical standards, common vocabularies, and APIs for skills, education, and employment datasets so Member States publish higher-quality, timely, granular, and interoperable open data. The goal is to enable reliable AI-driven labour market tools and upskilling programmes.

This would require Member States to collect and publish this data using common EU-wide vocabularies and APIs, significantly improving its quality, granularity, timeliness, and interoperability for reuse in AI-driven labour market tools and upskilling programmes.

National Land Survey of Finland: Stresses that core geospatial datasets must meet high quality standards—being up-to-date, harmonised, and easily accessible—to maximise reuse and interoperability.

Furthermore, core ge- ospatial datasets must be up-to-date, harmonised, and easily accessible to stakeholders.

ACEA (European Automobile Manufacturers' Association): Highlights inconsistent open data quality across Member States and warns that free datasets are often incomplete or outdated. Urges enforceable quality standards and common requirements so open data is reliable, understandable, and reusable.

Therefore, enforceable quality standards should be established so that open data becomes reliable, reusable and fit for purpose.

Doctrine: Advocates a coherent EU-level open data regime with binding obligations, harmonised reuse rules, and the inclusion of legal and justice data as High-Value Datasets. This would unlock innovation, strengthen democracy, and support robust, sovereign AI.

By establishing binding obligations, expanding High-Value Datasets to include legal data, and harmonising reuse rules, Europe can unlock innovation, strengthen democracy, and ensure that citizens, businesses, and professionals benefit equally from access to the law.

ENSHPO - The European Network of Safety and Health Professional Organizations: Notes that occupational accident datasets cannot achieve full representativeness, limiting the reliability of open data analyses. Recommends clear metadata on coverage and biases to guide appropriate reuse.

EuroGeographics: Emphasises that sustainably providing high-quality open geospatial data is costly and requires stable, long-term funding. Without it, dataset quality, freshness, and accessibility are at risk.

DigitalTrade4.EU: Promotes aligning ESG-related metadata and reporting requirements to create interoperability and reduce compliance burdens. Better metadata synergies would enhance discoverability and cross-regulatory reuse.

Inter IKEA Group: Calls for explicit data quality criteria and clearly assigned stewardship roles and responsibilities to ensure trustworthy, reusable open datasets across value chains.

Plateforme de la filière Automobile: Advocates imposing common EU-wide open data requirements on format, timeliness, and metadata to harmonise supply and enable consistent cross-border reuse.

InfoCert: Requests clear, measurable data quality metrics and defined refresh cadences (update frequencies) for open datasets so downstream services can rely on their accuracy and timeliness.

European Savings and Retail Banking Group: Observes low international uptake of open data due to uneven quality and usability. Calls for stronger standardisation and richer metadata to improve findability and reuse.

Mistral AI: Supports reinforcing open access to public data while restricting exclusive reuse agreements that undermine fair access and competition, particularly for AI training. Favors transparent governance and metadata to track availability and conditions of reuse.

Estonian Ministry of Justice and Digital Affairs: Urges security-conscious open data governance that balances openness with privacy and safety, using risk-based release policies. Recommends robust metadata for provenance, sensitivity, and access controls.

International Federation of Library Associations and Institutions: Proposes including research publications and associated bibliographic metadata within Open Data frameworks to improve discoverability, reuse, and equitable access.

2.5 Privacy, Consent and Anti-Tracking Protections

The strongest shift is toward privacy-by-default with legally binding, machine-readable signals that end consent fatigue and curb pervasive tracking and profiling. Meaningful consent requires equal prominence and easy refusal, honoring lasting choices, banning tracking walls, and plain-language transparency about purposes like ads and location. Proposals focus on standardized browser/OS settings (e.g., Global Privacy Control), limits on re-solicitation, interoperable CMPs, and prohibitions on dark patterns, while acknowledging context-specific consent and past pitfalls of unenforceable signals and fingerprinting. ePrivacy and GDPR work in tandem: protect terminal equipment and communications, then govern processing via valid legal bases, with risk-based DPIAs, caution against weakening rules, clear boundaries for law-enforcement access, and attention to AI Act overlaps. Robust anti-tracking safeguards device agency and treats location as sensitive, requiring consent, anti-fingerprinting, and strong remedies for circumvention. Profiling-based adtech is a root cause; stakeholders urge opt-in for behavioral and location ads, bans for children, and a shift to contextual first-party models. Data

minimization enforces strict necessity, purpose limitation, and proportionate sharing and retention. PETs—federated learning and on-device—embed privacy by design, without outsourcing consent to AI. Policymakers must also address business-model tensions: simplification should reduce friction without lowering protections. Across sub-categories, the trend is enforceable, user-centric controls, minimization, and device-level protections under a harmonized GDPR/ePrivacy regime, paired with curbs on profiling and clearer UX that protect ordinary users by reducing invisible data flows.

2.5.1 Legal Bases, GDPR/ePrivacy & Enforcement

This category captures how the ePrivacy framework and the GDPR complement each other: ePrivacy safeguards the confidentiality and integrity of terminal equipment and communications, while GDPR governs subsequent personal data processing. It underscores lawful bases—especially valid consent that is knowingly and freely given—and the continued importance of consent decisions and privacy-by-default to sustain trust. Stakeholders also note that media and publishing use multiple legal bases beyond consent. Compliance and enforcement are framed through a risk-based lens: data protection impact assessments are required when processing, particularly using new technologies, is likely high-risk; any revision of rules such as ePrivacy Article 5(3) should be accompanied by comprehensive impact assessments; and simplification should align with processing risk, not organization size. Relaxing ePrivacy (e.g., exempting "simple analytics" cookies) is viewed as an inadequate fix. Calls are made for clear limits on law-enforcement access, careful reforms that avoid lowering standards, and clarity on overlaps with the AI Act (e.g., when prompts are personal data). Practical challenges like information fatigue among data subjects are acknowledged alongside the need to preserve the confidentiality of communications within a harmonized legal framework.

> *But that would not be compatible with GDPR, as consent has to be knowingly and freely given.* („Internet. Time to act!" Foundation)
>
> *The requirement for consent decisions remains essential.* (Usercentrics)
>
> *Clarification is also needed on the interaction between the definition of input data under Article 3(33) of the AI Act and personal data under the GDPR (Article 4.1), when it comes to whether and under which circumstances prompts fall into the personal data category therefore triggering compliance under GDPR.* (ENGIE)
>
> *For this reason, and contrary to a common misconception, the digital press does not rely on consent and data processing only for advertising purposes.* (EMMA-ENPA)
>
> **CNIL (French Data Protection Authority):** Advocates maintaining a distinct ePrivacy regime to protect terminal equipment confidentiality, with GDPR applying to subsequent personal data processing.
>
> *First, it is essential to preserve a specific regulatory framework for operations falling within the scope of ePrivacy, since the objective of the Directive is to ensure the integrity and confidentiality of users' terminal equipment while GDPR governs the subsequent processing of personal data.*
>
> **„Internet. Time to act!" Foundation:** Emphasizes that consent must meet GDPR standards of being informed and freely given, rejecting approaches that undermine valid consent.
>
> *But that would not be compatible with GDPR, as consent has to be knowingly and freely given.*
>
> **Technology Industries of Finland:** Proposes aligning requirements by replacing a fundamental rights impact assessment with the GDPR data protection impact assessment to avoid duplication.
>
> *Art. 27: Replace the fundamental rights impact assessment with the GDPR data protection impact assessment.*
>
> **European Disability Forum:** Highlights the ePrivacy Directive as foundational for user trust online and supports robust privacy protections.
>
> *The ePrivacy Directive is a cornerstone of trust in cyberspace*
>
> **Volkswagen Group:** Supports reforms that deliver effective data protection without lowering standards or disrupting the established regulatory framework.
>
> *The aim of any reform should be to achieve effective data protection without lowering standards or fundamentally altering the established regulatory framework.*

EMMA-ENPA: Clarifies that digital press data processing relies on multiple legal bases and purposes beyond advertising and consent.

For this reason, and contrary to a common misconception, the digital press does not rely on consent and data processing only for advertising purposes.

German Insurance Association: Observes that extensive GDPR transparency information often exceeds what data subjects want or engage with in practice.

In practice, however, data subjects are often not interested in the extensive infor- mation as outlined in the GDPR and the EDPB guidelines.

Government Office of the Czech Republic: Calls for amending ePrivacy to clearly delineate lawful access for authorities to certain data, coordinated at EU level.

Finally, to meaningfully implement the conclusions of the High-Level Group on "Lawful Access to Data", it is likely necessary to amend the ePrivacy Directive to clearly define the limits of law enforcement and judicial authorities' access to certain types of data, rather than treating such access merely as an exception to the right to privacy; this should be coordinated within the responsible services of the Commission.

ENGIE: Requests clarity on when AI prompts constitute personal data under GDPR, triggering compliance obligations.

Clarification is also needed on the interaction between the definition of input data under Article 3(33) of the AI Act and personal data under the GDPR (Article 4.1), when it comes to whether and under which circumstances prompts fall into the personal data category therefore triggering compliance under GDPR.

Centre for Democracy and Technology Europe: Stresses that DPIAs must be conducted prior to high-risk processing, particularly when using new technologies.

Required prior to the processing, where processing in particular using new technologies is likely to result in high risk to rights and freedoms of individuals

BEUC - The European Consumer Organisation: Welcomes the proposed ePrivacy Regulation to strengthen privacy in electronic communications.

BEUC welcomes the Commission proposal for a Regulation on Privacy and Electronic Communications ("e-Privacy Regulation").

Centre for Information Policy Leadership (CIPL): Advocates risk-based simplification of obligations tied to processing risk rather than organisation size.

Simplification should be driven by the level of risk associated with data processing activities, not solely focused on organisation size.

egta - the international trade body of multiplatform TV and audio businesses: Supports revising ePrivacy Article 5(3) but insists on a comprehensive impact assessment covering privacy gains and market effects.

A revision of Article 5(3) of the ePrivacy Directive, while necessary, should be accompanied by a comprehensive impact assessment, to properly assess the opportunities to improve privacy as well as the economic consequences of the proposed changes on the digital and media markets.

The Danish Consumer Council: Warns that unsubstantiated deregulatory changes could create harmful incentives and undermine confidential communications.

This suggestion therefore lacks concrete data to support its supposed benefits to companies and does not account for any bad incentives being created as a byproduct, which could harm users right to confidential communication.

FiCom ry: Urges preserving confidentiality of communications within a harmonized legal framework covering all providers, technologies, and uses.

The principle of confidentiality of communications should be preserved and integrated into a harmonized legal framework that encompasses all communication providers, technologies, and usages (e.g., the DNA).

WKÖ - Austrian Federal Economic Chamber: Suggests extending GDPR privacy-by-default to template and newsletter system providers, akin to product safety requirements.

It would also be worth considering extending the "privacy by default" principle pursuant to Article 25 of the GDPR to manufacturers/providers of templates, such as website templates or newsletter distribution systems, as a kind of product safety regulation.

Didomi: Opposes easing ePrivacy (e.g., exemptions for analytics cookies), arguing such changes would not resolve underlying issues.

Calls to ease ePrivacy rules, for instance by exempting simple analytics cookies, would also fail to solve the problem.

2.5.2 Data Minimization, Identifiability & Sharing Controls

This category centers on collecting, processing, sharing, and retaining the least amount of data needed to achieve a clearly defined, lawful purpose. It emphasizes strict necessity tests (including zero-questions-style assessments), purpose limitation, and direct measurement to avoid ancillary data capture, alongside forbidding pretextual collection such as harvesting contact details without genuine need. Identifiability is actively constrained by default through aggregation and pseudonymisation, with a caution that pseudonymised data remains within the regulatory perimeter and that broad exemptions, misreadings of personal data definitions, or GDPR-classification loopholes must not be used to weaken protections. Sharing and disclosure are tightly constrained: only the minimum data per request should be provided, retention must be targeted and proportionate, and foreseeable third-party misuse must be considered before granting access. Sectoral examples illustrate the stakes: do not compel raw search query histories; avoid dissemination of raw medical data; and in finance, expansive availability mandates or lengthy historical windows (e.g., seven years) risk eroding privacy. Overall, the approach rejects blanket increases in data availability in favor of precise, least-data solutions with strong disclosure controls and accountability.

At the same time, this minimises the risk compared to the use of fully identifiable personal data. ()

Search and discovery services: Need structured, machine-readable metadata (e.g., publisher identifiers, standardised tags, access logs) but should not be compelled to disclose raw query histories that can expose personal data. (Siinda)

Siinda: Advocates that search and discovery services provide structured metadata but must not be compelled to disclose raw query histories that could expose personal data, supporting strong minimization and identifiability controls.

Search and discovery services: Need structured, machine-readable metadata (e.g., publisher identifiers, standardised tags, access logs) but should not be compelled to disclose raw query histories that can expose personal data.

: Supports pseudonymisation to reduce risks compared to processing fully identifiable personal data, reinforcing data minimization and sharing controls.

At the same time, this minimises the risk compared to the use of fully identifiable personal data.

ENSHPO - The European Network of Safety and Health Professional Organizations: Affirms that data minimization protects privacy and mitigates tracking and identifiability risks.

European Law Institute: Urges prevention of foreseeable third-party misuse, prefers direct measurement that avoids unnecessary processing, and forbids pretextual collection of contact details to tighten minimization and sharing controls.

DigitalTrade4.EU: Calls for strict controls on data disclosure to prevent unnecessary sharing and limit identifiability.

MedTech Europe: Recommends limiting data sharing that could be unsafe or privacy-compromising, especially in healthcare contexts.

Association des Constructeurs Européens de Motocycles: Advocates sharing only the minimum data necessary per request with clear purpose limitation.

Public Defender of Rights: Promotes assessing necessity from a zero-data baseline, justifying each data element to enforce minimization.

Movement for an Open Web: Warns that deregulating pseudonymised data weakens protections, clarifies identifiability principles, and corrects misinterpretations of the personal data scope.

CLEPA: Highlights risks of circumventing protections via GDPR personal data classification and urges robust controls to prevent identifiability through loopholes.

European Digital Rights (EDRi): Critiques broad exemptions and reliance on anonymisation that may fail, advocating stronger minimisation and limits on data sharing.

Siemens Healthineers AG: Alerts to risks from disseminating raw medical data that can enable re-identification, calling for tight controls and minimisation.

European Savings and Retail Banking Group: Argues FiDA proposals risk eroding privacy through excessive access and retention and deems a seven-year historical limit disproportionate to minimisation principles.

AI Accountability Lab (AIAL), Trinity College Dublin: Rejects increasing data availability to organisations, advocating minimisation and strict sharing limits to protect privacy.

BUGLAS e.V.: Supports allowing only targeted retention necessary for specific purposes, rejecting blanket retention.

2.5.3 Consent UX, Transparency & User Choice

This category captures design and policy practices that make consent meaningful, balanced, and easy to exercise. Enforcement of existing rules and UX that make rejecting as easy as accepting (equal prominence and standardized refuse options) are central, alongside honoring persistent choices in both directions and prohibiting coercive tracking walls. Transparency must be practical, accessible, and genuinely informative: plain-language notices, centralized mechanisms where appropriate, and disclosures that clearly surface purposes like advertising and location uses without hiding them behind extra clicks or bundling multiple purposes. Stakeholders warn that dark patterns and manipulative cookie banners drive cookie fatigue, nudging users toward opt-in through pressure, repetition, or defaults, which undermines freely given, informed consent and EU fundamental-rights standards.

The focus should be on more rigorous enforcement and clarifying that rejecting consent must be as easy as granting it buttons for refuse consent should be equal in size, color, and visibility to the accept consent option. („Internet. Time to act!" Foundation)

For example, `tracking walls' should be explicitly prohibited. (BEUC - The European Consumer Organisation)

While we do not see the need, should the Commission nonetheless envisage clarifying so-called 'persistent choices', it must ensure that this applies both ways. (EMMA-ENPA)

Examples from publications show that that up to 90% of readers of digital press publications are not continuously confronted with consent requests. (EMMA-ENPA)

„Internet. Time to act!" Foundation: Calls for enforcing existing rules and ensuring that rejecting consent is as easy and prominent as accepting it. Equal design and visibility for refuse and accept options are emphasized.

The focus should be on more rigorous enforcement and clarifying that rejecting consent must be as easy as granting it buttons for refuse consent should be equal in size, color, and visibility to the accept consent option.

EMMA-ENPA: Argues that any clarification of persistent choices must apply symmetrically and that repeat consent prompts are less frequent than commonly claimed. Emphasizes user choice durability in both directions.

While we do not see the need, should the Commission nonetheless envisage clarifying so-called 'persistent choices', it must ensure that this applies both ways.

FEBIS: Advocates practical, scalable transparency, favoring centralized privacy notices for B2B and sole traders over impractical individual notifications. Seeks clarity without overwhelming data subjects.

For B2B data uses-especially those involving sole traders-centralized privacy notices and public transparency mechanisms should be preferred over individual notifications that may be impractical or lead to confusion, in line with Article 14(5)(b) GDPR.

BEUC - The European Consumer Organisation: Urges human-centric privacy with clear, granular, and non-deceptive consent practices, exposing manipulative nudges, bundling, and hidden disclosures. Calls to explicitly ban tracking walls to protect genuine choice.

Explicitly ban 'tracking walls' which oblige users to consent to the monitoring of their activities in exchange for unrestricted access to a certain website.

CERMI: Stresses universally accessible consent management and plain-language, multi-format information so all users can make informed decisions. Emphasizes universal design principles for consent UX.

Any simplified or centralised mechanism for managing cookies and other tracking technologies must be designed following universal design principles.

: Critiques dark-pattern pressure from repeated consent prompts that push users to accept tracking. Condemns the normalization of non-ethical pressure despite business incentives.

This needs to be done on every visit to the website, unless consent is given, which is yet another form of pressure to consent to be tracked.

: Recommends standardized, clearly labeled consent options with an equally prominent Refuse button. Consistent order, colors, and dimensions are proposed to improve user comprehension and choice.

I think that a clearer 'Refuse' button would suffice, perhaps with graphic standardisation obliging sites to have symbols, to express the options 'Accept', 'Refuse' or 'customise' always in the same order and with identical buttons such as colours and dimensions.

Deutscher Caritasverband e.V.: Urges preventing manipulative cookie consent designs and requiring plain-language transparency about data uses. Seeks to ensure informed, non-coerced decisions.

: Criticizes intrusive cookie banners and Pay-or-Okay models that pressure users into consent. Calls for approaches that preserve free choice.

Ingka Group IKEA: Warns about consent fatigue and the need to design mechanisms that reduce repeated prompts and burden. Prioritizes user-friendly consent flows.

European Law Institute: Calls to prohibit dark patterns and designs that induce unlawful consent, ensuring interfaces do not force GDPR breaches. Urges balancing transparency with confidentiality and addressing misunderstandings about consent risks.

German Property Federation: Proposes simplifying privacy notices with pictograms to enhance user understanding and informed choice. Aims to make key information quickly graspable.

U.Di.Con. APS UNIONE PER LA DIFESA DEI CONSUMATORI: Seeks solutions to cookie fatigue and better consent mechanisms that respect user autonomy. Emphasizes clearer, less burdensome choices.

: Advocates removing cookie banners in favor of less intrusive, more effective consent approaches. Aims to reduce annoyance while preserving user control.

Danish Society of Engineers (IDA): Urges maintaining strong consumer protection within cookie consent regimes. Emphasizes transparency and meaningful, non-coerced choice.

Federation of German Consumer Organisations (vzbv): Supports conditionally reducing consent prompts without undermining transparency, warning against consent-free expansions. Recommends short texts and pictograms for clarity.

Advertising Information Group: Highlights consent fatigue and questions whether abstract preference signals reflect informed intent. Calls for mechanisms that truly capture user choices.

: Warns that opaque, complex cookie banners marginalize users and obstruct informed consent. Calls for clearer, more inclusive design.

AK Wien: Contends that claims of widespread consent fatigue are often manufactured and points to dark patterns driving acceptance. Urges stricter controls on manipulative designs.

Movement for an Open Web: Emphasizes strong information duties to ensure genuinely informed consent and user control. Advocates transparency as the foundation of choice.

The Center for Countering Digital Hate: Advocates straightforward opt-out options and greater user control over data. Seeks to make refusal as accessible as acceptance.

Homo Digitalis: Supports robust cookie banner rules to safeguard privacy and ensure authentic user choice. Opposes manipulative consent flows.

EUROCINEMA: Favors opt-in/opt-out mechanisms over compelled consent, reinforcing user autonomy. Opposes coercive access conditions.

European Digital Rights (EDRi): Asserts that deceptive consent banners violate the law and undermine user autonomy. Calls for enforcement against unlawful dark patterns.

Usercentrics: Promotes transparent, accountable consent communication to build trust and compliance. Emphasizes clarity about data uses and choices.

noyb: Insists simplification must not weaken rights and condemns dark patterns that drive consent fatigue. Calls for reforms that protect data subjects' agency.

European Savings and Retail Banking Group: Notes significant challenges in implementing permission dashboards for consent management at scale. Warns of usability and operational burdens.

Open-Xchange AG: Reaffirms that established consent principles remain valid and should guide UX changes. Cautions against shortcuts that dilute informed choice.

Euroconsumers: Calls for standardized data protection icons and warns that legalistic language reduces notice effectiveness. Seeks clearer, more user-centric disclosures.

Skyscanner: Observes widespread user misunderstanding of cookie consent, indicating the need for clearer UX. Encourages simplification and education.

: Encourages preserving user attention and reporting unfair, manipulative interfaces. Supports accountability for deceptive consent designs.

AI Accountability Lab (AIAL), Trinity College Dublin: Urges preventing coercive misuse of consent while cautiously supporting streamlined processes that maintain protections. Emphasizes preserving meaningful choice.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Recommends clear purpose labeling for cookies, warns about opt-out fatigue, and stresses informed decisions. Seeks transparent, comprehensible consent flows.

Access Now Europe: Highlights consent fatigue and dark patterns, noting that deceptive consent interfaces violate the law. Calls for stronger enforcement and user-centric design.

INRIA and Utrecht University: Advocates reducing cookie consent fatigue and identifies dark patterns in banners. Finds many transparency disclosures ineffective for enabling informed consent.

2.5.4 Consent Signals, Standards & PIMS

Stakeholders converge on reducing consent fatigue by introducing binding, automated privacy signals and standardized settings that can be honored across services under the GDPR and ePrivacy regime. Proposals include limiting re-solicitation (e.g., one-year cooldown), enabling consent or objection via software/browser settings, and making signals legally effective so that users avoid repetitive popups while their choices remain enforceable and respected. There is active debate over centralising consent at the browser or OS level. Proponents argue for simple, standardised signals (including binary tracking preferences and the Global Privacy Control) to make choices portable and automatic. Critics—particularly publishers and AdTech—warn that valid consent must be specific, informed, and context-dependent; that centralised gatekeeping risks revenue, trust, and ill-advised user choices; and that consent given to a service must not be overridden by software or external managers. Past efforts like Do Not Track illustrate pitfalls of non-enforceable signals and unintended fingerprinting risks. Emerging common ground points to machine-readable, legally binding signals and PIMS that are technology-neutral and user-friendly; interoperable CMPs for cross-domain consistency; bans on dark patterns and "popup harassment" once a signal is present; automated withdrawals with durable, traceable records; and public interfaces to ensure recognition, implementation, and compliance across the ecosystem.

GPC is very simple: it works via an automated technical signal and when re- ceived in an applicable jurisdiction it cre- ates a single-controllership situation. ()

The possibility to express consent by using the appropriate technical settings of software enabling access to the internet (Article 9.2) should also help reduce the number of consent requests, as long as service providers do not systematically request separate consent for privacy invasive purposes such as tracking for targeted behavioural-based advertising. (BEUC - The European Consumer Organisation)

Ultimately, the DNT initiative was abandoned because: 1) there was no effective way to enforce compliance by websites, and 2) it increased the potential for tracking scripts to infringe on user privacy, by adding one more bit of information to fingerprinting scripts. („Internet. Time to act!" Foundation)

As such, where individual consent is required by law, it must be a fundamental principle to ensure that publishers can obtain and manage consent in a practical manner (i.e., right to request; no prohibition on requesting), and that any consent given is directly implemented and cannot simply be ignored by software settings, consent managers or other gatekeepers (e.g., obligation to implement for browsers, personal consent management tools, etc.) (EMMA-ENPA)

CNIL (French Data Protection Authority): Advocates rules to reduce consent fatigue by limiting re-prompting after refusals and respecting user signals, favoring non-identifying tracking methods. Emphasizes a defined cooldown period to make choices effective.

In order to reduce the so-called "consent fatigue" caused by repeated consent requests, it would be useful to introduce into the regulation - in line with what is already provided for under the Digital Markets Act (DMA) - a rule ensuring that users who have refused or withdrawn their consent cannot be asked again for a certain period of time.

„Internet. Time to act!" Foundation: Warns that centralized consent standards and fixed purpose catalogs are impractical and can harm privacy, citing the failure of DNT and fingerprinting risks. Argues against simplistic browser-level signals.

Ultimately, the DNT initiative was abandoned because: 1) there was no effective way to enforce compliance by websites, and 2) it increased the potential for tracking scripts to infringe on user privacy, by adding one more bit of information to fingerprinting scripts.

: Promotes Global Privacy Control as an automated browser signal compatible with GDPR/ePrivacy, creating binding obligations and reducing popups. Positions GPC as a corrective to DNT's shortcomings.

GPC is very simple: it works via an automated technical signal and when re- ceived in an applicable jurisdiction it cre- ates a single-controllership situation.

EMMA-ENPA: Insists publishers must be able to request, obtain, and implement consent in practice, with user choices enforced and not overridden by software or gatekeepers. Calls for obligation on browsers and tools to respect consent.

As such, where individual consent is required by law, it must be a fundamental principle to ensure that publishers can obtain and manage consent in a practical manner (i.e., right to request; no prohibition on requesting), and that any consent given is directly implemented and cannot simply be ignored by software settings, consent managers or other gatekeepers (e.g., obligation to implement for browsers, personal consent management tools, etc.)

Amazon: Opposes centralized browser or OS-level consent controls, arguing preferences are context-specific and centralization misrepresents user intent. Warns such shifts won't solve consent fatigue properly.

Efforts to reduce consent fatigue should not involve shifting to centralised user controls such as browser, or OS-level consent management systems.

BEUC - The European Consumer Organisation: Supports binding consent via technical settings to reduce requests, requiring comprehensive information and forbidding bypassing user choices. Emphasizes fewer prompts without privacy-invasive exceptions.

Comprehensive and fully visible information is also necessary to ensure valid consent and it should not be possible to "bypass" the choice made by the user in the settings.

egta - the international trade body of multiplatform TV and audio businesses: Warns centralized consent would undermine publisher revenues and cede control to potential bad actors, risking privacy and trust. Calls for preserving direct relationships with audiences.

Centralised consent would have a negative impact on publishers' revenue streams, as well as ceding control to potential bad actors.

: Proposes a standardized signal for expressing personal data collection preferences once and sending them with web requests. Envisions a simple binary "do not track" choice.

This could be as easy as a binary value: I do not want to be tracked: yes/no.

: Notes low public awareness of privacy plugins and that DNT wasn't respected, advocating a browser-based solution to improve user control. Sees built-in approaches as more scalable.

For this reason, I strongly support a browser-based solution.

Anitec-Assinform: Criticizes a narrow focus on cookie rules and opposes shifting to centralized browser/OS consent management to reduce fatigue. Calls for more ambitious, context-aware approaches.

Efforts to reduce cookie fatigue should not involve shifting to centralized user controls such as browser- or OS-level consent management systems.

Didomi: Argues browser-level centralization is unworkable under GDPR's specificity and information requirements, proposing interoperable cross-domain CMPs to reduce banner fatigue. Emphasizes consistent preferences across sites.

From our perspective, the only viable way to reduce banner fatigue while preserving user protection is cross-domain consent.

: Encourages adoption of Global Privacy Control as a standardized, binding privacy signal for consent and opt-out across services. Sees GPC as a practical way to embed user choices.

European Law Institute: Proposes automated consent and rights functions, a mandated one-year consent expiry, durable machine-readable records, and public interfaces to improve traceability and enforcement. Addresses expiration, evidence, and accessibility gaps.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Calls for stronger, clearer consent standards and practical guidance to ensure consistent implementation of privacy signals and PIMS. Aims to reduce ambiguity in compliance.

: Suggests a simplified two-choice cookie consent standard to streamline decisions and reduce fatigue while remaining legally valid. Focuses on usability and clarity.

Federation of German Consumer Organisations (vzbv): Advocates legally binding centralized preference signals to protect consumers, noting voluntary tools tend to favor AdTech interests. Seeks enforceable recognition of user choices.

Ecommerce Europe: Critiques centralized consent tools as ill-suited to contextual preferences and potentially burdensome for compliance. Urges caution in mandating such mechanisms.

European Broadcasting Union: Highlights risks from centralized consent gatekeepers and calls for safeguards ensuring user choices are reliably implemented. Emphasizes publisher ability to honor consent.

Advertising Information Group: Opposes centralized consent gatekeeping that can override or block user-publisher consent flows. Supports direct, transparent implementation of choices.

: Supports implementing standardized, legally grounded machine-readable consent signals to increase ease and legal certainty. Sees standards as clarifying obligations for all parties.

Because it will create ease and legal certainty.

MVFP Medienverband der freien Presse e.V.: Rejects centralized consent schemes, arguing they don't reduce fatigue or reflect context, and calls for practical management with enforceable implementation. Emphasizes publisher control and compliance.

Agilitation: Endorses interoperable third-party CMP solutions to manage consent across domains and contexts beyond cookies. Argues consent management should cover broader processing activities.

German Newspaper Publishers and Digitalpublishers Association (BDZV): Opposes centralized browser-level consent, favoring publisher-managed solutions reflecting contextual specificity and user choice. Warns against one-size-fits-all settings.

MFE-MEDIAFOREUROPE N.V.: Warns against centralization and unauthorized data scraping, emphasizing authorized, auditable consent processes. Calls for safeguards against misuse.

European Digital Rights (EDRi): Urges legal recognition and embedding of privacy preference signals like GPC to reduce manipulative prompts and enforce user rights. Supports binding, standardized signals.

Usercentrics: Argues universal centralized consent cannot meet GDPR specificity and information requirements, advocating interoperable CMP approaches. Seeks user-centric, compliant mechanisms.

noyb: Supports binding, standardized automated privacy signals to enable efficient opt-outs and withdrawals and curb dark patterns. Promotes enforceable, user-friendly standards.

European Publishers Council: Criticizes centralized consent systems that threaten publisher autonomy and user trust, calling for practical direct implementations of user choices. Favors context-specific management.

ACT (Association of Commercial Television and Video on Demand Services in Europe): Opposes centralized gatekeeping and urges frameworks enabling direct, enforceable consent between users and services. Prioritizes transparency and control.

Open-Xchange AG: Recommends banning dark patterns and mandating standardized, user-friendly browser consent mechanisms to reduce fatigue and improve control. Encourages tech-neutral standards.

Skyscanner: Finds browser-level cookie preferences flawed and insufficiently granular, recommending alternatives that reflect context and purpose. Seeks more precise controls.

: Calls for EU-level standardisation of consent signals and tooling to ensure consistent compliance and user protection. Aims for uniform practices across markets.

AMETIC: Rejects centralized consent management in browsers or OS, favoring solutions that respect contextual differences and industry practicalities. Warns against one-size approaches.

AI Accountability Lab (AIAL), Trinity College Dublin: Advocates automated privacy signals (e.g., GPC, ADPC) that prevent popup harassment, bind future processing, and enable instant withdrawals across contexts. Promotes legal duties triggered by signals.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Calls for technology-neutral, user-friendly PIMS-based signals and recognition of PIMS within evolving standards. Supports dynamic, empirically informed approaches.

Ada Lovelace Institute: Highlights failures of current cookie consent practices and recommends mandating standardized browser-level settings to reduce manipulation and fatigue. Seeks stronger defaults and enforcement.

Access Now Europe: Supports legally binding privacy signals like GPC to curb manipulative consent flows and strengthen user autonomy. Emphasizes machine-readable, enforceable choices.

Confederation of Swedish Enterprise: Urges maintaining robust consent standards ensuring specificity and informed choice while accommodating practical business needs. Warns against diluting requirements.

INRIA and Utrecht University: Proposes standardized browser consent management grounded in empirical user preferences on tracking, aligning signals with actual intent. Seeks usable, compliant mechanisms.

2.5.5 Privacy-Enhancing Technologies & AI Safeguards

Stakeholders converge on embedding privacy-enhancing technologies and safeguards across the AI lifecycle. They advocate privacy by design/default and practical PETs—such as federated learning and on-device processing—to minimize data flows, align with GDPR, and reduce compute demand while supporting innovation. Calls for clearer legal bases (e.g., amending GDPR Article 9) focus on enabling AI training and commercialization with robust protections against sensitive-data leakage, particularly in health contexts. Balancing Access by Design with Privacy by Design is emphasized, noting the limits of pseudonymization and the need to avoid undermining data-subject rights. There is caution against weakening protections or outsourcing consent decisions to AI. Consumer groups urge strong privacy-by-default across browsers, operating systems, apps, and connected devices to curb cross-device tracking, and warn that expanding exceptions is unlikely to spur PET investment without evidence. Others highlight that AI agents cannot deliver truly informed, specific consent given inconsistent processing taxonomies, and that trusting automated systems with legal-ethical nuance is premature. Overall, PETs are promoted to enhance privacy rights and prevent surveillance creep, while guidance and incentives are sought to increase adoption and overcome industry reservations.

Lastly, on data legislation, we encourage the Commission to prioritize, or where possible require, federated learning and on-device processing. (Encode Europe)

Embedding data protection measures and privacy enhancing technologies directly into the design of information technologies, systems and services. (BEUC - The European Consumer Organisation)

We are not aware of any evidence supporting the causal connection that broadening exceptions for companies somehow incentivizes them to invest in privacy enhancing technology. (The Danish Consumer Council)

In case of doubt, give precedence to the right of data access when personal data is pseudonymized in accordance with recognized standards. (Bitkom e.V.)

DigiFinland: Proposes clarifying GDPR to permit AI training on personal data with strong safeguards, particularly for sensitive contexts like rare diseases. Aims to accelerate safe AI adoption and commercialization without compromising safety or data protection.

Consider amending Article 9 of the GDPR to explicitly allow the processing of personal data for AI training and development, while ensuring robust safeguards against the leakage of sensitive information, especially in rare disease contexts.

Encode Europe: Urges prioritization or requirements for federated learning and on-device processing to protect privacy, help entrepreneurs, and reduce compute demand in line with GDPR. Emphasizes PETs-first approaches for responsible AI.

Lastly, on data legislation, we encourage the Commission to prioritize, or where possible require, federated learning and on-device processing.

Bitkom e.V.: Argues Privacy by Design and Access by Design can be reconciled if planned from the outset, while ensuring data subject rights are not undermined. Notes pseudonymized data still triggers GDPR duties, requiring careful safeguards.

Moreover, Privacy by Design and Access by Design do not have to be contradictory if both principles are considered together from the outset.

BEUC - The European Consumer Organisation: Criticizes the lack of privacy-by-default obligations and calls for default high-privacy settings across browsers, operating systems, apps, and connected devices to prevent tracking. Warns the current approach could undercut GDPR Article 25.

The settings of all end-users' devices and software shall be configured to provide the highest level of privacy protection from the outset and prevent tracking of users' activities by third parties.

The Danish Consumer Council: Disputes claims that broadening processing exceptions will incentivize investment in PETs, citing a lack of evidence. Cautions against weakening protections based on unproven assumptions.

We are not aware of any evidence supporting the causal connection that broadening exceptions for companies somehow incentivizes them to invest in privacy enhancing technology.

Adigital (Asociación Española de la Economía Digital): Emphasizes protecting personal data across the entire AI lifecycle, aligning with regulator guidance. Calls for lifecycle-wide safeguards as AI systems are developed and deployed.

Others, like France's authority, stress the need to protect personal data throughout the Al lifecycle.

WKÖ - Austrian Federal Economic Chamber: Advocates federated learning and differentiated data protection to enable decentralized ML while safeguarding IP and trade secrets. Urges wider promotion of these PETs to unlock data-driven AI potential.

Technologies such as federated learning and differentiated data protection offer effective solutions to enable machine learning on decentralized data while protecting intellectual property and trade secrets.

Didomi: Rejects delegating consent choices to AI agents, arguing that without standardized purposes and mature capabilities, automation cannot provide informed and specific consent. Highlights legal and ethical risks of premature reliance on AI for consent.

Trusting AI systems to interpret legal and ethical nuances reliably is premature and risky.

ENSHPO - The European Network of Safety and Health Professional Organizations: Encourages innovation using privacy-preserving techniques while acknowledging tensions between GDPR data minimization and AI safety needs. Calls for balanced safeguards that protect rights without stifling safety-related uses.

European Law Institute: Calls for robust consent standards and limits on identity cloning, while maintaining protections against sensitive attribute inference. Supports strong guardrails on AI use of personal data to prevent harm.

Milestone Systems: Highlights differing modes of biometric processing and their privacy implications, advocating context- and risk-tailored safeguards. Stresses proportionate controls to protect individuals in biometric use cases.

Ecommerce Europe: Argues that the current consent regime discourages adoption of PETs. Seeks reforms that enable privacy-enhancing solutions while preserving user protection and trust.

AK Wien: Warns that misclassifying AI-related data or purposes can undermine GDPR protections. Urges precise definitions and enforcement to maintain privacy safeguards in AI contexts.

Digital Currencies Governance Group (DCGG): Assesses certain CSAM detection proposals as technically unfeasible and harmful to end-to-end encryption, threatening core privacy safeguards. Advocates rights-preserving alternatives that do not erode PETs like strong encryption.

Insurance Europe: Calls for clear legal bases and robust safeguards for using personal data in AI training. Seeks a balance that enables innovation without compromising data protection obligations.

Usercentrics: Recommends stronger guardrails for AI-driven consent mechanisms to ensure transparency, specificity, and user control. Emphasizes preserving meaningful consent in automated interfaces.

AI Accountability Lab (AIAL), Trinity College Dublin: Warns that rapid AI adoption risks expanding mass surveillance. Urges deploying PETs to enhance privacy rights and mitigate systemic surveillance harms.

Estonian Ministry of Justice and Digital Affairs: Proposes practical guidelines and standards to implement privacy-enhancing technologies for compliant, trustworthy AI. Aims to operationalize PETs across sectors.

VAUNET - German Association of Private Media: Suggests opt-in or compensation models for using data in AI training to reinforce user choice and accountability. Positions consent and fair value exchange as privacy safeguards.

2.5.6 Anti-Tracking, Device & Location Protections

Anti-Tracking, Device & Location Protections center on preserving high levels of privacy by restricting tracking technologies, guarding terminal equipment, and treating location data as sensitive metadata. Regulators and advocates emphasize ePrivacy's Article 5(3) as a cornerstone safeguarding confidentiality of communications and devices across telecom and OTT services and public Wi-Fi, requiring consent before accessing or storing information on user devices or collecting emissions, with narrow, low-risk exceptions and full GDPR alignment. Because location data reveals real-time movements and sensitive inferences, the default should be explicit consent for any collection or processing, regardless of whether data comes from telecom networks, GPS, or Wi-Fi, with strong limitations, opt-outs when consent isn't needed, anonymization for public interest uses, and impact assessments. Stakeholders warn against proposals that would allow physical location tracking without consent and highlight real-world deficiencies like "Location History" settings that are hard to truly disable and retain data unless manually deleted. Effective anti-tracking also requires device agency and anti-fingerprinting: browsers should minimize exposed signals, since consent preferences can themselves be used to augment fingerprints and bypass cookie consent; service providers must not disable or circumvent user anti-tracking tools. Users should have the right to secure their equipment with best available techniques, and violations of terminal equipment protections should be treated as seriously as breaches of communication confidentiality, addressing threats like pervasive analytics, cross-device tracking, and cookie syncing.

Always consider "location data" as "metadata" and consequently, consent shall be generally required for its processing under Article 6.2 (c). (BEUC - The European Consumer Organisation)

The use by service providers of mechanisms to disable or circumvent 'anti-tracking tools' without prior consent from end-users' should be prohibited. (BEUC - The European Consumer Organisation)

Fingerprinting can be used to completely bypass lack of cookie consent. („Internet. Time to act!" Foundation)

If browsers would automatically signal to websites the purposes for which a user consents or does not consent to cookies, this adds additional bits of information that tracking scripts could exploit for fingerprinting. („Internet. Time to act!" Foundation)

CNIL (French Data Protection Authority): Calls to preserve a high level of data protection against online tracking, noting persistent user concerns and enforcement against abusive tracking.

In our view, these reflections should preserve a high level of data protection in relation to online tracking.

„Internet. Time to act!" Foundation: Warns that consent signaling and fingerprinting can bypass cookie consent, urging browsers to minimize disclosure about users, devices, and cross-site choices.

If browsers would automatically signal to websites the purposes for which a user consents or does not consent to cookies, this adds additional bits of information that tracking scripts could exploit for fingerprinting.

Civil Liberties Union for Europe: Criticizes efforts to downplay ePrivacy Article 5(3), stressing it is a core safeguard against intrusive state and corporate surveillance and not just a cookie banner issue.

However, this paragraph is a foundational element of EU digital rights law, safeguarding individuals from arbitrary or disproportionate state or commercial surveillance in numerous contexts.

BEUC - The European Consumer Organisation: Advocates strong consent-based controls over location data and device emissions, broad confidentiality across services and networks, and bans on circumventing anti-tracking tools. Calls for stricter protections and security of end-user devices, impact assessments for exceptions, and the ability to opt out.

Ensure strong protection of end-users against intrusions or interferences in their technical equipment and against online tracking.

Federation of Austrian Industries: Supports limiting the digital lifetime of identifiers and setting boundaries on monitoring to curb persistent tracking and protect privacy.

Federation of German Consumer Organisations (vzbv): Calls for strict consent requirements for accessing terminal equipment and device data, ensuring robust user control over tracking and interference.

Fedoweb - Federazione Operatori Web: Supports retaining current ePrivacy rules while limiting tracking practices, seeking proportionality that reduces intrusiveness.

Fastweb S.p.A.: Supports prohibiting harmful tracking practices and misuse of communications data, prioritizing user safety and privacy.

Skyscanner: Supports maintaining consent requirements for invasive tracking and profiling, ensuring users retain control over cross-site and device-level tracking.

: Highlights privacy risks of technical device fingerprinting and urges measures to limit unique identifiers that enable cross-site tracking.

Enedis: Urges tight restrictions on accessing and processing IoT device metadata, limiting secondary uses that could enable tracking of users and devices.

Ada Lovelace Institute: Emphasizes user and device agency in emerging environments, warns about AI-enabled browsers and fingerprinting, and calls for clear rules for privacy-enhancing technologies.

Access Now Europe: Supports strong ePrivacy protections against device tracking and interference, guarding against both commercial and state surveillance across networks and contexts.

INRIA and Utrecht University: Documents widespread analytics tracking, data leakage, and cross-device identification via cookie syncing, underscoring the need for stronger anti-tracking safeguards.

2.5.7 Adtech, Profiling & Targeted Marketing Limits

Profiling-based adtech is repeatedly identified as the driver of pervasive tracking, consent fatigue, and erosion of user choice. The industry floods users with consent prompts to maximize deployment of trackers, ties access to services to acceptance of targeted ads (including pay-or-OK models), and relies on defaults that compel data collection. Consumers are often unaware of the scope and purpose of data processing by opaque third parties, while consent banners and business models primarily serve the ad ecosystem rather than protect privacy. Stakeholders call for strong limits: opt-in is required for tracking, profiling, behavioral and location-based advertising, and for marketing communications; targeted ads and profiling should be categorically prohibited for children, with dedicated safeguards; regulators should curb mislabeling of tracking purposes and prefer contextual, first-party approaches. Normalizing tracking undermines trust and market integrity, and exceptions for profiling/marketing should be excluded. Risks are concrete: large platforms continuously collect granular data (including precise indoor location) for advertising, often by default and retained indefinitely, creating comprehensive profiles beyond reasonable user expectations. Weak cookie rules risk unlawful political tracking and manipulation. Advertising can be funded without surveillance, provided genuine consent and privacy-preserving models are used.

> *Targeted advertising is one of the main reasons of the widespread tracking and monitoring practices that consumers are subjected to online.* (BEUC - The European Consumer Organisation)
>
> *Moreover, European data protection authorities have already stated that "opt-in consent would almost always be required [...] for tracking and profiling for purposes of direct marketing, behavioural advertisement, location-based advertising or tracking-based digital market research".* (BEUC - The European Consumer Organisation)
>
> *The location data collected through Location History is derived from GPS, Wi-Fi scanning, and Bluetooth scanning, which means that Google can track a user's precise location inside buildings as well as outside.* (BEUC - The European Consumer Organisation)
>
> *Use of online advertising to spread malware.* (BEUC - The European Consumer Organisation)

„Internet. Time to act!" Foundation: Says consent fatigue is driven by ad industry practices that bombard users with prompts to enable tracking, not by privacy laws. Criticizes manipulative consent flows used to maximize tracking scripts across sites.

> *Consent fatigue is not caused by ePrivacy or GDPR regulations, but by the practices of the advertising industry, which blasts users with consent prompts to maximize the deployment of tracking scripts across websites.*

BEUC - The European Consumer Organisation: Urges strict limits on targeted advertising, including opt-in and bans on using children's data, and condemns pervasive, default-on tracking like account-level location collection. Highlights that consumers lack real choice or awareness and face significant privacy harms from profiling.

> *Targeted advertising is one of the main reasons of the widespread tracking and monitoring practices that consumers are subjected to online.*

The Danish Consumer Council: Warns that companies mislabel marketing trackers as 'statistics' to bypass consent and transparency. This undermines enforcement and enables hidden profiling.

> *This suggestion therefore risks incentivizing companies to categorize their tracking to be for simple statistical purposes, even if it isnt the case.*

: Criticizes marketing-driven cookie banners and accept-tracking-or-pay models that force targeted ads as the price of access. Calls this a misuse of user privacy and personal data.

> *I consider this practice a misuse of user privacy, as it allows companies to exploit users personal data.*

: Notes that expansive treatment of personal data and consent demands hinder analytics and attribution used for marketing. Signals a trade-off between privacy protections and adtech measurement.

EuroGeographics: Describes tracking users to tailor services, reflecting reliance on profiling for personalization. Points to the need to limit tracking while enabling basic service customization.

European Law Institute: States that targeted marketing and profiling can constitute large-scale processing requiring qualified evaluation, whereas simple service offers are not profiling. Flags risks from use of intimate social media data (e.g., in recruitment) and calls to constrain profiling.

Federation of German Consumer Organisations (vzbv): Calls to ban tracking- and profiling-based advertising due to consumer harms and erosion of trust. Endorses contextual and first-party models as privacy-preserving alternatives.

Movement for an Open Web: Advocates strong consent and clear limits on profiling in online advertising. Emphasizes user control over tracking and restraint on behavioral targeting.

noyb: Argues that consent banner ecosystems primarily benefit third-party adtech rather than users. Says current consent mechanics entrench pervasive tracking.

Open-Xchange AG: Asserts that parts of the advertising industry undermine privacy protections to sustain tracking and profiling. Urges stronger safeguards against these practices.

Skyscanner: Claims strict consent rules impede attribution and performance tracking needed for marketing. Seeks more flexible, privacy-respecting approaches to measurement.

: Warns that deregulating cookies would enable unlawful political tracking and facilitate manipulation. Emphasizes the democratic risks of data misuse in targeted influence.

AI Accountability Lab (AIAL), Trinity College Dublin: Calls to exclude exceptions that allow tracking, profiling or marketing from privacy rules, given widespread third-party tracking. Supports tighter limits on adtech data flows.

Access Now Europe: Urges comprehensive regulation of the adtech ecosystem that drives pervasive trackers and profiling. Supports stronger limits on targeted advertising to protect privacy.

2.5.8 Economic, Ecosystem & Compliance Trade-offs

Across stakeholders, there is a clear tension between safeguarding privacy and sustaining viable digital business models, with compliance design sitting at the center. News publishers argue their financing and operations depend on consent at scale and warn that centralised consent mechanisms could harm the press and broader digital economy without robust evidence or impact assessment. Others stress that duplicative or fragmented consent systems defeat regulatory goals by increasing costs and complexity, and caution that deregulation or abandoning ePrivacy sends the wrong signal about fundamental rights. Consumer advocates insist simplification must not lower protections, including vis-à-vis trade agreements. Proponents of a single-controller model (e.g., GPC) frame it as a way to reduce compliance burden, preserve first-party access to audience data, and rebalance competition away from third-party trackers—while being implementable with minimal changes via existing CMPs. At the same time, firms relying on performance and affiliate marketing warn that privacy-preserving attribution APIs severely limit data granularity, undermining validation and payments to publishers. Smaller operators note that strict opt-in improves privacy but can impose heavy costs. The throughline: simplification should reduce fatigue and compliance friction without sacrificing privacy, and policy tools must be applied strategically to meet the needs of people and businesses alike.

Ever stricter data protection laws have led to a legal framework in which the digital press can only operate, let alone be financed, with the consent of a large number of individual readers. (EMMA-ENPA)

For businesses: businesses get much reduced compliance cost - supporting GPC is the simplest compliance work I ever did, my team implemented it across 70 products in record time - and get to keep no-nonsense access to their audience data. ()

This means that, at best, transaction values can be grouped into 3 price ranges. (Sheridans, on behalf of Awin AG)

Additionally, it protects media against their audience data being reused by competitors and it protects all businesses against their data being used for AI training with no compensation. ()

„Internet. Time to act!" Foundation: Maintaining dual consent systems undermines regulatory goals by adding operational burden rather than simplifying compliance.

That would defeat the purpose of this new regulation, as website owners would have to maintain two systems for consent instead of one.

: Advocates a single-controller signal to reduce compliance costs and level competition. Warns that simplification must be strategic to avoid counterproductive outcomes.

For businesses: businesses get much reduced compliance cost - supporting GPC is the simplest compliance work I ever did, my team implemented it across 70 products in record time - and get to keep no-nonsense access to their audience data.

EMMA-ENPA: Argues centralized consent would severely damage the economics of the digital press, which depends on consent from many readers for financing. Calls for evidence and impact assessment before such changes.

The damage that centralised consent mechanisms would bring to the press sector cannot be overstated.

Civil Liberties Union for Europe: Warns that shelving stronger ePrivacy rules signals fundamental rights are negotiable, risking shifts toward corporate interests over privacy.

With the ePrivacy Directive being the main piece of legislation tackling privacy and confidentiality of communications, and with the withdrawal of the ePrivacy Regulation (the much-needed update of the Directive), the EU is sending the signal to corporations and to politicians that our rights are open for negotiation.

BEUC - The European Consumer Organisation: Urges maintaining strong consumer and privacy protections and ensuring trade rules do not erode EU data safeguards. Seeks updates that balance innovation with rights.

Trade rules must not undermine EU privacy protections or weaken data safeguards as personal data is not a commodity, and its protection is a fundamental right.'

Sheridans, on behalf of Awin AG: Finds privacy-preserving attribution mechanisms too data-poor for validation, threatening the commercial viability of affiliate marketing. Insufficient granularity impedes accurate reconciliation and payment to publishers.

In either case, this prohibits validation and makes it impossible for networks to reconcile transactions to publishers accurately, preventing publishers from being paid what they are due.

ISP Alliance a.s.: Acknowledges opt-in enhances privacy but imposes heavy costs on small site operators. Sees limited urgency for simplification in data protection for ISPs.

In summary, while opt-in increases privacy protection, for many small website operators it imposes heavy costs that may outweigh benefits.

: Warns against cookie reforms that sacrifice privacy for monetization, prioritizing citizens' rights over business data extraction.

It would be very unfortunate if the "modern approach to cookies" were to just give up on the citizens' privacy at all in favor of businesses monetizing the collected personal data.

Didomi: Supports reducing consent fatigue and simplifying compliance while maintaining strong data protection. Frames the Digital Omnibus as a chance to modernize without weakening rights.

It directly supports the Commissions dual objectives: simplifying compliance while upholding Europes high level of data protection.

: Notes GDPR rights are underused and create administrative overhead, reflecting practical inefficiencies that raise compliance burdens.

European Law Institute: Indicates consent management responsibilities shift toward non-exempt actors, altering compliance costs and obligations across the ecosystem.

VDMA - Advancing Europe´s machinery industry: Advocates a risk-based approach over uniform GDPR rules to better align compliance effort with actual risk and support innovation.

Palombar - Associação de Conservação da Natureza e do Património Rural: Warns that proposed tools and regulatory withdrawals could weaken ePrivacy/GDPR, distorting incentives and risking privacy for economic expediency.

European Public Service Union: Cautions that simplification efforts may weaken GDPR protections, undermining trust and fair competition in the digital economy.

Confederation of Norwegian Enterprise (NHO): Argues GDPR impedes effective fraud prevention, highlighting tension between privacy compliance and risk management efficiency.

Federation of German Consumer Organisations (vzbv): Recognizes GDPR's balanced framework can foster trust and innovation, yet ecosystem complexity undermines consumer control and transparency.

Salesforce, Inc.: Supports simplifying compliance without weakening data privacy to reduce burdens while preserving consumer trust.

CPME: Backs high-standard GDPR simplification that cuts unnecessary burdens but retains robust protections.

Verband der Automobilindustrie e.V.: States incoherent consent rules hinder innovation and data-driven services in automotive, calling for clearer, consistent requirements.

: Reports systemic blocking of privacy technologies by authorities, industry, and politics, limiting competitive, compliant alternatives.

MVFP Medienverband der freien Presse e.V.: Emphasizes the digital press's reliance on consent for operations and financing, making consent frameworks economically pivotal.

AK Wien: Contends prevailing models of privacy economics are flawed, mispricing externalities and producing suboptimal outcomes.

CLEPA: Highlights consent burdens that restrict fleet access to vehicle data, hampering service efficiency and market dynamics.

Skyscanner: Notes that reject-all options materially reduce revenue, illustrating direct economic impacts of stricter consent choices.

Middle Tech Europe: Asserts consent burdens on low-risk essential ad cookies are disproportionate and harm smaller publishers' business models.

DIGITALEUROPE: Claims GDPR hinders AI model training, exposing friction between privacy safeguards and innovation capacity.

Wolt: Finds consent rules skew analytics and create resource-intensive compliance burdens, complicating data-driven decisions.

Association Française des Entreprises Privées: Argues GDPR's balance supports innovation but criticizes some enforcement practices for adding excessive compliance costs.

Access Now Europe: Disputes assertions about incentivizing privacy-enhancing technologies, calling them illogical and evidence-free.

Confederation of Swedish Enterprise: States GDPR dampens innovation and growth, including cuts to pharma and biotech R&D, revealing broad economic trade-offs.

INRIA and Utrecht University: Warns that meeting formal compliance can still harm privacy, creating perverse outcomes across the data ecosystem.

2.5.9 Miscellaneous

This category highlights the tension between the benefits of digital services and the escalating risks to user privacy. While consumers gain convenience and value, the expansion of data collection and tracking creates significant challenges for protecting personal information. The insights call for stronger, broader safeguards that protect ordinary users from unintentionally or unconsciously sharing data. This implies privacy-by-default, clearer consent mechanisms, and anti-tracking protections that reduce invisible data flows and make privacy controls more accessible and effective.

> *The digital revolution has brought enormous benefits to consumers, but it has also created significant challenges for the protection of their privacy.* (BEUC - The European Consumer Organisation)
>
> *I believe we need a broader solution that protects ordinary users from unintentionally and unconsciously sharing their data.* ()

BEUC - The European Consumer Organisation: Highlights that digital advancements bring consumer benefits but also introduce significant challenges to protecting privacy, signaling the need for stronger safeguards.

> *The digital revolution has brought enormous benefits to consumers, but it has also created significant challenges for the protection of their privacy.*

: Calls for a broader, systemic privacy solution to prevent ordinary users from unintentionally and unconsciously sharing their data, implying current consent mechanisms are inadequate.

> *I believe we need a broader solution that protects ordinary users from unintentionally and unconsciously sharing their data.*

2.6 Digital Identity, Trust Services and Wallet Integrity

The strongest signal is the need for harmonized, outcome-based regulation that clarifies scope, liability, and timelines so QTSPs, wallet providers, and banks can adopt EUDIW/eIDAS 2.0 without redundant audits or fragmented obligations. Stakeholders urge replacing technology-specific rules with tech-neutral ones, streamlining qualified service assessments, and mitigating operational risks from multi-year QSCD certification cycles, while future-proofing long-term validation/preservation across root expiries and algorithm changes. Security and interoperability priorities emphasize testable minimums for identity proofing (biometrics, anti-spoofing, document authenticity, deepfake defenses), permission for unattended onboarding and qualified issuance, and reliance on proven PKI/PKD and trust registries over speculative blockchain. A trusted verification layer should scale Union-wide, protect exclusive user control, and avoid overstandardization and dependency bloat that have already delayed deployments. Governance and business sustainability are prerequisites: define roles, responsibilities, and cost-sharing among issuers, QTSPs, wallet providers, attribute authorities, and relying parties; resolve QES free-of-charge scope and unlinkability-driven billing; formalize outsourcing (e.g., SCA) and ensure interoperability with existing trust services. User protections demand transparency, voluntariness, sectoral discretion to reject insecure implementations, and inclusive design. Beyond the EU, initiatives should favor capability over compliance, privacy-by-design, clear trust anchors, and minimal, secure cross-border rails. Across all sub-categories, the common thread is pragmatic simplification: tech-neutral, testable security and interoperability, clear liability and governance, and user-centric, sustainable deployment.

2.6.1 Governance, Business Models & User Protections

Stakeholders stress that robust governance and viable business models are prerequisites for trustworthy EUDI Wallet deployment. They call for urgent legal clarification of roles, responsibilities, liability, and cost-sharing across issuers, wallet providers, QTSPs, attribute authorities, and relying parties. Ambiguities around free-of-charge QES for non-professional use and unlinkability-driven billing raise concrete disputes, while private participation depends on a clear, sustainable model. Operational governance is also highlighted: data quality and attribute refresh policies for authentic sources, formal outsourcing agreements when delegating SCA, and interoperability with existing trust services. Public investment should be preceded by sustainability assessments that leave room for competitive market operators; the European Business Wallet should be market-driven, reflect legal representation, and privilege usability over complexity, with emerging ETSI work enabling new QEAA-based value propositions. User protections cut across all recommendations. Transparency

is needed to prevent digital identity and related tools from drifting into control and classification, while tiered verification helps balance transparency with privacy. Safeguards must not be weakened by deregulation or mandates; participation should remain voluntary, with sectors (e.g., banks) empowered to reject insecure implementations. A design-for-all approach is essential so that digital identity does not exclude people from civic, social, or economic life, anchoring trust and integrity in everyday use.

> *There is an urgent need for legal clarification regarding the roles, responsibilities, and business model for actors in the EUDI Wallet ecosystem.* (Evotrust)
>
> *A major point of ambiguity is the provision for free-of-charge use of qualified electronic signatures (QES) by natural persons for non-professional use, with no clear definition of "non-professional use" and guidance on who is to bear the costs.* (Intesi Group)
>
> *A possible dispute could arise when a Relying Party requests an attestation and, due to unlinkability, cannot know who the issuer is to pay for the service.* (Intesi Group)
>
> *Operationally, it would also be practical for a QEAA QTSP to have clarity on the data quality of authentic sources and how often requests must be made to ensure attributes remain up to date.* (Evotrust)

Intesi Group: Highlights legal and economic uncertainty in the EUDI Wallet ecosystem, including unclear roles, responsibilities, and who pays for QES and attestations. Stresses that a defined business model is needed to attract private sector participation and prevent disputes caused by unlinkability.

> *There is an urgent need for legal clarification regarding the roles, responsibilities, and business model for actors in the EUDI Wallet ecosystem.*

Evotrust: Calls for legal clarity on roles and business models for EUDI Wallet actors, alongside operational guidance for data quality and attribute freshness. Emphasizes that unresolved cost allocation and technical uncertainties deter private participation.

> *There is an urgent need for legal clarification regarding the roles, responsibilities, and business model for actors in the EUDI Wallet ecosystem.*

Namirial Spa: Advocates governance measures like sustainability assessments to ensure public wallet investments are efficient and leave room for competitive, value-adding private models. Argues the European Business Wallet should be market-driven, interoperable, and support QEAA-based use cases.

> *The forthcoming European Business Wallet must be conceived as a market-driven initiative, not a public monopoly.*

CERMI: Frames accessibility as a core governance and user protection requirement for digital identity. Warns that excluding accessibility by default would marginalize people from civic and economic life.

> *An inaccessible digital identity equates to exclusion from civic, social, and economic life.*

: Warns that without transparency and safeguards, digital identity tools risk enabling unilateral control and classification. Calls for governance that prioritizes transparency of state structures to protect users.

> *Without transparency, new digital tools such as digital euro or digital identities risk being used unilaterally for control and classification, rather than first of all making the state structures themselves more transparent.*

DigitalTrade4.EU: Proposes tiered verification approaches to balance transparency needs with privacy in governance of digital identity interactions. Suggests calibrated assurance levels to align business utility with user protection.

European Banking Federation: Notes that if wallets or third parties perform strong customer authentication for banks, formal outsourcing agreements and clear liability frameworks are needed. Governance should delineate responsibilities to maintain compliance and user protection.

epicenter.works - for digital rights: Warns that deregulation of the EUDI framework could erode essential safeguards for users and wallet integrity. Urges maintaining strict rules to prevent mission creep and protect fundamental rights.

Centre for Cybersecurity Belgium: Recommends making digital identity validation voluntary and consent-based to preserve user autonomy. Governance should avoid coercive mandates while enabling secure verification options.

InfoCert: Stresses the need to clarify EUDI actor roles, funding responsibilities, and sustainable business models, including for QES and attribute attestations. Clear governance is required to give market participants certainty.

Trans Sped: Points to ambiguity over wallet roles and cost allocation that could hinder adoption. Calls for guidance on who pays for attestations and signatures to ensure a viable business model.

European Digital Rights (EDRi): Opposes mandates and eID deregulation that could undermine privacy and user protections. Advocates strong legal safeguards and limits on scope and compulsion.

European Entrepreneurs CEA-PME: Supports voluntary uptake of digital identity and opposes mandated acceptance by private entities. Emphasizes market-driven evolution to protect SMEs and user choice.

European Savings and Retail Banking Group: Argues banks must retain the right to decline EUDIW-based authentication if security or compliance standards are not met. Governance should allow risk-based acceptance to protect customers and financial stability.

Free ICT Europe Foundation: Urges that the Business Wallet prioritize usability and practical value over complexity to drive adoption. Governance should avoid burdensome requirements that stifle SME participation and user experience.

2.6.2 Security & Interoperability Standards

Security & Interoperability Standards for digital identity, trust services, and wallet integrity converge on outcome-based, testable requirements and proven trust infrastructures. Stakeholders call for clear, publicly benchmarked minimum criteria for identity proofing (biometric accuracy, anti-spoofing and liveness, document authenticity, deepfake defenses) and for explicitly permitting secure fully automated, unattended onboarding and qualified certificate issuance. Architectures should favor PKI/PKD and international trust registries over untested blockchain approaches. Interoperability must scale across the Union via a trusted verification layer that preserves exclusive user control while enabling open verification without data modification. The agenda emphasizes sovereign, interoperable EU identity wallets, robust safeguards and strong wallet security standards, coordinated EUDIW technical development, and harmonized eIDAS continuity through EUCC ISAC. Practical concerns include avoiding overstandardization and dependency bloat, addressing unlinkability implications for attestation payments, and ensuring sustainable deployment: nearly 190 standards and certifications create complexity, some Member States have postponed rollouts, and weak business models risk adoption where mature national eID schemes already exist.

lear minimum technical criteria such as biometric accuracy, anti- spoofing, liveness detection, document checks, and deepfake defenses should be defined and publicly benchmarked, with regular reviews. (Evotrust)

The implementation of the European Digital Identity Wallet involves nearly 190 technical standards and certification dependencies. (Namirial Spa)

Automated solutions now match or surpass hybrid methods in security and reliability. (Evotrust)

Several Member States have postponed deployment due to technical and financial infeasibility. (Namirial Spa)

Evotrust: Argues EU regulations should explicitly allow fully automated, unattended identity proofing for qualified certificates and EUDI Wallet onboarding, as automation now matches or surpasses hybrid methods in security and reliability. Calls for clear, publicly benchmarked minimum technical criteria (biometric accuracy, anti-spoofing, liveness, document checks, deepfake defenses) with regular reviews.

While its rejection is positive, EU regulations should explicitly permit fully unattended identity proofing for qualified certificates and EUDI Wallet onboarding to ensure legal clarity.

Namirial Spa: Warns that EUDI Wallet implementation is overstandardized—entailing nearly 190 standards and certifications—leading to delays and infeasibility in several Member States. Highlights the absence of a sustainable business model for providers, especially where mature national eID schemes already exist.

The implementation of the European Digital Identity Wallet involves nearly 190 technical standards and certification dependencies.

Entrust SAS: Recommends grounding the EUDI Wallet's trust architecture in proven infrastructures like PKI/PKD and international trust registries rather than untested blockchain. Emphasizes reliability and established governance for security and interoperability.

Its architecture must be grounded in proven infrastructures such as PKI/PKD, supported by international trust registries rather than untested blockchain approaches.

DigitalTrade4.EU: Proposes a Union-wide trusted verification layer that enables open verification of credentials without modifying them. Stresses exclusive issuer control while maintaining broad interoperability across the EU.

: Advocates robust security safeguards in digital identity systems to protect users and ensure trust services integrity and interoperability.

secunet Security Networks AG: Calls for sovereign, interoperable EU identity wallets built on stringent security standards and public oversight.

Cigref: Urges prioritization of trust and the deployment of EU digital identity wallet technologies with clear, harmonized security and interoperability standards across sectors.

Charter of Trust: Supports strong security standards for digital identity wallets to guarantee resilience, integrity, and user trust.

InfoCert: Notes that strict unlinkability requirements can complicate payment-related attestations, urging balanced standards that preserve privacy while enabling essential functionality.

European Savings and Retail Banking Group: Calls for coordinated technical development and governance of the EUDI Wallet to secure interoperability among financial institutions, service providers, and Member States.

: Promotes harmonized continuity between eIDAS schemes and coordinated security via EUCC ISAC to strengthen trust and incident response across the EU.

2.6.3 Legal, Regulatory & QTSP Compliance

This category consolidates calls for legal certainty, proportionality, and cross-regulatory alignment for QTSPs and wallet providers under eIDAS 2.0 and the EUDIW. Stakeholders flag ambiguous legal terms and misaligned applicability dates that impede compliance planning, alongside practical needs for operational guidance (e.g., the quality and refresh cadence of authentic sources to keep attributes current). QTSPs describe a disproportionately heavy compliance load due to overlapping EU rules and redundant audits, with each qualified service demanding separate assessments, reporting, and supervision. Regulatory simplification is welcomed only if carefully calibrated: replace duplicative, technology-specific obligations with harmonized, technology-neutral ones, without weakening security, liability clarity, or cross-border recognition. Additional operational risk stems from Article 30's five-year QSCD certification cycle and biennial vulnerability testing, which can force disruptive customer migrations if manufacturers cease certification. In finance, banks seek clear scope and liability rules for EUDIW acceptance: mandatory use limited to identification, optional for authentication/authorization, and alignment with PSD2/PSR/AMLR to avoid SCA/SUA conflicts and unallocated liability for unauthorized transactions. To future-proof trust services, stakeholders also propose explicitly anchoring long-term validation and preservation (LTV/LTA) of qualified signatures and seals across root expiries and algorithm transitions via future implementing acts.

The current and future eIDAS framework imposes avoidable administrative and financial burdens, mainly due to overlapping compliance with other EU rules, redundant audits, and technical standards. (Evotrust)

Each service (QES, QeRDS, QEAA, eArchiving) requires individual conformity assessments, incident reports, and continuous supervision. (Namirial Spa)

If a manufacturer stops certifying a device, QTSPs must migrate customers to new devices, causing service disruptions and higher costs for citizens. (Evotrust)

The EUDIW acceptance in accordance with Art. 5f(2) eIDAS 2.0 poses an incalculable risk for PSPs in cases of unauthorised transactions or malfunctions within the sphere of the EUDIW provider. (European Associations of Co-operative Banks (EACB))

Docusign: Supports regulatory simplification under eIDAS but warns the one in, one out principle must not remove safeguards essential to trust, security, liability, and interoperability. Recommends replacing duplicative rules with harmonised, technology-neutral obligations.

The principle should not lead to a "mechanical" repeal of provisions that are essential for security, liability clarity, or cross-border recognition.

Intesi Group: Points to ambiguous legal terms and conflicting implementation dates that impede QTSP compliance and audit readiness. Calls for operational clarity on authentic sources data quality and update frequencies for attribute management.

Confusing or conflicting applicability dates further complicate compliance; for example, Article 51 requires remote qualified electronic signature management by 21 May 2026, but relevant rules only take effect from 19 August 2027.

Evotrust: Argues QTSPs face avoidable, overlapping compliance burdens across eIDAS and horizontal cybersecurity laws, alongside risky QSCD recertification cycles. Proposes explicitly anchoring long-term validation and preservation of qualified signatures and seals.

The current and future eIDAS framework imposes avoidable administrative and financial burdens, mainly due to overlapping compliance with other EU rules, redundant audits, and technical standards.

Namirial Spa: Warns QTSP compliance has become disproportionately costly, with separate conformity assessments, incident reporting and supervision for each service. Notes NIS 2 obligations further multiply administrative and financial burdens.

Operating as a QTSP under eIDAS has become disproportionately expensive.

European Associations of Co-operative Banks (EACB): Requests legal certainty on the EUDIW scope, its interaction with PSR/AMLR, and where acceptance is mandatory versus optional. Highlights liability and unauthorized-transaction risks for PSPs if EUDIW acceptance is imposed.

The EUDIW acceptance in accordance with Art. 5f(2) eIDAS 2.0 poses an incalculable risk for PSPs in cases of unauthorised transactions or malfunctions within the sphere of the EUDIW provider.

DigitalTrade4.EU: Advocates stronger QTSP compliance and security requirements and broader mandating of qualified signatures and seals to raise trust and legal certainty.

European Banking Federation: Seeks clarity and alignment between the EUBW and EUDIW, including SCA liability and wallet responsibilities. Calls for guidance on the PSD2/eIDAS2 interplay, the definition of online identification, and payments via EUDIW.

Association of Netherlands Municipalities: Asks for clear definitions of the wallet scope, obligations and responsibilities to ensure compliant public-sector deployment.

D-Trust: Urges treating eIDAS as lex specialis to prevent overlapping regimes and compliance conflicts. Warns Article 30 five-year QSCD limit risks service disruption.

Charter of Trust: Requests clarity on permissible inspection of wallet contents and measures to strengthen the digital identity trust framework.

InfoCert: Supports permitting fully automated identity proofing with safeguards and embedding eIDAS requirements consistently across EU legislation.

Trans Sped: Promotes integrating the European Business Wallet through eIDAS and anchoring eIDAS obligations across related laws for coherence and compliance.

European Entrepreneurs CEA-PME: Proposes making the EUDI compulsory for high-security operations to ensure strong assurance and consistent acceptance.

European Savings and Retail Banking Group: Calls for clarity on EUDIW acceptance in the PSR and clear allocation of liability to EUDIW providers for malfunctions or unauthorized transactions.

Eurosmart: Highlights security and assurance risks in remote QSCD models and concerns about Article 30 certification.

Österreichische Notariatskammer: Urges integrating notaries as trusted legal actors within digital identity and trust service processes to preserve legal certainty.

: Argues remote QSCD certifications are less thorough and that Article 30 amendments could disadvantage local QSCD ecosystems and assurance levels.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Suggests conditional certification models where specific legal privileges are granted based on compliance levels to balance innovation and assurance.

2.6.4 Miscellaneous

Within the Miscellaneous category of Digital Identity, Trust Services and Wallet Integrity, the insights critique EU-style regulatory complexity and urge African digital identity initiatives to prioritize capability over compliance. They advocate privacy-by-design architectures with clear trust anchors and cross-border interoperability that avoids replicating burdensome European models, balancing trust, usability, and scalability across Member States. Strategically, the emphasis shifts from ticking regulatory boxes to building resilient capabilities—identity wallets, trust frameworks, and interoperability rails—grounded in minimalism, security-by-default, and practical implementation maturity.

Interoperability and trust anchoring: Africa's digital identity systems should adopt privacy-by-design while ensuring that interoperability across Member States does not replicate Europe's complexity. ()

Africa's Al future depends less on compliance and more on capability. ()

: The document critiques EU-style regulatory complexity and urges Africa to prioritize capability over compliance. It recommends privacy-by-design, interoperable digital identity systems with strong trust anchoring across member states.

Interoperability and trust anchoring: Africa's digital identity systems should adopt privacy-by-design while ensuring that interoperability across Member States does not replicate Europe's complexity.

2.7 Cybersecurity Resilience and Incident Reporting

The strongest takeaway is the push to harmonize and simplify EU incident reporting across NIS2, DORA, GDPR, PSD2, and the CRA so responders can focus on containment and recovery while authorities gain meaningful, non-duplicative situational awareness. Stakeholders advocate risk-based thresholds, realistic timelines (limiting 24-hour alerts to truly critical events), fewer data fields, API-enabled single or group-level submissions, and impact-focused criteria. Consistent EU governance is essential: an empowered ENISA, early operational guidance, common platforms, and coordinated oversight that avoids rushed revisions and clarifies scope, registration, and critical infrastructure lists. Secure disclosure must preserve confidentiality, safe-harbour protections, data minimisation, and careful handling of vulnerabilities, while keeping consumer notices clear and timely. Sector fit and SME support are vital, including flexible CRA application and targeted solutions for energy, maritime, internet infrastructure, and gaming. Supply chains need upstream assurance, pragmatic exemptions (e.g., rail), stronger procurement, and diversified technology dependencies. Operational preparedness—exercises, role-based training, CSIRT/ISAC sharing, redundancy, and controlled containment—anchors resilience. Reusing standards and efficient certification (ISO/IEC, ETSI, ECCF) reduces burden without lowering protection. Across inputs, cybersecurity is treated as a strategic necessity, calling for coordinated,

proportionate rules and sustained public-private collaboration. Common trends are alignment, proportionality, secure channels, and readiness rooted in standards and shared responsibility.

2.7.1 EU Governance, ENISA & Policy Workability

This category converges on strengthening EU-level cybersecurity governance and an empowered, well-resourced ENISA to deliver consistent implementation across regimes (e.g., NIS2, DORA, the Cybersecurity Act) while improving policy workability. Stakeholders call for coherent, streamlined compliance that reduces duplication and inconsistencies without weakening protections, with EU guidance to align standards, accountability, and trust across sectors and borders. Workability themes include early, practical clarity on incident-reporting operationalization (technical and procedural specifications), proportionate obligations that lower administrative burden yet preserve resilience, and attention to data holders' security in model contractual terms. Contributors warn against rushed revisions and ad-hoc requests that drain scarce cyber resources, urge remedies for fragmented frameworks, and highlight needs such as EU-level critical infrastructure lists, scope and registration clarity, targeted exemptions, ENISA-led platforms and guidance, and concentration risk analyses. The governance perimeter is also expanding: ENISA's collaboration with the AI Act's committee underscores cross-domain supervision, and some inputs stress global cooperation and technology enablement (including joint R&D testbeds) alongside Europe's internal simplification goals to sustain competitiveness and confidence.

> *FERMA insists on the need to strengthen cybersecurity governance at EU level, notably through streamlined compliance structures.* (FERMA - Federation of European Risk Managers Associations)
>
> *Strengthen and resource the EU Cybersecurity Agency to ensure consistent implementation.* (Mastercard Europe SA)
>
> *It is worth noting that the AI Act explicitly provides for ENISA to collaborate with the European Artificial Intelligence Committee to address emerging cybersecurity issues in the internal market.* (FERMA - Federation of European Risk Managers Associations)
>
> *While the EU focuses on streamlining compliance, Africa's primary need remains technology enablement - access to secure infrastructure, encryption tools, and forensic capacit* ()
>
> **FERMA - Federation of European Risk Managers Associations:** Calls to strengthen EU-level cybersecurity governance and streamline compliance, highlighting coordination with AI oversight to address emerging risks.
>
> *FERMA insists on the need to strengthen cybersecurity governance at EU level, notably through streamlined compliance structures.*
>
> **Kaspersky Labs Limited:** Supports simplification that preserves robust cybersecurity and data protection, urging policies to maintain objectives while reducing burdens.
>
> *Simplification must not come at the cost of resilience or accountability.*
>
> **Government Office of the Czech Republic:** Urges EU model contractual terms and guidance to account for data holders' security and cybersecurity concerns within governance frameworks.
>
> *CZ also encourages the Commission to take into consideration the security and cybersecurity concerns of the data holders when drafting the model contractual terms and guidelines for data access and use.*
>
> **Airbus:** Supports a strong EU regulatory role to reinforce security, trust, and accountability across the market.
>
> *We welcome the EU's role in cybersecurity, as regulations help reinforcing security, fostering trust, and establishing accountability.*
>
> **Verisure:** Flags uncertainty around how incident and resilience reporting will be implemented and calls for early, detailed guidance from ENISA for operational clarity across Member States.
>
> *As these requirements will directly affect Verisure at both group and national level-across our operations in twelve EU Member States-it is essential to have early clarity on the technical and procedural aspects to be defined by ENISA.*

Mastercard Europe SA: Advocates resourcing ENISA to ensure consistent EU-wide implementation and applying the highest security standards for sensitive credentials.

Strengthen and resource the EU Cybersecurity Agency to ensure consistent implementation.

: Argues EU simplification debates should be coupled with technology enablement and joint R&D testbeds to make policies workable beyond Europe.

Simplification dialogues should therefore include joint investment in cyber R&D testbeds under ASRIC coordination.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: Backs a holistic EU approach to bolster cyber-resilience, integrating governance coherence with practical implementation.

In light of the ever-increas- ing cyber-risk environment, German industry supports this holistic approach to enhancing Europe's cyber-resilience.

: Supports simplification that retains strong protection standards so citizens maintain trust in digital services.

At the same time, I believe simplification should not mean lowering standards.

American Chamber of Commerce to the EU: Recommends empowering ENISA to scrutinize and stress-test EU cybersecurity policy for coherence and practicality.

Business & Science Poland: Supports clarifying ENISA's mandate and strengthening security assessments to enhance governance consistency.

FME: Requests clarification of NIS2 registration scope to improve policy workability and reduce administrative ambiguity.

IDRS Platform: Argues that improved EU governance frameworks directly enhance resilience and systemic strength.

Federation of Austrian Industries: Proposes exemptions for affiliates under NIS2 Article 22(5) to make reporting and governance obligations more workable.

Confederation of Industry of the Czech Republic: Warns that ad-hoc information requests drain cybersecurity resources, urging more predictable governance processes.

Confederation of Norwegian Enterprise (NHO): Calls for an EU-level critical infrastructure list and better alignment between disparate cybersecurity frameworks that currently operate in isolation.

CPME: Cautions against rushed revisions to cybersecurity rules, emphasizing careful sequencing for workable implementation.

Association des Constructeurs Européens de Motocycles: Seeks clearer guidance on ENISA platform operations to ensure consistent obligations and support for industry.

epicenter.works - for digital rights: Urges smart, risk-based regulation that strengthens security while addressing global systemic risks.

Google: Supports strengthening ENISA and advancing practical security measures to improve EU-wide cyber resilience.

Forvis Mazars: Advocates stronger ENISA oversight and a clearer mandate to ensure consistent supervision and guidance.

NCC Group: Opposes weakening cybersecurity protections and cites rising threats as justification for strong, enforceable regulation.

European Fund and Asset Management Association (EFAMA): Highlights DORA implementation challenges, seeking clearer reporting expectations and proportionate compliance costs.

Connect Europe: Calls to clarify and align overlapping cybersecurity regulations to reduce fragmentation and improve workability.

ESYS Foundation: Proposes that ENISA lead EU-level concentration risk analysis to inform governance and resilience planning.

Clever Cloud: Argues policy changes should not trade off resilience and protection, emphasizing reliable, secure cloud operations.

Deutsche Industrie- und Handelskammer: Supports enhancing cyber resilience while reducing regulatory inconsistencies and burdens on businesses.

Zentralverband Deutsches Baugewerbe: Backs simplifying rules without weakening cybersecurity, emphasizing practical compliance for SMEs.

Dedalus S.p.A.: Calls to strengthen ENISA's mandate and capacity to support healthcare cybersecurity and coordinated incident response.

APPLiA (Home Appliance Europe): Requests adjustments to the Cybersecurity Act to improve policy workability and alignment for manufacturers.

2.7.2 Unified Incident Reporting & Definitions

The insights highlight pervasive fragmentation and duplication in EU cybersecurity incident reporting across NIS2, DORA, GDPR, PSD2, the CRA, and related regimes. Companies often must notify multiple authorities for the same event, repeating largely similar information in different formats and timelines, sometimes even across separate legal entities within the same group. This creates administrative burden and legal uncertainty, diverts scarce resources during crises, and can distort situational awareness—raw incident counts look alarming while saying little about true resilience. Stakeholders converge on the need to unify and clarify reporting and definitions: harmonised templates and thresholds, aligned terminology and materiality criteria, and options for centralised or group-level reporting. Proposals range from a single EU reporting window to standardised national channels, with some emphasising that trusted, direct communication via national CSIRTs should be preserved. Practical enablers include API-based submissions with clear guidance and universally accessible tools, while refining impact criteria (e.g., focusing on actual impact rather than duration) ensures that reporting is meaningful and actionable.

At present, reporting requirements under instruments such as NIS2, DORA, and GDPR breach notification rules remain overly complex, duplicative, and inconsistently applied. (Dun & Bradstreet)

One of the most pressing challenges in the current cybersecurity landscape lies in fragmented reporting obligations. (Bitkom e.V.)

This complexity distorts the picture: a raw count of "incidents" may appear alarming, but it conveys little about resilience. (Telefonica, S.A.)

Members of ISP Alliance acknowledge that reporting incidents via published and further processable APIs is not overly burdensome provided that clear guidelines are in place. (ISP Alliance a.s.)

: Describes how companies must notify multiple authorities about the same cybersecurity incident, each with different formats and deadlines. Notes that the data requested is largely the same, just presented differently.

Currently, and even more so with the CRA, some companies must report the same cybersecurity incident to multiple authorities, using different formats and deadlines.

Dun & Bradstreet: Argues that incident and breach reporting across NIS2, DORA, and GDPR is overly complex, duplicative, and inconsistently applied. Warns this fragmentation creates administrative burden and legal uncertainty for cross-border, cross-sector businesses.

At present, reporting requirements under instruments such as NIS2, DORA, and GDPR breach notification rules remain overly complex, duplicative, and inconsistently applied.

Government Office of the Czech Republic: Advocates keeping incident reporting at the national level, emphasizing Member States' existing platforms tailored to local needs. Stresses that trust and direct communication between national authorities and entities are essential.

For the reasons outlined, we are of the opinion that incident reporting should remain in the hands of Member States.

Telefonica, S.A.: Points to overlapping, fragmented reporting channels introduced by newer frameworks, leading to redundancy across recipients. Warns that raw incident counts can misrepresent resilience while compliance processes drain resources.

The administrative complexity is compounded by newer frameworks, such as the Cyber Resilience Act (CRA) and the European platform for vulnerability notification, which introduce additional reporting channels.

Bitkom e.V.: Identifies fragmented reporting obligations as a key challenge. Notes that groups must register each legal entity separately rather than handle reporting centrally at enterprise level.

One of the most pressing challenges in the current cybersecurity landscape lies in fragmented reporting obligations.

ISP Alliance a.s.: States that incident reporting via well-documented APIs is manageable when clear guidelines exist. Acknowledges the importance of cyber-incident reporting obligations.

Members of ISP Alliance acknowledge that reporting incidents via published and further processable APIs is not overly burdensome provided that clear guidelines are in place.

CERMI: Calls for universally accessible incident reporting platforms and public breach communications. Emphasizes inclusivity and usability for all users.

All platforms for incident reporting, as well as all public communications directed at citizens following a security breach, must be universally accessible.

Union of Entreprenuers and Employers: Details how multiple legal regimes can create four separate notification channels for one event, with divergent formats and timelines. Notes that such fragmentation complicates crisis management and creates uncertainty about notification order.

PSD2 requires payment-related breaches to be reported to national central banks, and GDPR Article 33 obliges controllers to notify data protection authorities of personal data breaches, creating four separate notification channels for a single event.

European Associations of Co-operative Banks (EACB): Calls for refining impact criteria so reporting thresholds better reflect materiality. Supports harmonised, standardised reporting templates to improve efficiency and operational response.

Harmonisation of incident reporting obligations is critical to ensure efficient compliance and effective operational response.

ACEA (European Automobile Manufacturers' Association): Highlights discrepancies across EU instruments that impose incident and data breach reporting. Points out differing procedures, timelines, and authorities across NIS2, CRA, DORA, and GDPR.

The NIS 2 Directivexiii, the Cyber Resilience Act (CRA)xiv, the Digital Operational Resilience Act (DORA)XY and the GDPR lay down different procedures, different timelines, and appoint different reporting authorities for the reporting of relevant incidents and breach.

American Chamber of Commerce to the EU: Advocates prioritising reporting to national CSIRTs to focus coordination and response. Emphasizes leveraging existing national capabilities rather than adding duplicative channels.

Uber B.V.: Notes that reporting obligations can divert scarce resources from active incident response. Urges calibrating requirements to avoid impairing containment and recovery.

FME: Supports streamlining and rationalising incident reporting obligations. Seeks reduced duplication and clearer processes across frameworks.

Bundesministerium für Inneres: Expresses doubt about imposing immediate reporting changes without careful evaluation. Calls for pragmatic timelines that do not hamper response.

Test and Measurement Coalition: Points to lack of clarity on reporting templates and formats. Requests standardised, well-defined templates to reduce ambiguity.

Bayerische Motoren Werke Aktiengesellschaft: Advocates a single EU incident reporting platform to avoid duplication. Seeks unified processes and data fields across regimes.

Japan Business Council in Europe (JBCE): Urges alignment of reporting requirements and incident terminology across frameworks. Aims to facilitate consistent implementation by multinational firms.

Healthtech Finland: Highlights overlapping cybersecurity reporting obligations across sectors and laws. Calls for coordination to reduce unnecessary duplication.

Federation of German Consumer Organisations (vzbv): Supports maintaining robust incident reporting and notification duties to protect consumers. Emphasizes that simplification should not weaken accountability.

Verband der Automobilindustrie e.V.: Calls for clear EU-level definitions and thresholds for incident reporting. Aims to ensure proportionate, consistent triggers across sectors.

Association des Constructeurs Européens de Motocycles: Requests clearer definitions of significant incidents and concrete case examples, plus harmonised content requirements. Raises concerns about added platform reporting and cross-border notification expectations.

epicenter.works - for digital rights: Argues that structured incident reporting strengthens overall security and resilience. Supports obligations that improve situational awareness and response.

AFME: Warns that a central incident hub must be carefully governed to avoid new risks. Advocates harmonisation while preserving operational practicality for firms.

Delivery Platforms Europe: Criticises overcomplicated cybersecurity reporting processes. Calls for simplification to reduce burden during incidents.

European Fund and Asset Management Association (EFAMA): Recommends simplifying existing incident reporting before embarking on broader reforms. Seeks coherent, proportionate requirements across regimes.

D-Trust: Supports a unified incident reporting window to streamline obligations. Envisions a single entry point reducing duplication and inconsistencies.

Prosus Group: Highlights burdens associated with reporting and notification across overlapping frameworks. Seeks clarity and consolidation to limit disruption during incidents.

INVERCO: Urges caution about centralising reporting in an EU hub, noting governance and effectiveness concerns. Recommends balanced approaches that complement national systems.

Zentralverband Deutsches Baugewerbe: Supports retaining mandatory notification requirements to ensure transparency and accountability. Emphasizes consumer protection and timely alerts.

Wolt: Notes that overlapping and duplicative reporting can hinder incident response by diverting resources. Calls for alignment to avoid repeated submissions of similar information.

Council of European Municipalities and Regions (CEMR): Addresses rising incident reporting burdens on municipalities and regions. Encourages manageable processes and support for local authorities.

2.7.3 Risk-Based Obligations & Timelines

Across frameworks, very short notification deadlines (24–72 hours) often arrive before technical facts are known, producing rushed, incomplete, sometimes inaccurate, and duplicative preliminary reports. Fragmented and overlapping regimes (including weekend reporting and complex triage thresholds) increase administrative load and pull responders away from containment and recovery, sometimes prolonging incident management. Many stakeholders propose limiting 24-hour alerts to truly critical incidents and aligning timelines with investigative reality. The consensus favors risk-based, proportionate, and targeted obligations: simplify and harmonize criteria; focus on ICT services supporting critical or important functions and on cyber incidents over minor operational events; reduce data fields; enable group-level submissions to avoid dozens of duplicative filings for one root cause; and remove low-value triggers such as recurring or geographic-spread criteria. Simplification should not weaken security effectiveness; it should cut redundant bureaucracy so organizations can prioritize defense, containment, and recovery while meeting clear, achievable reporting timelines and transition periods.

Regulations impose very short deadlines (24 to 72 hours) for incident notification, often before technical investigations are complete. ()

Reporting should focus on ICT services that support critical or important functions, and the amount of information required should be reduced to avoid unnecessary complexity and facilitate compliance. (European Associations of Co-operative Banks (EACB))

In practice, for example, a group with over 80 entities may be required to submit more than 80 reports for a single incident arising from the same root cause. (European Associations of Co-operative Banks (EACB))

Yet the steady rise in regulatory obligations has created a paradox: measures intended to enhance security often divert resources away from practical risk mitigation. (Bitkom e.V.)

: Very short incident-notification deadlines (24-72 hours) lead to rushed, incomplete reporting and increased administrative workload across overlapping regimes.

Regulations impose very short deadlines (24 to 72 hours) for incident notification, often before technical investigations are complete.

Bitkom e.V.: Escalating regulatory obligations and short reporting deadlines divert resources from practical risk mitigation; policy should empower decisive defence, containment and recovery over excessive compliance.

Most importantly, regulation must empower companies to act decisively in times of crisis - focusing on defence, containment and recovery - rather than tying resources to excessive compliance tasks.

Trellix: Supports simplification that removes redundant bureaucracy without weakening security effectiveness, keeping focus on real cyber defence.

We agree with the Commission that simplification efforts must not compromise security effectiveness; rather, they should eliminate redundant bureaucracy that diverts resources from actual cyber defence.

European Associations of Co-operative Banks (EACB): Recommends simplifying and targeting reporting to ICT supporting critical functions, reducing information demands and avoiding duplicative group-level submissions. Timelines should be adjusted so reporting does not prolong incident response, with priority on cyber incidents over minor operational ones.

Financial institutions prioritise swift incident resolution, and the current reporting obligations may inadvertently prolong incident management processes.

American Chamber of Commerce to the EU: EU incident triaging criteria cause overreporting and unnecessary burden. Calls to remove recurring-incident, geographic-spread, and weekend reporting requirements to make obligations more risk-based.

ENSHPO - The European Network of Safety and Health Professional Organizations: Fragmented reporting timelines across regimes hinder effective safety and incident management. Advocates harmonized, coherent timelines to support resilient response.

Bayerische Motoren Werke Aktiengesellschaft: Suggests restricting 24-hour alert requirements to truly critical incidents to align effort with risk and reduce noise. Endorses more flexible timelines that accommodate investigative completeness.

Japan Business Council in Europe (JBCE): Requests clearer CRA Annex III classifications so obligations and timelines are applied proportionally to risk. Better definitions would prevent misclassification and inappropriate reporting burdens.

Federation of Austrian Industries: Supports a 36-month CRA transition to implement obligations realistically while maintaining resilience. Longer timelines enable thorough compliance without disrupting operations.

Association des Constructeurs Européens de Motocycles: Strict 24/72-hour reporting deadlines impose significant burdens and often yield preliminary, incomplete submissions. Proposes more pragmatic, risk-based timing aligned with incident severity and information availability.

Renault Group: Advocates risk-based NIS 2 enforcement, tailoring obligations and timelines to sectoral risk and organizational profile. Proportionality would prevent undue compliance strain while preserving resilience.

European Entrepreneurs CEA-PME: Calls for proportional cybersecurity and resilience duties for SMEs, aligning reporting scope and timelines with risk exposure and capacity. Opposes one-size-fits-all mandates that overwhelm smaller firms.

Free ICT Europe Foundation: Urges proportionate cybersecurity responsibilities and reporting across ecosystem actors, matched to actual control and capability. Risk-based obligations and timelines should reflect accountability and operational realities.

APPLiA (Home Appliance Europe): Promotes risk-based access controls and governance that streamline compliance while safeguarding security. Obligations and timelines should adapt to product and operational risk.

2.7.4 Standards & Certification Alignment

This category emphasizes aligning cybersecurity risk-management, resilience, and reporting obligations with established European and international standards (e.g., ISO/IEC 27001/27002, ETSI EN 319 401, CEN/TS 18026). Stakeholders argue that leveraging widely adopted frameworks ensures consistency, reduces duplicative compliance, and limits regulatory burden—especially for high-tech sectors already using ISO/IEC 27000-series practices. Involving security providers in standardization is encouraged to keep measures practical and state-of-the-art. On certification, the insights call for an efficient and predictable EU Cybersecurity Certification Framework (ECCF) under the Cybersecurity Act, with recognition of voluntary CSA schemes and caution against blanket ICT product certification. They highlight realistic timelines (e.g., for CRA-related standards), inclusion of non-technical supply-chain risks, and, in some cases, the use of audits to strengthen assurance. The overarching goal is a coherent, market-accepted certification and reporting ecosystem that reuses proven standards, avoids overlap, and enhances resilience.

We welcome the fact that the cybersecurity risk-management measures in the Annex of the latest Implementing Act are aligned with European and international standards, including ISO/IEC 27001, ISO/IEC 27002, ETSI EN 319 401, and technical specifications like CEN/TS 18026:2024, relevant to network and information system security. (European Tech Alliance)

Imposing additional cybersecurity requirements without aligning with these frameworks would result in duplicated efforts and regulatory burden. (European Tech Alliance)

However,many industries, particularly those in high-tech sectors, already adhere to established security frameworks, such as the ISO/IEC 27000 standards. (European Tech Alliance)

We welcome the initiative to revise the Cybersecurity Act, particularly with regard to increasing the efficiency of the European Cybersecurity Certification Framework (ECCF), expanding its scope, and

considering non- technical risk factors in ICT supply chains. (WKÖ - Austrian Federal Economic Chamber)

European Tech Alliance: Advocates aligning cybersecurity requirements with existing European and international standards to avoid duplication and regulatory burden. Supports referencing ISO/IEC 27001/27002, ETSI EN 319 401 and CEN/TS 18026 across industries.

We welcome the fact that the cybersecurity risk-management measures in the Annex of the latest Implementing Act are aligned with European and international standards, including ISO/IEC 27001, ISO/IEC 27002, ETSI EN 319 401, and technical specifications like CEN/TS 18026:2024, relevant to network and information system security.

WKÖ - Austrian Federal Economic Chamber: Welcomes revising the Cybersecurity Act to improve efficiency of the European Cybersecurity Certification Framework and broaden its scope. Calls for integrating non-technical supply-chain risk factors into certification.

We welcome the initiative to revise the Cybersecurity Act, particularly with regard to increasing the efficiency of the European Cybersecurity Certification Framework (ECCF), expanding its scope, and considering non- technical risk factors in ICT supply chains.

: Promotes mandatory data and cybersecurity audits as a way to enforce consistent, standards-based practices. Suggests audits could anchor alignment and accountability.

BusinessEurope: Warns that timelines for developing standards under the Cyber Resilience Act are too tight. Cautions this may hinder effective alignment and practicable certification.

Federation of Austrian Industries: Urges recognition of voluntary CSA certifications to incentivize adoption without imposing rigid mandates. Favors alignment with established standards through market-driven schemes.

Orgalim - Europe's Technology Industries: Supports keeping CSA certification voluntary to reduce burdens on industry. Emphasizes aligning with existing standards rather than imposing mandatory certification.

E.ON SE: Opposes mandatory certification for ICT products. Argues for risk-based alignment with standards instead of blanket certification programs.

Charter of Trust: Calls for involving security providers in standards-setting to ensure practical, effective alignment. Highlights the need for stakeholder participation to improve certification relevance.

Association Française des Entreprises Privées: Supports an ambitious EU cybersecurity certification scheme that is efficient and internationally aligned. Seeks a framework that strengthens resilience while remaining workable for businesses.

2.7.5 Supply Chain Security & CRA Alignment

Supply Chain Security & CRA Alignment centers on making cybersecurity assurance a shared, upstream-first responsibility across complex industrial supply chains. Under the CRA, component suppliers must demonstrate conformity before OEMs and integrators can assess final products, which drives end-to-end assurance but also yields time-consuming, costly readiness efforts across both upstream and downstream tiers. Stakeholders broadly support streamlining obligations to reduce friction, so long as protection standards are preserved, reflecting the increased risk landscape. Sector-specific flexibility is sought to preserve delivery continuity and interoperability, particularly in rail, through risk-based alternatives and targeted exemptions for project extensions—explicitly anchored in CRA Recital 55 and Article 13(4). Beyond core conformity, alignment challenges include timing burdens, lifecycle and terminology coordination, data-access uncertainties, and multi-year support obligations. Strengthening procurement with trusted suppliers, clarifying OEM accountability, and broadening contractual security clauses are seen as practical levers. Extending and harmonizing incident reporting to services and across supply chains enables timely information sharing that boosts resilience. Strategically, the EU is urged to reduce unilateral dependencies on foreign technologies and invest in diverse, robust infrastructures resilient to cyber, disinformation, and geopolitical shocks. Achieving this demands proactive investment, coordinated defense, and a trade policy that fosters supply chain diversity and cross-

border preparedness—complementary to CRA's objectives of consistent, innovation-friendly security across the product and service ecosystem.

> *Thus, to ensure end to end security, it would be valuable that the suppliers ensure these components conform with the CRA first, and after this is ensured the conformity of the final product is assessed.* (SIEMENS AG)
>
> *Securing the entire supply chain, both upstream and downstream, requires significant time and effort:* (SIEMENS AG)
>
> *ANIE ASSIFER considers it essential to preserve delivery continuity for existing projects by allowing manufacturers to adopt alternative measures that ensure an adequate level of cybersecurity protection, to justify the non-application of CRA cybersecurity requirements.* (ANIE Federazione - ANIE ASSIFER)
>
> *This approach is consistent with Recital 55 of the CRA and Article 13(4).* (ANIE Federazione - ANIE ASSIFER)

: Argues Europe must reduce unilateral dependency on foreign technologies and diversify supply chains, investing in robust, secure infrastructure resilient to cyber and geopolitical shocks. Calls for proactive investment and cross-border preparedness to strengthen supply chain security.

his requires proactive investment, coordi- nated defence strategies, a trade policy that focuses on supply chain diversity and cross-border preparedness.

SIEMENS AG: Advocates an upstream-first CRA conformity sequence where suppliers certify components before OEMs, noting that complex B2B supply chains will face significant time and cost to become CRA-ready. Emphasizes end-to-end security across upstream and downstream actors.

Thus, to ensure end to end security, it would be valuable that the suppliers ensure these components conform with the CRA first, and after this is ensured the conformity of the final product is assessed.

ANIE Federazione - ANIE ASSIFER: Supports CRA goals but urges risk-based flexibility for existing and extended rail projects to maintain delivery continuity. Proposes alternative cybersecurity measures and targeted exemptions where interoperability constraints prevent full CRA compliance.

ANIE ASSIFER considers it essential to preserve delivery continuity for existing projects by allowing manufacturers to adopt alternative measures that ensure an adequate level of cybersecurity protection, to justify the non-application of CRA cybersecurity requirements.

Verisure: Supports streamlining CRA obligations while insisting simplification must not lower protection standards. Seeks consistent, innovation-friendly rules that preserve high cybersecurity across the supply chain.

The company supports streamlining obligations from the Cyber Resilience Act (CRA) and related frameworks, emphasizing that simplification should not lower protection standards but instead foster a consistent, innovation-friendly cybersecurity environment.

WKÖ - Austrian Federal Economic Chamber: Notes that supply chain-related cyber risk has increased, underscoring the need for stronger resilience measures and CRA-aligned controls. Highlights escalating exposure across interconnected suppliers.

The risk has increased.

Swedtrain - the Swedish Railway Industry Association: States support for CRA cybersecurity objectives in the rail ecosystem, implying coordinated supplier alignment. Emphasizes sector-wide collaboration to raise supply chain security baselines.

VDMA - Advancing Europe´s machinery industry: Warns that CRA timelines and sequencing place heavy compliance burdens on machinery supply chains. Calls for pragmatic scheduling to allow suppliers and OEMs to align without disruption.

Mafex – Spanish Railway Association: Stresses aligning CRA lifecycle expectations with sector standards and TSI terminology to avoid gaps in supply chain compliance. Seeks consistent definitions that suppliers can implement across product lifecycles.

Confederation of Norwegian Enterprise (NHO): Flags uncertainty around data access and sharing as a barrier to meeting CRA obligations across the supply chain. Requests clarity to enable timely vulnerability handling and incident reporting.

ENTSO-E: Recommends extending CRA reporting to covered services and ensuring timely supplier incident information to operators. Urges harmonized, cross-framework reporting for supply chain incidents to reduce duplication.

Centre for Cybersecurity Belgium: Promotes procurement practices that prioritize trusted, secure suppliers to strengthen supply chain resilience under CRA objectives. Encourages embedding security criteria into purchasing decisions.

secunet Security Networks AG: Calls for stronger supply chain security measures, including rigorous supplier assurance aligned with CRA requirements. Emphasizes comprehensive coverage of third-party components and dependencies.

CLEPA: Criticizes the CRA's five-year support obligation as a heavy burden that cascades through automotive supply chains. Warns it may strain SME suppliers and complicate lifecycle alignment.

E.ON SE: Asserts OEM accountability for product security and updates, clarifying roles across the supply chain. Seeks clear delineation of responsibilities to ensure CRA-aligned end-to-end security.

WindEurope: Urges broadening cybersecurity clauses to cover suppliers and contractors across the wind energy value chain. Aims to ensure consistent supply chain security obligations aligned with CRA expectations.

2.7.6 Operational Preparedness & Technical Resilience

Operational Preparedness & Technical Resilience centers on proving readiness before crises and sustaining core services during them. Stakeholders call for mandated, documented incident response exercises subject to supervisory review; clear, role-based training expectations; and robust baseline protocols to curb access-rights misuse. Two-way CSIRT information sharing and ISAC-enabled risk governance strengthen situational awareness and reporting, while oversight mechanisms ensure controls are enforced across decentralized assets and critical infrastructure, preserving existing safeguards and aligning with frameworks like DORA. Technical resilience priorities include high availability, redundancy, and the controlled containment of incidents—up to temporarily suspending services to protect data integrity—backed by secure national communications, threat intelligence integrated into risk models, and advanced methodologies to detect data leaks. With rising fraud and cybersecurity risks and evidence of slow responses and missed warnings, the insights emphasize continuous preparedness, timely escalation, and capacity building across public and private sectors to protect operations and trust.

In order to promote good risk management practices, FERMA recommends introducing the requirement to carry out annual cyber incident response exercises, with their execution and outcomes properly documented and made available for review by the relevant supervisory authorities. (FERMA - Federation of European Risk Managers Associations)

This measure would ensure not only the existence of formal response plans but also their actual operability, fostering an organisational culture of continuous preparedness for cyber incidents. (FERMA - Federation of European Risk Managers Associations)

FERMA - Federation of European Risk Managers Associations: Recommends mandating annual cyber incident response exercises with documented execution and outcomes for supervisory review to ensure plans are operable and preparedness is continuous.

In order to promote good risk management practices, FERMA recommends introducing the requirement to carry out annual cyber incident response exercises, with their execution and outcomes properly documented and made available for review by the relevant supervisory authorities.

German Property Federation: Emphasizes tighter control and monitoring of access rights to prevent misuse as a core element of technical resilience and operational readiness.

DigitalTrade4.EU: Advocates designing systems for high availability with redundancy and oversight to ensure operational continuity during disruptions.

Bundesministerium für Inneres: Stresses that a planned cybersecurity measure is critical to resilience and should be prioritized and implemented without delay.

Elia Group: Calls for mandating and enforcing strong cybersecurity for decentralized assets to strengthen operational resilience across the system.

Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs (VÖWG): Urges robust protection of critical infrastructure and sensitive data as foundational to operational preparedness and service continuity.

U.S. Chamber of Commerce: Warns that the lack of robust security protocols undermines operational readiness and calls for stronger, standardized controls.

ENTSO-E: Supports mandatory two-way information sharing with CSIRTs to improve situational awareness, preparedness, and coordinated incident response.

Verband der Automobilindustrie e.V.: Flags unclear training requirements under NIS 2, seeking clarity so organizations can implement effective preparedness and resilience programs.

Association des Constructeurs Européens de Motocycles: Advocates strict platform security protocols and notes that DORA enforces resilience requirements that should guide operational robustness.

Comitato Elettrotecnico Italiano - CEI: Recommends integrating threat intelligence into risk models to anticipate threats and enhance proactive technical resilience.

epicenter.works - for digital rights: Highlights that cyberfraud disrupts operations and erodes trust, necessitating stronger safeguards and incident reporting practices.

Forvis Mazars: Observes that resilience is central in the revised act and urges embedding practical operational resilience measures across organizations.

The Center for Countering Digital Hate: Calls for enhanced safety resources and reporting protocols, noting slow responses and missed warnings that weaken preparedness and resilience.

ESYS Foundation: Proposes mandating a secure national communications platform to maintain reliable coordination and resilience during crises.

PensionsEurope: Advocates preserving and reinforcing existing digital resilience safeguards to protect operations and beneficiaries.

European Savings and Retail Banking Group: Notes heightened fraud and cybersecurity risks and urges enhanced preparedness, controls, and monitoring to maintain service continuity.

Eurosmart: Promotes ISACs as effective forums for risk governance and information exchange to strengthen collective preparedness and resilience.

DIGITALEUROPE: Endorses the ability to suspend services to protect data integrity during incidents, prioritizing containment and resilience.

Council of European Municipalities and Regions (CEMR): Affirms that cybersecurity is essential for local and regional resilience and calls for capacity building and preparedness investments.

INRIA and Utrecht University: Presents technical methodologies to detect data leaks, improving detection capabilities and overall technical resilience.

2.7.7 Secure Disclosure, Privacy & Liability

This category focuses on enabling secure disclosure while safeguarding confidentiality, privacy, and commercially sensitive information. Stakeholders call for harmonised, cybersecurity-by-design reporting across GDPR, NIS2, CRA, DORA and the AI Act, backed by high-security single-entry points, robust confidentiality for authorities (including protection of trade secrets and IP), strong integrity/confidentiality controls, and secure channels for PIMS and critical infrastructure. Proposals include stricter safeguards for source-code access, careful handling of zero-days and exploit information, and avoiding obligations to report unpatched exploits that could raise risk. Trust and accountability hinge on clear liability protections to remove disincentives to report: notifications should not increase exposure to claims or spill-over effects, and missing safe-harbour clauses are seen as barriers to sharing. Several warn that data sharing—especially aggregation or transfers to third countries—can heighten cybersecurity and privacy risks; they prioritise data minimisation and security over wider sharing. At the same time, consumer transparency must be preserved through timely, clear and actionable breach notices, while service providers and repositories should share essential vulnerability information responsibly under strict confidentiality.

> *n parallel, technical standards should be enhanced in order to protect sensitive information in notifications under NIS2, CRA, GDPR, and DORA and to ensure common high-level security standards for government entities designated as reporting entry points - such as those defined in the National Security Scheme (ENS) in Spain.* (FERMA - Federation of European Risk Managers Associations)

> *simplification must not weaken reporting: it should address fragmented reporting obligations across GDPR, NIS2, CRA while enhancing transparency for consumers.* (BEUC - The European Consumer Organisation)

> *While Art 23(1) of NIS2 states that notification shall not subject the notifying entity to increased liability, the law should also clarify that they should not be liable for potential spill-over effects caused by the act of notification.* (Ibec)

> *PIU stresses that regulatory initiatives should enhance data security rather than promote mechanisms facilitating the exchange of such data, including with third countries.* (Polish Chamber of Insurance (PIU))

FERMA - Federation of European Risk Managers Associations: Calls for stronger technical standards and confidentiality safeguards for incident notifications across NIS2, CRA, GDPR and DORA, including secure government entry points. Emphasizes protecting trade secrets while maintaining explainability.

> *n parallel, technical standards should be enhanced in order to protect sensitive information in notifications under NIS2, CRA, GDPR, and DORA and to ensure common high-level security standards for government entities designated as reporting entry points - such as those defined in the National Security Scheme (ENS) in Spain.*

Enel SpA: Advocates strengthening protections for non-personal yet sensitive data and applying cybersecurity-by-design so AI and data systems bolster critical infrastructure resilience.

> *Strengthen protections for non-personal data, particularly in contexts where such data may be commercially sensitive or strategically important.*

BEUC - The European Consumer Organisation: Warns that simplifying cyber reporting must not weaken obligations; proposes a single entry point paired with stronger, timely consumer notifications.

> *simplification must not weaken reporting: it should address fragmented reporting obligations across GDPR, NIS2, CRA while enhancing transparency for consumers.*

Ibec: Highlights gaps in liability protections that deter information sharing, calling for explicit clauses shielding notifiers from spill-over liabilities.

> *NIS2 and CRA are missing liability clauses necessary to allow the information to be shared in a more controlled manner.*

Polish Chamber of Insurance (PIU): Argues regulatory efforts should prioritize data security over expanding data-sharing mechanisms, especially cross-border exchanges.

PIU stresses that regulatory initiatives should enhance data security rather than promote mechanisms facilitating the exchange of such data, including with third countries.

American Chamber of Commerce to the EU: Sees clear value in a coordinated vulnerability repository to support secure disclosure and resilience.

SEC4AI4SEC: Stresses ensuring data integrity and confidentiality within AI security contexts and incident reporting.

DigitalTrade4.EU: Calls for robust compliance processes and secure channels for cyber incident reporting and data exchange.

European Public Service Union: Warns that expanded cybersecurity reporting could threaten worker and consumer privacy, requiring strict safeguards.

Confederation of Industry of the Czech Republic: Urges adding liability protections for notifications and cautions that broader data sharing can heighten cybersecurity risks.

Ministry of Industry and Trade of the Czech Republic - this entry represents the official position of the Czech Republic for the section "Targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules: Advocates stricter safeguards for access to source code in oversight and reporting to prevent privacy and security risks.

Mafex – Spanish Railway Association: Notes that vulnerability disclosure can expose critical infrastructure and must be managed through secure, controlled processes.

Polish Confederation Lewiatan: Requests explicit liability clauses to enable incident reporting without undue legal exposure.

: Supports preserving direct breach notifications to consumers to ensure timely, actionable information and trust.

Association des Constructeurs Européens de Motocycles: Emphasizes obligations to notify recipients and customers promptly and clearly in case of cyber incidents.

SGI Europe: Urges maintaining security-related exemptions and provisions and warns that data aggregation can increase security risks, necessitating strict controls.

Broadcom: Supports a single confidential reporting entry point with strong safeguards and addresses challenges when service providers restrict sharing cybersecurity information.

E.ON SE: Calls for explicit policies on zero-day vulnerability reporting and handling to ensure secure disclosure.

Charter of Trust: Advocates balancing transparency with protection of trade secrets and cybersecurity-sensitive information in reporting.

Danish Entrepreneurs: Recommends securing data access for oversight with strong controls to prevent privacy breaches and misuse.

DIGITALEUROPE: Argues against mandatory reporting of unpatched exploits to avoid increasing risk and liability, favoring secure, coordinated disclosure.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Calls for robust security and confidentiality in communications of Personal Information Management Systems, including incident reporting.

INRIA and Utrecht University: Emphasizes maintaining confidentiality and integrity protections throughout cyber reporting and disclosure processes.

2.7.8 Sector Tailoring & SME Support

This category captures calls to tailor cybersecurity resilience regimes to sector-specific contexts and to scale practical support for SMEs. Stakeholders urge ENISA and the European Cybersecurity Competence Centre to co-develop clear, actionable guidance that boosts SME compliance capacity, while noting that even small providers of essential infrastructure can fall under stringent NIS2 obligations. Industrial players support the objectives of the Cyber Resilience Act but seek flexible application that recognizes sector realities (e.g., long project lifecycles, legacy systems) to prevent excessive costs and delivery delays. Energy and other networked sectors highlight concrete gaps where targeted solutions are needed: the CRA's current scope overlooks batteries and solar inverters, leaving risk management of distributed, flexible assets under-addressed despite their role in demand response and grid resilience. There is a lack of tailored cybersecurity solutions for distributed solar installations, and sectors would welcome targeted support. Additional inputs point to the need for clearer sectoral guidance, green-digital-aligned maritime rules, proportionate oversight for internet infrastructure operators, and security requirements calibrated to combat serious crime in gaming—aiming for fit-for-purpose obligations and reporting that improve resilience without undue burden.

> *Concretely, ENISA and the European Cybersecurity Competence Centre should cooperate with the private sector and provide clear guidance on best cyber risk management practices, particularly aimed at SMEs to enhance compliance capacity.* (FERMA - Federation of European Risk Managers Associations)
>
> *There is a lack of tailored cybersecurity solutions for distributed solar installations, which are increasingly critical to the energy transition.* (Enel SpA)
>
> *The current Cyber Resilience Act does not consider batteries or solar inverters in its framework, providing a gap on how to assess and manage cybersecurity risks for flexible and distributed energy assets, which are central to demand response and grid resilience.* (Enel SpA)
>
> *Under the NIS2 Directive, even small companies may face critical obligations if they provide essential infrastructure.* (Centre for Information Policy Leadership (CIPL))

FERMA - Federation of European Risk Managers Associations: Calls for ENISA and the EU Cybersecurity Competence Centre to cooperate with industry and deliver clear, SME-focused cyber risk management guidance to strengthen compliance capacity.

> *Concretely, ENISA and the European Cybersecurity Competence Centre should cooperate with the private sector and provide clear guidance on best cyber risk management practices, particularly aimed at SMEs to enhance compliance capacity.*

Enel SpA: Highlights gaps in the CRA for batteries and solar inverters and the need for tailored cybersecurity solutions for distributed solar and flexible energy assets, inviting targeted sector support.

> *There is a lack of tailored cybersecurity solutions for distributed solar installations, which are increasingly critical to the energy transition.*

Centre for Information Policy Leadership (CIPL): Notes that under NIS2 even small firms operating essential infrastructure face significant obligations, underscoring the need for SME-aware guidance and support.

> *Under the NIS2 Directive, even small companies may face critical obligations if they provide essential infrastructure.*

ALSTOM: Supports CRA objectives while urging railway-specific flexibility to accommodate project extensions, legacy programs, and lifecycle support to manage costs and avoid delivery delays.

> *Recognizing railway-specific constraintssuch as project extensions, legacy programs, and lifecycle supportis crucial to managing the significant cost burden of CRA implementation and avoiding contractual delivery delays.*

American Chamber of Commerce to the EU: Observes that the CRA lacks clear sectoral guidance, signaling the need for tailored direction to help businesses implement requirements effectively.

DigitalTrade4.EU: Advocates sector-specific maritime cybersecurity regulation aligned with the green digital transition, emphasizing tailored approaches for maritime stakeholders.

CENTR - Council of European Top Level Domain Registries: Argues for sector-specific exemption of TLD registries from DORA oversight, reflecting a need for tailored regulatory treatment.

European Casino Association (ECA): Highlights sector-specific cybersecurity concerns in the casino industry related to serious crime, advocating tailored measures to ensure secure gaming.

2.7.9 Miscellaneous

Across a diverse set of industry voices, cybersecurity is framed as a strategic necessity and a non-negotiable pillar for European competitiveness and safety. Rising cyberattacks are seen as a clear driver for public policy, and stakeholders broadly support protective objectives and justified legislation to raise the baseline of cybersecurity across Europe. For resilience and incident reporting, the insights imply the need for coordinated, clear, and proportionate regulatory frameworks that enable swift detection, reporting, and response while fostering collaboration between industry and authorities. The emphasis is on harmonized rules that strengthen systemic resilience without stifling innovation, anchoring incident reporting within a broader, proactive security posture.

eco understands the necessity for such regulation and supports the increase of the level of cybersecurity throughout Europe. (eco - Verband der Internetwirtschaft e.V.)

eco - Verband der Internetwirtschaft e.V.: The association endorses the necessity of EU-level cybersecurity regulation to elevate security standards, supporting measures that strengthen resilience and coherent incident reporting across Europe.

eco understands the necessity for such regulation and supports the increase of the level of cybersecurity throughout Europe.

Federation of Austrian Industries: It frames cybersecurity as a matter of strategic survival for industry, demanding resilient capabilities and effective incident reporting to safeguard operations.

Verband der Automobilindustrie e.V.: It positions cybersecurity as a non-negotiable pillar of automotive operations, requiring strong resilience and adherence to incident reporting obligations across the supply chain.

Association des Constructeurs Européens de Motocycles: It argues that escalating cyberattacks warrant regulatory action to bolster resilience and harmonize incident reporting in the mobility sector.

Dassault Systèmes: It supports protective cybersecurity objectives that enhance organizational resilience through preventive controls and proportionate incident reporting.

DIGITALEUROPE: It recognizes that cybersecurity legislation is justified to raise baseline security and resilience, while calling for balanced, workable incident reporting.

2.8 AI Governance, Transparency and High-Risk Safeguards

The central insight is a lifecycle, risk-proportionate regime that preserves core safeguards while clarifying scope and roles, aligning upstream model accountability with downstream deployment controls and public transparency. High-risk classification should be precise, sector-aware, and tiered where needed, without eroding protections or overburdening innovation. Transparency and registration remain pillars: clear user notices, deep-fake labelling, a usable public database, and training-data summaries balanced against trade-secret safeguards. Strong data governance underpins fairness and auditability through provenance, continuous bias monitoring, EU-wide benchmarking, and privacy-preserving retention. Safety-by-design, adversarial robustness, and meaningful human oversight, backed by independent assurance, are integral. A rights-first approach mandates FRIAs distinct from DPIAs, accessibility checks, and leverages procurement, certification, and liability to steer markets. Documentation, quality management, post-market monitoring, and broad incident reporting create early warning, with clarified duties for deployers and modular systems and proportionate support for SMEs. Legal certainty depends on firm timelines, empowered enforcement, and guidance; standards operationalize but do not condition obligations. Coherence with sectoral regimes (e.g., MDR, finance) and horizontal EU law avoids gaps while preserving distinct purposes. For GPAI, clearer systemic-risk criteria,

upstream transparency, provenance/watermarking, and workable IP safeguards prevent responsibility shifting. A pragmatic ethos prioritizes societal benefit and targeted governance. Across sub-categories, the dominant trends are consolidation around robust safeguards plus proportionality, and a shift toward upstream accountability, evidence-based testing, and transparent, enforceable oversight.

2.8.1 Implementation, Standards, Enforcement & Legal Certainty

This category centers on making the EU AI Act workable through clear implementation timelines, robust enforcement architecture, and legal certainty. Stakeholders frame the Act as product safety legislation that should deliver high-quality, rights-respecting AI, cautioning against reopening core obligations or delaying application. A concrete compliance horizon for high-risk systems (e.g., by August 2, 2027) is seen as essential to predictability and enforcement, alongside empowering the EU AI Office and ensuring responsive guidance (especially for the public sector) to keep obligations on track. Standards and guidance are treated as key instruments for operationalizing compliance, but not as prerequisites for legal duties; obligations apply even absent harmonised standards. Calls for simplification are welcomed only if they preserve precision and safeguards for fundamental rights. Implementation readiness depends on institutional capacity, sector-specific clarity (e.g., AI-first public services), and transparency with competent oversight to build trust and enable confident adoption.

> *Article 111 of the AI Act states that, starting August 2, 2027, all high-risk AI systems falling under the New Legislative Framework (NLF) - including those used in medical devices- must fully comply with the AI Act before they can be placed on the market.* (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)
>
> *Harmonised Standards are important tools for operationalising compliance, but they are not a precondition for legal obligations as they are voluntary tools.* (ANEC)
>
> *Capacity before codification: Simplification cannot be meaningful where institutional capacity to implement complex frameworks remains limited.* ()
>
> *The fourth part of the Omnibus considers amendments to the EU's AI Act, despite the nascent nature of its implementation and enforcement.* (Civil Liberties Union for Europe)
>
> **:** Frames the AI Act as product safety legislation compelling providers to deliver high-quality AI, anchoring enforcement in product conformity and reliability.
>
> *The EU AI Act is a valid product safety legislation that follows the target of forcing providers of AI systems to create high-quality products.*
>
> **FERMA - Federation of European Risk Managers Associations:** Calls for strengthened governance through empowering the EU AI Office to ensure effective oversight and enforcement.
>
> *This better governance must also be implemented through the empowerment of the EU AI Office.*
>
> **Encode Europe:** Supports simplification for efficiency but warns that poor implementation could erode legal precision and human rights protections, undermining legal certainty.
>
> *The AI Act is complex structurally & linguistically, thus an attempt at simplifying for efficiency/effectiveness is welcome but needs careful implementation strategies so not to lose precision & specificity and cause ambiguity, or less stringent protection of human rights.*
>
> **COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry:** Highlights a binding compliance deadline from 2 August 2027 for high-risk AI under the NLF, including medical devices, as a market access enforcement trigger.
>
> *Article 111 of the AI Act states that, starting August 2, 2027, all high-risk AI systems falling under the New Legislative Framework (NLF) - including those used in medical devices- must fully comply with the AI Act before they can be placed on the market.*
>
> **Civil Liberties Union for Europe:** Cautions against amending the AI Act during its nascent implementation phase, stressing the need for enforcement stability and legal certainty.
>
> *The fourth part of the Omnibus considers amendments to the EU's AI Act, despite the nascent nature of its implementation and enforcement.*

German Social Insurance European Representation: Welcomes Commission guidance and an AI Act Service Desk but urges more responsive support tailored to public sector implementation needs.

The guidelines announced by the Commission and the planned AI Act Service Desk are welcomed in principle, but need to be more responsive to the needs of the public sector.

Accountancy Europe: Emphasizes that robust governance and oversight beyond market forces are essential to ensure trustworthy AI and protect businesses and citizens.

1.) Digitalisation, automation and AI are too important to leave it to the markets alone to create confidence in their suitable functioning and to properly protect businesses and citizens

Centre for Democracy and Technology Europe: Opposes any postponement and urges timely application of all AI Act obligations to preserve legal certainty and safeguards.

Finally, we reiterate our position that there should be no delay in the application of any obligations under the AI Act, as targeted as any such delays may be.

BEUC - The European Consumer Organisation: Rejects reopening, exemptions, or delays, insisting on full and prompt implementation to protect consumers and uphold safeguards.

BEUC opposes any measures to reopen, exempt or delay the implementation of the AI Act.

National Land Survey of Finland: Argues that an AI-first policy requires clear rules and guidance to prioritize compliant, productivity-enhancing use cases in practice.

The proposed "AI first" policy requires clear rules and guidance so that productivity-enhancing use cases (e.g., cus- tomer service, document processing) are identified, and agreed upon.

Democracy Reporting International (DRI): Warns that the simplification package risks reopening core obligations, endangering negotiated safeguards and legal certainty.

We are concerned that the simplification package will lead to a reopening of the AI Acts core obligations, elements that were the result of a long and difficult negotiation process.

CERMI: Stresses that effective implementation must be inclusive and rights-respecting to ensure equitable enforcement outcomes.

Optimal implementation is, by definition, inclusive and respectful of rights.

The Danish Consumer Council: Reiterates that the Act must uphold safety, fundamental rights, and trust while enabling innovation, requiring strong enforcement.

The Act was designed to promote innovation and most critically to address urgent risks to safety, fundamental rights, and trust in artificial intelligence.

: Argues that institutional capacity should precede further codification or simplification to ensure feasible implementation.

Capacity before codification: Simplification cannot be meaningful where institutional capacity to implement complex frameworks remains limited.

WKÖ - Austrian Federal Economic Chamber: Calls for high transparency and competent oversight of algorithms, data, and operations to build company trust and enable confident adoption.

A high level of transparency regarding the design of the algorithms, the data used, the business models and the operating mechanisms, as well as the assurance of oversight by a competent institution, are crucial for companies' trust in AI technologies and their confident adoption.

AI & Partners B.V.: Advises against substantive AI Act amendments in the Omnibus to maintain legal certainty and predictable enforcement.

But with respect to the Artificial Intelligence Act, the Commission should avoid substantive amendments to primary law in this Omnibus.

ANEC: Notes that harmonised standards support compliance but are voluntary, and obligations apply regardless of standards' availability.

Harmonised Standards are important tools for operationalising compliance, but they are not a precondition for legal obligations as they are voluntary tools.

2.8.2 Sectoral Alignment & Regulatory Coherence

This category captures calls to align the AI Act's high-risk regime with sectoral rules and product legislation to avoid gaps, overlaps, and legal uncertainty. Stakeholders from rail, energy, healthcare/medical devices, and consumer goods stress that exemptions or cross-references are insufficient unless paired with precise, sector-specific definitions, use cases, and governance pathways. Ambiguities in Article 6 and Annex I for New Legislative Framework products, unclear "safety component" scopes, and risks of backdoor high-risk expansion (e.g., via standards under the Radio Equipment Directive) are seen as threats to regulatory coherence. Several contributors also urge integration with existing sector frameworks (e.g., MDR for medical AI) and the development of sector-specific guidance, while public bodies emphasize the need to tailor toolkits and policies to national legal contexts. A second theme is horizontal coherence with EU digital laws. Industry seeks to streamline duplicative processes (e.g., GDPR DPIA-related notifications or extra questionnaires), yet civil society and academia caution that different instruments serve distinct purposes and scopes (AI Act vs DSA/GDPR/ePrivacy), warranting preservation of separate risk and rights assessments—especially given the AI Act's focus on AI-specific risks and reasonably foreseeable misuse. In finance, obligations should combine with existing risk management while addressing deployment and legacy-system gaps; more broadly, stakeholders call to preserve core safeguards, clarify provider liability beyond the GDPR, and leverage EU frameworks to ensure consistent, sector-aware governance across high-risk contexts.

Particularly serious from the perspective of ZVEI are the ambiguities and inconsistencies arising from Art. 6 (1) in combination with Annex I, Section A of the AI Act, which determines the high-risk AI criteria for products that are already regulated under other legal acts of the New Legislative Framework (NLF) (e.g. machinery, radio equipment and medical devices). (ZVEI e.V.)

To support companies in the classification of Al systems as "high-risk" and provide them with better visibility on the resulting obligations, it will be essential to clarify not only the definition and perimeter of "safety components" for the energy sector, but also the way companies can classify Al systems as "high-risk" in complex circumstances outside of the use cases of the Act. (ENGIE)

The Al Act's default position of a DSA risk assessment being dispositive of a risk assessment under the AI Act may however be far too simple in light of the challenges emerging from the integration of AI systems or GPAI models. (Centre for Democracy and Technology Europe)

The AI Act risk management requirement for AI systems encompasses risks emerging from both intended uses and reasonably foreseeable misuses, which the DSA does not explicitly require. (Centre for Democracy and Technology Europe)

SIEMENS AG: Siemens warns that the AI Act's general high-risk requirements could be applied to railway products without adequately reflecting sector-specific needs, urging alignment with the Interoperability Directive via delegated or implementing acts.

Therefore, there is the risk that the AI Act introduces its high-risk requirements into railway products, without addressing the requirements of the different applications in the railway sector to the necessary extent.

ZVEI e.V.: ZVEI highlights ambiguities in how the AI Act defines high-risk AI for products already regulated under New Legislative Framework laws, calling for clearer, consistent criteria across sectors.

Particularly serious from the perspective of ZVEI are the ambiguities and inconsistencies arising from Art. 6 (1) in combination with Annex I, Section A of the AI Act, which determines the high-risk AI criteria for products that are already regulated under other legal acts of the New Legislative Framework (NLF) (e.g. machinery, radio equipment and medical devices).

Bitkom e.V.: Bitkom urges streamlining to avoid duplicative obligations by aligning AI Act risk processes with GDPR DPIA practices, including removing authority notifications and an extra AI Office questionnaire.

Additionally, the obligation to notify authorities (Art. 27(3)) should be deleted, as DPIAs under the GDPR do not have such a mandatory notification requirement.

ENGIE: ENGIE stresses that unclear high-risk classifications and absent sector-specific definitions in energy hinder compliance, calling for tailored guidance beyond the Act's listed use cases.

The lack of sector-specific definitions and use cases makes compliance all the more challenging for energy actors who are faced with great uncertainty over the obligations they might be subject to for providing/deploying AI systems.

Centre for Democracy and Technology Europe: CDT argues that AI Act, DSA, GDPR and sectoral risk assessments serve different scopes and should remain distinct, cautioning against simplistic equivalence while supporting coordinated but separate safeguards.

We find that those procedures and assessments have little overlap in personal and/or material scope, underscoring the need for these separate assessments to be preserved.

National Land Survey of Finland: The National Land Survey of Finland supports an AI toolkit for public administrations but says it must be adapted to national law and paired with clear rules for prioritizing suitable use cases.

The proposed AI toolkit for public administrations is commendable, but it requires national adjustment; for example, the implementation of the toolkit must consider the Finnish Data Management Act (tiedonhallintalaki).

Danish Society of Engineers (IDA): IDA calls for sector-specific AI guidelines to translate the AI Act into practical, coherent requirements across industries and professions.

Federation of German Consumer Organisations (vzbv): The German consumer federation urges preserving robust AI Act safeguards and aligning them coherently with adjacent frameworks to ensure consistent consumer protection across sectors.

University of Amsterdam: The University of Amsterdam highlights gaps between ePrivacy and AI strategies and necessary safeguards, calling for stronger alignment and regulatory coherence.

BVMed - Bundesverband Medizintechnologie e.V.: BVMed seeks integrated AI governance with the Medical Device Regulation and clarity for investigational devices to avoid gaps and conflicting obligations in healthcare.

Insurance Europe: Insurance Europe emphasizes that existing sectoral rules already govern AI uses in insurance and finance, urging the AI Act to recognize and align with them to prevent duplication.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: The authors note that AI regulation can complement GDPR by addressing provider liability gaps, advocating coherent allocation of responsibilities across regimes.

European Society of Radiology: The European Society of Radiology calls for clear, health-specific obligations for general-purpose AI in clinical contexts, aligned with medical standards and existing regulations.

Mistral AI: Mistral advocates aligning and leveraging EU AI frameworks to ensure coherent obligations that support innovation and cross-sector interoperability.

APPLiA (Home Appliance Europe): APPLiA warns against expanding high-risk scope via Radio Equipment Directive standardization and calls for clear boundaries to maintain regulatory coherence.

2.8.3 Risk Classification, Proportionality & Burden Reduction

This category synthesizes calls to clarify and calibrate the AI Act's high-risk scope while preserving core safeguards. Stakeholders stress precise, sector-aware risk classification—e.g., clearer definitions of "safety component," alignment with MDR/IVDR for medical AI, and detailed examples to ensure harmonized interpretation across domains like healthcare and finance. Several urge moving beyond a rigid high/other binary by introducing clearer thresholds or intermediate tiers to better match real-world risk profiles, while civil society warns that current rules may already omit risky systems and that any "simplification" must not erode Article 6's high-risk protections. Proportionality and burden reduction are central: providers caution against

disproportionate obligations, especially for highly evolutive systems where conformity assessment and post-market monitoring can become impractical and innovation-chilling. Proposals emphasize high thresholds for "significant changes," evidence-based streamlining to remove duplicative reporting, and reliance on standards, codes, and guidance—reducing administrative load without reopening the Act's foundations or weakening rights and safety safeguards. The unifying theme is a risk-based, targeted regime that avoids over- or under-classification, supports trustworthy AI uptake, and maintains robust protections for fundamental rights and safety.

> *It is very important that the risk classifications are comprehensively defined and supported by detailed sector-specific examples that take into account the unique risk profiles of certain sectors to facilitate a harmonized interpretation (e.g. healthcare, gambling, finance, etc.).* (WKÖ - Austrian Federal Economic Chamber)
>
> *It is essential to avoid imposing a disproportionate and counter-productive burden on our development teams.* (Airbus)
>
> *This leads to a perverse outcome: a regulation intended to enhance safety would, in this instance, directly cause a reduction in the level of safety on our aircraft.* (Airbus)
>
> *The logic of conformity assessment is very difficult to apply to AI systems with high evolutivity such as platforms hosting AI features.* (Airbus)

GSMA: Calls for clearer AI Act scope and high-risk criteria in telecoms, including a precise definition of "safety component" and detailed guidance to ensure consistent, proportionate classification.

> *The term 'safety component' should therefore be more precisely defined in the law and should remain to be the primary criterion for assessing high risk AI within the scenarios outlined in the AI Act.*

Airbus: Warns that disproportionate post-market and conformity burdens on evolving high-risk, safety-focused AI could force abandonment of beneficial projects, urging high thresholds for significant changes.

> *This leads to a perverse outcome: a regulation intended to enhance safety would, in this instance, directly cause a reduction in the level of safety on our aircraft.*

Civil Liberties Union for Europe: Insists simplification must not undermine Article 6 or the high-risk scope, noting current rules may omit systems that should be classified as high-risk.

> *It is imperative that the simplification process is not used as a tool to weaken, waterdown, or otherwise derogate the higher standards for high-risk AI systems, and the safeguards mandated under Article 6 or supporting articles, such as Article 27.*

Centre for Democracy and Technology Europe: Argues the AIA rightly complements MDR/IVDR by classifying certain medical AI as high-risk to address AI-specific risks like bias and information failures.

> *The Act stipulates that medical devices will be considered to be a high-risk AI system if the AI system is a safety component of a medical device - or the Al system is itself a medical device - and the medical device is subject to a third-party conformity assessment by a notified body in accordance with the MDR/IVDR.*

Democracy Reporting International (DRI): Supports simplification only with robust evidence and cautions that it must not dilute core high-risk obligations; current evidence does not justify deregulation.

> *Without such evidence, there is a major risk that simplification is a code word for deregulation.*

Meta Platforms Ireland Limited: Highlights gaps in standards and clarity that risk disproportionate burdens and fragmented interpretation of the high-risk framework, potentially hindering innovation.

> *These deficiencies may impose disproportionate burdens on providers and potentially impede AI innovation within the EU.*

2Dyles Services: Criticizes the binary high-risk/other model as too rigid and calls for a defined medium-risk tier with proportionate mitigation to avoid unnecessary burdens.

The current binary classification (high-risk vs. other) is too rigid.

WKÖ - Austrian Federal Economic Chamber: Requests comprehensive, sector-specific risk classifications and examples to ensure harmonized, proportionate interpretation across domains.

It is very important that the risk classifications are comprehensively defined and supported by detailed sector-specific examples that take into account the unique risk profiles of certain sectors to facilitate a harmonized interpretation (e.g. healthcare, gambling, finance, etc.).

AI & Partners B.V.: Advocates keeping strong high-risk safeguards while reducing administrative burden through pragmatic tools that support uptake without weakening protections.

That strengthens competitiveness by reducing administrative burden and enabling diffusion of trustworthy AIwithout undermining its role.

Compagnie Nationale des Commissaires aux Comptes (professional organisation for statutory auditors): Notes that compliance burdens under high-risk regimes largely fall on AI providers, underscoring the need for proportionate allocation and support.

: Suggests moving beyond simple tiers and baselines toward nuanced governance that calibrates obligations across the risk spectrum.

ENSHPO - The European Network of Safety and Health Professional Organizations: Calls for smart, flexible risk-based regulation that scales obligations to actual hazards while safeguarding health and safety.

Business & Science Poland: Warns that outdated compute-based metrics can misclassify risk and urges updated, proportionate criteria to avoid blind spots.

European Law Institute: Endorses a nuanced risk-based approach that treats automated decisions, biometric/body data, profiling, and systematic monitoring as high-risk, with obligations scaling by context and scale while exempting necessary sharing where justified.

German Property Federation: Supports risk-based record-keeping and thresholds to tailor obligations and avoid excessive burdens.

Nordic Financial Unions - the Nordic financial trade unions confederation: Emphasizes employment-related AI as high-risk and calls for strong oversight and safeguards proportionate to impacts on workers.

European Public Service Union: Warns that AI Act simplification must not become deregulation that weakens high-risk safeguards in public services.

TÜV-Verband e. V.: Opposes deregulation and favors risk-based safeguards and assessments that ensure proportional safety without unnecessary expansion.

U.S. Chamber of Commerce: Calls for ambitious, risk-based simplification that reduces burdens for low-risk uses while clarifying high-risk criteria.

Danish Society of Engineers (IDA): Urges clearer definitions of high-risk AI to ensure predictable, proportionate obligations.

Federation of German Consumer Organisations (vzbv): Supports maintaining a broad high-risk scope to protect consumers while implementing proportionate, risk-based obligations.

CPME: Backs a risk-based information and transparency approach calibrated to medical risk profiles.

AI Standards Lab: Observes that multiple AI Act assessments are uncommon, implying current burdens may be manageable but should remain proportionate.

Advertising Information Group: Advocates shifting toward risk-based regulation in advertising while challenging simplistic claims that downplay risks.

ICMP - International Confederation of Music Publishers: Urges avoiding any weakening of the AI Act's calibrated risk framework and keeping strong obligations for high-risk use cases.

Google: Proposes targeted simplifications to reduce duplicative burdens and clarify scope without compromising high-risk safeguards.

AK Wien: Notes high-risk AI is prevalent in practice, reinforcing the need for robust safeguards and oversight.

AFME: Asks for clarity that traditional models like logistic regression are regulated when used in Annex III contexts and supports use-case-based high-risk triggers.

Forvis Mazars: Highlights unclear risk classification criteria and calls for proportional, risk-based obligations to avoid unnecessary burdens.

MFE-MEDIAFOREUROPE N.V.: Opposes AI Act simplification that would lead to deregulation, favoring retention of the current risk calibrations.

Homo Digitalis: Warns that deregulation would heighten risks and urges preservation of stringent high-risk safeguards.

Connect Europe: Seeks to avoid blanket high-risk labels and to distinguish safety from security considerations in classification.

Bayer AG: Accepts that high-risk AI warrants full compliance and oversight aligned with potential harms.

E.ON SE: Calls for clearer high-risk definitions and harmonized standards to enable proportionate compliance.

LinkedIn Ireland: Expresses concern about over-classifying benign AI as high-risk and urges proportional scoping and obligations.

Prosus Group: Requests clearer high-risk definitions to protect users without chilling beneficial innovation.

Dassault Systèmes: Supports a risk-based approach that tailors obligations to impact and avoids blanket burdens.

Computer & Communications Industry Association (CCIA Europe): Warns against overclassification of low-risk AI and seeks recalibration to reduce unnecessary burdens.

Danish Industry: Advocates proportionate, risk-based rules with clear definitions to limit unnecessary compliance costs.

Eurosmart: Argues that company size is not a proxy for AI risk and obligations should hinge on the system's actual risk.

DIGITALEUROPE: Urges preventing unjustified expansion of the high-risk scope and keeping obligations proportionate to risk.

AI Accountability Lab (AIAL), Trinity College Dublin: Rejects the use of dual-use arguments to downgrade risk classification and calls for safeguards based on actual risks.

SaferAI: Asserts that high-risk requirements are reasonable and necessary, cautioning against weakening them under simplification efforts.

2.8.4 Fundamental Rights, Impact & Accountability

This category advances a rights-first model for governing high-risk AI, with Fundamental Rights Impact Assessments (FRIAs) as non-negotiable safeguards distinct from GDPR DPIAs. FRIAs cover the full spectrum of fundamental rights, prompt analysis of disparate impacts, and are systematically required for public-sector deployments; they include notifying competent authorities and publishing summaries in the high-risk database, bolstering transparency and accountability before deployment. In tandem with prohibitions and due-diligence duties under the AI Act, these tools steer innovation away from bias and harm and toward trustworthy, rights-respecting systems. Contributors oppose deregulation or "simplification" that would dilute core protections, emphasizing that risks to safety, consumer and fundamental rights are immediate and that the AI Act operates as a due-diligence framework, not a mere burden. They call for ethical performance indicators beyond administrative burden reduction and for conformity assessments of high-risk systems to explicitly evaluate accessibility and discriminatory impacts for persons with disabilities, with guidance co-created with disability organizations. Public procurement, certification, and liability incentives are highlighted as levers to uphold rights, create a level playing field, and maintain EU leadership in accountable AI governance.

> *The Fundamental Rights Impact Assessments (FRIAs) are essential for preventing rights violations before deployment.* (Civil Liberties Union for Europe)
>
> *The AIA offers certain provisions for AI system developers, providers and users that are necessary to mitigate bias and harm, to enhance transparency and accountability, and to ensure compliance with EU fundamental rights.* (Civil Liberties Union for Europe)
>
> *For the Digital Fitness Check that will analyze the cumulative effects of the simplification, we encourage to not only analyse the reduced administrative burden, but also include ethical performance indicators, e.g. transparency of AI-related decision-making & notifications of bias and harm caused by AI-systems.* (Encode Europe)
>
> *This imperative is clear from the AI Act, which notably requires a summary of the FRIA to be made publicly available upon registration of an AI system in the high-risk database23 - in stark contrast to DPIAs, which are never required to be made public.* (Centre for Democracy and Technology Europe)

Encode Europe: Urges including ethical performance indicators like transparency, bias and harm notifications in AI evaluations, not only reduced administrative burden.

> *For the Digital Fitness Check that will analyze the cumulative effects of the simplification, we encourage to not only analyse the reduced administrative burden, but also include ethical performance indicators, e.g. transparency of AI-related decision-making & notifications of bias and harm caused by AI-systems.*

European Disability Forum: Warns against deregulating the AI Act and frames it as due diligence to address risks, guiding innovation toward trustworthy, rights-respecting AI.

> *Prohibitions (e.g., Article 5) and due diligence requirements guide innovation towards trustworthy, rights-respecting AI, ensuring a level playing field and protecting responsible actors.*

Civil Liberties Union for Europe: Insists FRIAs remain intact and distinct from GDPR DPIAs to prevent rights violations and enhance transparency and accountability.

> *The Fundamental Rights Impact Assessments (FRIAs) are essential for preventing rights violations before deployment.*

Centre for Democracy and Technology Europe: Explains why FRIAs are indispensable and broader than DPIAs, especially for public authorities, as a last line of defense for fundamental rights.

> *FRIAs are the line last of defense standing between a harmful deployment of an Al system and an - often unsuspecting - affected population.*

BEUC - The European Consumer Organisation: Recognises the AI Act as essential for safeguards and prohibitions based on risks to fundamental and consumer rights.

> *The AI Act is an important embodiment of this ambition, introducing safeguards and prohibiting some types of AI based on identified risks to fundamental and consumer rights.*

Democracy Reporting International (DRI): Stresses preserving AI Act safeguards as central to accountability and fundamental rights, maintaining EU leadership on trustworthy AI.

These measures are central to ensuring accountability, protecting fundamental rights, and maintaining the EU's leadership in setting global standards for trustworthy Al.

CERMI: Calls for accessibility and discrimination checks within high-risk AI conformity assessments, clarified via guidelines with disability groups.

The conformity assessment process for high-risk AI systems must explicitly include an evaluation of their accessibility and potential discriminatory impact on persons with disabilities.

ANEC: Emphasises the AI Act's role in addressing urgent risks to safety, fundamental rights, and consumer trust, outweighing convenience concerns.

The Act was designed to promote innovation and most critically to address urgent risks to safety, fundamental rights, and trust in artificial intelligence.

ENSHPO - The European Network of Safety and Health Professional Organizations: Highlights increased stress from AI-driven management, underscoring the need for safeguards to protect workers' rights and accountability.

European Law Institute: Advocates introducing new AI-specific rights to strengthen protections and accountability frameworks.

Irish Farmers' Association: Calls for transparency and fairness in AI to protect farmers' rights and ensure accountable governance.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Promotes intersectional, power-aware compliance and exit rights to justify high-risk AI, critiquing harmful assumptions to protect rights.

Nordic Financial Unions - the Nordic financial trade unions confederation: Warns of digital dehumanisation from algorithmic management and urges democratic worker-led co-design to uphold rights and accountability.

European Public Service Union: Centers worker involvement in AI governance to safeguard fundamental rights and ensure accountable deployment in public services.

AI Standards Lab: Argues the AI Act's constraints are necessary to prevent harms and protect fundamental rights and accountability.

eyeo GmbH: Supports maintaining strict consent requirements for high-risk AI to uphold transparency, autonomy, and rights.

Fedoweb - Federazione Operatori Web: Notes AI-amplified misinformation risks and calls for accountable safeguards to protect information integrity and rights.

ENNHRI - European Network of National Human Rights Institutions: Affirms the AI Act addresses fundamental rights risks through transparency, accountability, and high-risk safeguards.

WITNESS: Advocates rights-responsive, accountable AI governance and strong AI Act protections against harmful deployments.

MVFP Medienverband der freien Presse e.V.: Raises impact and scope concerns while stressing preservation of transparency and rights safeguards within the AI Act.

Danish Institute for Human Rights: Calls for mandatory impact assessments to identify and mitigate fundamental rights harms from high-risk AI deployments.

Bayer AG: Urges accountability for AI in cloud environments to ensure transparency and protect users' rights.

Renault Group: Supports thorough impact assessments for high-risk AI to prevent rights infringements and strengthen accountability.

: Advocates mandatory fundamental rights assessments for high-risk AI to safeguard rights and guide responsible deployment.

European Trade Union Committee for Education (ETUCE): Defends EU AI safeguards to protect education workers' and learners' rights and ensure accountable AI use in schools.

European Digital Rights (EDRi): Warns that reopening or weakening AI laws undermines co-legislators and erodes fundamental rights protections and safeguards.

Dassault Systèmes: Supports ethical AI consultations to improve transparency, accountability, and trust in governance.

European Network Against Racism (ENAR): Criticises AI Act deregulation and urges preserving safeguards to prevent racial discrimination and protect rights.

AI Accountability Lab (AIAL), Trinity College Dublin: Highlights AI risks to democracy and rights and opposes diluting the AI Act, calling for accountability-centred regulation.

Access Now Europe: Notes public support for strong protections given AI risks and urges robust accountability and rights-preserving safeguards.

2.8.5 Transparency, Disclosure & Registration

Transparency, disclosure, and registration are central safeguards in the AI Act's governance framework. Stakeholders emphasize robust enforcement of Article 50 obligations—clear labelling of synthetic content and deep fakes, notifications for emotion recognition and biometric categorization, and GDPR-compliant data handling—so people understand when and how AI affects them. Article 49's public EU database for high-risk systems is highlighted as a cornerstone for accountability, documenting intended purpose, operating logic, and data inputs to help individuals and organizations check compliance and seek remedies. General-purpose AI providers are expected to publish training-data summaries to enable rights holders to exercise copyright and other legitimate interests. Debate focuses on scope, accessibility, and proportionality. Some warn against postponements or derogations and oppose weakening transparency duties, while others seek clarity on what 'publicly available' entails to protect commercially sensitive information and trade secrets through well-defined safeguards. There are calls to remove registration burdens for non-high-risk systems and concerns about implementation timelines and standardization delays. Proposals to strengthen trust include mandating algorithmic transparency, publishing DPIA/FRIA elements, requiring vendor declarations, improving compute and server-side transparency, and leveraging open-source approaches—sometimes with controlled access via accredited persons—to balance openness with security and business confidentiality.

Under Article 49, providers must register high-risk AI systems in the EU database before market placement, with most information becoming publicly accessible (Centre for Democracy and Technology Europe)

For example, providers of AI systems generating synthetic content must ensure outputs are labelled in a machine-readable format; and deployers of AI systems generating deep fakes or manipulating texts informing the public on matters of public interest must disclose that the content has been artificially created or modified.51 (Centre for Democracy and Technology Europe)

Article 49 of the EU AI Act requires providers to register AI systems in an EU database, regardless of whether they are ultimately classified as high-risk. (Ibec)

GPAI providers must draw up and make publicly available a sufficiently detailed summary about the content used for model training, following a template provided by the AI Office. (Centre for Democracy and Technology Europe)

Technology Industries of Finland: Advocates deleting Article 49(2) to remove registration requirements for Annex III AI considered not high-risk. Opposes non-high-risk AI registration to streamline transparency obligations.

Art. 49(2): Delete Art. 49(2) on registration of AI systems within scope of Annex III but considered not high-risk, as per Article 6(3).

Civil Liberties Union for Europe: Urges immediate, full enforcement of Article 50 transparency duties, including deepfake labelling and informing users of emotion recognition/biometric categorisation. Rejects derogations or delays that would let deployers evade these requirements.

Transparency provisions under Article 50 must also be preserved and enforced without delay.

Accountancy Europe: Calls for algorithm transparency as essential to build trust and protect businesses and citizens.

5.) Transparency of algorithms is necessary, as only transparency can build trust among and adequately protect businesses and citizens

ENGIE: Seeks clarity on what 'publicly available' means for the EU AI database to manage access and mitigate commercial sensitivity risks.

Additionally, it will be paramount to clarify what "publicly available" (art. 71 par. 4) practically entails when it comes to the accessibility of the information registered in the EU database.

Centre for Democracy and Technology Europe: Supports public registration and accessible overviews of high-risk AI systems to enable accountability and oversight. Also backs synthetic content labelling and GPAI training data summaries to inform rights holders and the public.

Under Article 49, providers must register high-risk AI systems in the EU database before market placement, with most information becoming publicly accessible

Ibec: Warns that registration obligations and delayed harmonised standards make timely compliance unrealistic for enterprises.

There is significant concern on whether it realistic to expect enterprise to meet the current requirements on time.

CERMI: Insists that AI interaction disclosures be provided in universally accessible formats. Calls for explicit regulatory language mandating accessibility.

The obligation to inform individuals when interacting with an AI system (e.g., emotion recognition or biometric categorisation) must be fulfilled by providing information in universally accessible formats.

Almega: Requests well-defined exceptions and safeguards in disclosure obligations to protect trade secrets and confidential information. Stresses alignment with the Trade Secrets Directive.

Well-defined exceptions and safeguards must apply for disclosure obligations under Article 13 of the AI Act, so companies are protected from disclosure of confidential information.

WKÖ - Austrian Federal Economic Chamber: Argues that open-source approaches promote transparency and trust, spreading AI benefits more fairly across the economy.

pen Source approaches promote transparency, strengthen companies' trust in the technologies used and ensure that the benefits of artificial intelligence are distributed more broadly and fairly across the European economy.

: Proposes mandating open-source use for transparency and reliability while restricting access to accredited persons rather than the general public.

Of course, there is a need for simplification of laws, including all of them, making the use of open source mandatory, for reasons of transparency and reliability, but this access, paradoxically for businesses, by accredited persons, not the average person.

American Chamber of Commerce to the EU: Calls for increased transparency and robust stakeholder consultation in AI governance processes.

Compagnie Nationale des Commissaires aux Comptes (professional organisation for statutory auditors): Emphasizes transparent AI outputs to support auditability and strengthen trust in auditing.

European Travel Retail Confederation (ETRC): Opposes full exemptions from AI labelling requirements, supporting consistent transparency for consumers.

SEC4AI4SEC: Highlights that transparency and explainability are critical to building trust and ensuring secure AI deployment.

Kompetenznetzwerk Datentreuhandmodelle (DatNet): Advocates expanding governance details in the public AI register to bolster accountability and oversight.

Inter IKEA Group: Recommends mandating vendor declarations of AI systems to enhance supply-chain transparency.

Federation of German Consumer Organisations (vzbv): Opposes any weakening of AI transparency duties to protect consumer rights and informed use.

ENNHRI - European Network of National Human Rights Institutions: Urges upholding remedies and rights, including transparency, explanations, and registration, to safeguard fundamental rights.

AFME: Notes that downstream providers lack transparency into upstream compute usage, hindering risk assessment and compliance.

MFE-MEDIAFOREUROPE N.V.: Demands transparency over training data sources to protect media interests and intellectual property.

Bocconi University: Encourages disclosure of transparent, auditable methodologies to enable evaluation and oversight of AI systems.

European Publishers Council: Calls for strong transparency, labelling, provenance tracking, and enforcement to govern AI-generated content.

: Suggests pre-access review and server-side transparency measures to rebuild user trust in AI services.

Enedis: Supports applying trade secret and security exceptions to limit disclosure of sensitive AI information in public registries.

: Contends that transparency should be implemented through code and technical measures rather than additional legal mandates.

2.8.6 Data Governance, Testing & Traceability

Data governance, testing, and traceability for AI systems demand high-quality, well-documented, and provenance-verifiable datasets, with explicit provisions to ensure non-discrimination, accuracy, and traceability. Strong governance obligations over training, validation, and testing data should be maintained, paired with continuous, lifecycle bias monitoring rather than one-off corrections. This includes accommodating the rights of persons with disabilities and ensuring population coverage, while resolving tensions between deletion rules for special-category data and the need for auditability by using privacy-preserving retention (e.g., pseudonymisation) to enable retrospective verification and incident investigation. Testing and traceability extend into post-deployment monitoring, audit trails, reproducibility, and formal benchmarking capacity. Given AI's opacity and the difficulty of defining and verifying behavior, stakeholders call for EU-wide benchmarking and oversight, robust data accuracy requirements, and procurement practices that require proof of data provenance. Assurances must be evidence-backed through rigorous validation and quality control. Regulatory sandboxes and data reuse rules should support safe testing and improvement: current "substantial public interest" thresholds can be too narrow, and retrospective consent may be impractical in domains like health, so

lawful reuse under strong safeguards should be enabled while aligning with GDPR via purpose limitation, data minimisation, and accountability.

> *As the AI Act requires non-discrimination, accuracy, and traceability in datasets, we advocate for more explicit provisions ensuring datasets meet these standards.* (Encode Europe)
>
> *Clarify that bias monitoring should continue throughout the Al system's lifecycle and that personal data used for this purpose should not be automatically deleted once initial bias correction has been achieved;* (Bitkom e.V.)
>
> *Amend Art. 59 to allow companies to re-use personal data they already hold for the testing and improvement of AI systems, under strong privacy safeguards, even if they do not directly serve a substantial public interest.* (Bitkom e.V.)
>
> *Obtaining consent retrospectively for AI training would often not be practical.* (Bitkom e.V.)

Encode Europe: Calls for explicit dataset quality provisions to operationalize AI Act requirements on non-discrimination, accuracy, and traceability. Emphasizes that clearer standards will accelerate cross-sector and cross-member-state harmonization.

> *As the AI Act requires non-discrimination, accuracy, and traceability in datasets, we advocate for more explicit provisions ensuring datasets meet these standards.*

Bitkom e.V.: Advocates continuous lifecycle bias monitoring with retention of necessary personal data and broader, safeguarded data re-use in sandboxes to improve testing and performance, including for sensitive data where consent may be impractical. Seeks clarification and amendments to enable responsible re-use beyond narrowly defined public interest cases.

> *Clarify that bias monitoring should continue throughout the Al system's lifecycle and that personal data used for this purpose should not be automatically deleted once initial bias correction has been achieved;*

CERMI: Urges that simplification must not weaken data governance over training, validation, and testing datasets. Stresses strong bias detection, prevention, and mitigation to protect the rights of persons with disabilities.

> *Simplification must not mean relaxing governance obligations over training, validation, and testing datasets.*

: Highlights that using pseudonymised data enables traceability and retrospective verification of development and testing datasets after errors or incidents. This supports accountability and robust post-market monitoring.

> *The use of pseudonymised data is key because the data, even if used for development and testing, must still be able to be subject to retrospective verification in case an error or serious incident is detected.*

: Recommends requiring verifiable data provenance proof in AI procurement to ensure traceability of inputs and accountable data governance.

SEC4AI4SEC: Notes that AI systems can impede verification, testing, and precise behavior definition, creating challenges for assurance and traceability. Calls attention to the need for adapted testing regimes and governance measures.

European Law Institute: Argues that removing training data alone is insufficient for compliance, implying stronger lifecycle controls and traceability mechanisms are needed. Encourages comprehensive governance beyond deletion remedies.

IDEMIA: Calls to build EU capacity for AI benchmarking to rigorously test, compare, and validate systems. Such infrastructure underpins transparency, reliability, and data governance.

Insurance Europe: Supports clear data accuracy requirements for AI models to ensure reliable outputs. Emphasizes that accuracy must be evidenced through robust testing and validation.

Eurosmart: Advocates strengthening EU AI benchmarking and oversight to enable consistent testing, traceability, and effective regulatory enforcement. Promotes coordinated infrastructure for trustworthy evaluations.

Access Now Europe: Warns that assurances without empirical evidence risk harmful impacts and calls for rigorous evidence-based evaluation. Emphasizes strict adherence to AI Act requirements with strong quality control and documentation across the lifecycle.

The European Network of Expertise on Omics: Emphasizes rigorous validation and testing of AI systems, particularly in scientific and omics contexts, to ensure reliability and traceability. Highlights the need for robust evaluation frameworks.

2.8.7 Safety-by-Design, Security & Human Oversight

This category emphasizes making safety and security intrinsic to AI systems across the entire lifecycle—from design and development to deployment and post-market monitoring. It calls for mandated safety-by-design, robust EU AI Act-aligned security standards, continuous fault detection, adversarial robustness, data integrity protections, transparent documentation, and independent assurance. Risks like data poisoning, jailbreaks, and prompt manipulation motivate stronger oversight, especially for high-risk and sensitive contexts, while regulatory flexibility must not dilute core safety goals. Human oversight should be substantive rather than symbolic. Clear standards are needed for human-in-the-loop/over-the-loop roles: defined responsibilities, demonstrable competencies, meaningful intervention and shutdown capabilities, audit trails, and escalation pathways. Guidance and examples (e.g., under Article 15) should not narrow the scope of required safeguards. Overall, the approach integrates security engineering, transparency, and empowered human oversight to detect faults, prevent misuse, and rapidly correct failures in practice.

Research on Al risks underscores the need for caution and stronger oversight of the Al industry. (Democracy Reporting International (DRI))

Numerous research findings highlight serious risks in AI development and deployment. (Democracy Reporting International (DRI))

This challenges previous assumptions that poisoning attacks require large-scale data control. (Democracy Reporting International (DRI))

Meanwhile, real-world examples of "jailbreaking" Al chatbots reveal how easily they can be tricked into producing harmful or sensitive information, including instructions related to terrorism and pathogens. (Democracy Reporting International (DRI))

Democracy Reporting International (DRI): Research highlights serious AI risks, including data poisoning and jailbreaks, warranting stronger industry oversight and safety-by-design controls. It calls for caution and robust governance across development and deployment.

Research on Al risks underscores the need for caution and stronger oversight of the Al industry.

Compagnie Nationale des Commissaires aux Comptes (professional organisation for statutory auditors): Endorses safeguards and proportionate restrictions on AI to uphold safety, security, and accountable human oversight. Emphasizes the legitimacy of limits to prevent harm in high-risk uses.

SEC4AI4SEC: Advocates assurance and regulation across the entire AI lifecycle, integrating safety engineering and rigorous evaluation. Stresses early fault detection and mitigation as core to safe operation.

European Law Institute: Recommends stricter oversight and governance for high-risk systems, with enforceable safety and transparency duties. Supports tighter supervision to protect fundamental rights and users.

Digital Business Ireland: Supports strong safeguards for high-risk applications, including transparency and meaningful human oversight. Aims to reduce risks to consumers and ensure responsible deployment.

FINANSFORBUNDET (CVR 15320613): Calls to maintain transparency mechanisms and develop human oversight competencies within organizations. Seeks continuous accountability and the ability to intervene when risks emerge.

Palombar - Associação de Conservação da Natureza e do Património Rural: Urges robust, built-in safeguards to prevent environmental and societal harms from AI. Emphasizes proactive risk management and security-by-design.

Federation of Austrian Industries: Affirms that AI safety objectives and clear rules should prevail over ad hoc flexibility. Promotes consistent safety-by-design, risk controls, and oversight.

Inter IKEA Group: Requests clear, effective standards defining human oversight roles and interventions. Focuses on practical guidance to ensure humans can supervise and correct AI behavior.

WITNESS: Calls to strengthen safety and transparency obligations to make AI auditable and accountable. Seeks stronger disclosures and safeguards, especially where risks to rights are significant.

Brunel University of London: Proposes an ethical AI framework supported by oversight to ensure safe, accountable systems. Encourages governance structures that integrate transparency and human control.

secunet Security Networks AG: Advocates stronger security standards under the EU AI Act, including robustness, cybersecurity, and testing. Emphasizes rigorous safeguards against adversarial threats.

The Center for Countering Digital Hate: Urges mandated safety-by-design measures to reduce harmful outputs and misuse. Calls for enforceable oversight and guardrails across high-risk deployments.

Eurosmart: Warns that regulatory flexibility must not introduce additional risk. Supports maintaining strong, reliable safeguards and security baselines.

: Critiques tokenistic human oversight and calls to clarify meaningful human-in-the-loop responsibilities. Argues automated processes require stronger, consolidated safeguards.

Estonian Ministry of Justice and Digital Affairs: Cautions that listing Article 15 examples could narrow the scope of cybersecurity and robustness obligations. Advocates broad, technology-neutral safeguards to preserve security-by-design.

Access Now Europe: Advocates strong safeguards and human oversight for high-risk AI in sensitive contexts to protect fundamental rights. Emphasizes transparency and accountability for systems with significant impact.

2.8.8 Documentation, Monitoring & Incident Reporting

This category covers a lifecycle regime that ties together technical documentation, post-market monitoring, and incident/usage reporting to create accountability and early warning for high-risk and general-purpose AI. Providers carry primary responsibility for system-level incident reporting on short timelines, with “serious incidents” defined broadly to include safety, environmental, property harms and fundamental-rights infringements. Obligations extend to deployers (e.g., notifying authorities when risks arise), specialized notifications for real-time remote biometric identification and annual usage reports, and GPAI duties such as notifying the Commission when models meet systemic-risk computational thresholds and submitting risk assessment materials to the AI Office. Technical documentation is the backbone of this regime: it must capture design, data, risk and system characteristics (per Annexes) to enable effective risk management, bias detection, DPIAs, and market surveillance. Quality management systems centralize records, help demonstrate compliance, and can shield providers from liability; SMEs benefit from simplified forms and unified documentation with sectoral frameworks, which also reduce downstream compliance burdens for deployers. Stakeholders diverge on scope and practicality. Civil society defends robust reporting and opposes deregulation, arguing that providers—not regulators—should bear the burden of cross-authority notifications to ensure timely corrective action and public trust. Several industry voices seek flexibility, warning that documentation demands are overly

extensive and that mandated, Commission-designed post-market monitoring plans may be too prescriptive; they also flag ambiguities for modular AI and the need to clarify deployer logging, and caution that overly strict rules could even hinder effective bias mitigation and monitoring. Public-sector deployers face additional registration and reporting duties in sensitive uses like biometrics.

> *The AI Act establishes mandatory incident reporting for providers within a short timeframe to ensure rapid responses to AI-related safety and rights violations.* (Centre for Democracy and Technology Europe)
>
> *Providers are required to establish and document a post-market monitoring system which collects, documents and analyses relevant data provided by deployers or otherwise collected to evaluate compliance with the Al Act's obligations.* (Centre for Democracy and Technology Europe)
>
> *The AI Act provides a novel and broad definition for serious incidents based on the nature of AI technology and its risks, capturing a range of consequences resulting from an incident or malfunctioning of an AI system, ranging from the death of a person or serious harm to a person's health, property or the environment, to the infringement of an obligation under EU law intended to protect fundamental rights.* (Centre for Democracy and Technology Europe)
>
> *Additionally, GPAI providers are required to notify the Commission within two weeks if their GPAI model meets the computational threshold of systemic risks capabilities.* (Centre for Democracy and Technology Europe)
>
> **Technology Industries of Finland:** Advocates deleting the AI Act's mandated, Commission-defined post-market monitoring plan to give providers flexibility in how they monitor systems after deployment.
>
> *Art. 72(3): Delete Art. 72(3) which requires providers to follow a specific post-market monitoring plan, whose framework will be designed by the Commission in an implementing act, giving providers flexibility in developing their own post-market monitoring plan and activities.*
>
> **Volkswagen Group:** Argues that technical documentation requirements for high-risk AI under Article 11 and Annex IV are excessively extensive and burdensome, covering detailed system and hardware information.
>
> *The requirements for the documentation of high-risk use cases from Article 11 and its detailing in Annex 4 are too extensive (texts, system documentation, hardware requirements, possi- bly images of hardware components, design specification).*
>
> **Civil Liberties Union for Europe:** Urges retaining and enforcing notification and serious-incident reporting obligations for high-risk AI, rejecting proposals to weaken them. Emphasizes these duties as essential for early warning, accountability, timely corrective action, and public transparency.
>
> *This article serves multiple critical aims, including: creating an early-warning system that allows market surveillance authorities to identify harmful uses or flag potential risks of high-risk AI systems at an early stage; it establishes accountability for providers of high-risk systems, ensuring that they take responsibility for the proper functioning and safety of their products; it enables market surveillance authorities to take action and implement corrective measures in a timely manner to minimize the damage done when serious incidents do occur; and it creates transparency in how these systems are used, which will help build public trust.*
>
> **Centre for Democracy and Technology Europe:** Describes targeted reporting duties for high-risk AI and GPAI (including mandatory incident reporting and systemic-risk notifications), required post-market monitoring plans, and robust technical documentation to support accountability and rights protection. Notes specific notifications for biometric uses and additional reporting burdens for certain public deployers.
>
> *Technical documentation is a necessary means to ensure transparency and a better understanding of AI artifacts71 which is vital to ensure accountability and an effective enforcement of the Al Act's provisio*
>
> **Leverhulme Centre for the Future of Intelligence at the University of Cambridge:** Suggests a governance approach that moves beyond mere compliance and documentation, promoting proactive monitoring and safeguards that exceed minimum legal requirements.

Inter IKEA Group: Requests clearer, more practical logging and record-keeping obligations for deployers to enable feasible monitoring and traceability.

Digital Currencies Governance Group (DCGG): Highlights ambiguity in documentation expectations for modular and composable AI systems, calling for guidance suited to componentized architectures and interfaces.

DIGITALEUROPE: Warns that overly strict documentation and monitoring rules may hinder effective bias mitigation and continuous post-market oversight and improvement.

2.8.9 GPAI Governance, Upstream Duties & IP Rights

This category centers on governing general-purpose AI (GPAI) through upstream obligations and intellectual property (IP) safeguards to mitigate systemic risks and clarify accountability. Stakeholders emphasize that GPAI poses broad harms (from discrimination and privacy breaches to copyright and environmental impacts), while the AI Act leaves "systemic risks" under-specified and current compute-only thresholds for high-impact models are seen as ambiguous or insufficient. A capabilities-based approach and clearer criteria are urged to keep obligations proportionate and future-proof. Across the board, the call is to anchor duties upstream: prevent responsibility shifting from model providers to fine-tuners and deployers, maintain and strengthen Article 53 transparency (e.g., training data summaries, provenance/watermarking), and supply standardized disclosure templates. Codes of Practice should clarify roles rather than conflate them, and obligations like watermarking are best placed on model providers to protect downstream deployers. Proposals include tighter GPAI transparency and evaluation regimes, limited open-source exemptions, and no delays or dilution in enforcement; there is concern that current rules risk incentivizing downstream policing instead of upstream accountability. On IP rights, publishers and rightsholders demand stronger implementation of AI Act protections, opposing any simplification or dilution of Article 53 and calling the existing instruments a missed opportunity. They seek a balanced settlement that safeguards creators without unduly hindering innovation. The debate is polarized: some industry advocates promote a technology-neutral, use-case focus and even removing GPAIM-specific rules, while others insist on safeguarding and enhancing GPAI-specific transparency and IP protections to align with the Act's objectives.

> *The GPAI Code of Practice needs to become more user oriented by revising the thresholds for systemic risk and avoid an inappropriate shifting of responsibilities from model providers to finetuners and users of these models.* (Volkswagen Group)
>
> *On the contrary, as the Commission seeks to achieve optimal implementation of the AI Act, the simplification process presents an opportunity to revisit and greatly improve the AI Act implementation package adopted in July this year, comprising the General-Purpose AI (GPAI) Code of Practice, the Al Office's transparency template for GPAI model providers to summarise the training content, and the GPAI guidelines, which were a missed opportunity to provide meaningful protection of intellectual property rights in the context of generative AI and fell short of the EU Al Act's own objectives.* (EMMA-ENPA)
>
> *In particular, the GPAIM focused rules of the AIA should be removed - especially those outlined in Chapter V - to make this a reality.* (Meta Platforms Ireland Limited)
>
> *The AI Act does not specify what these risks may be.* (Centre for Democracy and Technology Europe)

: Highlights diverse risks from general-purpose AI, reinforcing the need for governance, transparency, privacy, and IP safeguards across the lifecycle.

> *General purpose" AI systems are dangerous in many ways (e.g. discrimination, bias, environmental impact, cognitive debt, critical thinking abilities decline, data privacy breaches, copyright infringements).*

Volkswagen Group: Urges a user-oriented GPAI Code of Practice with calibrated systemic risk thresholds that prevent shifting responsibilities from model providers to finetuners and users.

> *The GPAI Code of Practice needs to become more user oriented by revising the thresholds for systemic risk and avoid an inappropriate shifting of responsibilities from model providers to finetuners and users of these models.*

EMMA-ENPA: Calls to revisit GPAI implementation tools to provide meaningful protection of IP rights, strengthening transparency templates and guidelines under the AI Act.

On the contrary, as the Commission seeks to achieve optimal implementation of the AI Act, the simplification process presents an opportunity to revisit and greatly improve the AI Act implementation package adopted in July this year, comprising the General-Purpose AI (GPAI) Code of Practice, the Al Office's transparency template for GPAI model providers to summarise the training content, and the GPAI guidelines, which were a missed opportunity to provide meaningful protection of intellectual property rights in the context of generative AI and fell short of the EU Al Act's own objectives.

Seznam.cz, a.s.: Opposes any simplification of AI Act Article 53 copyright duties for GPAI and seeks clearer, expanded obligations that balance creators' interests with AI development.

As representatives of online content creators of text, audio, and video, we wish to voice our opposition to any simplification of the already vague copyright protections in Art. 53 of the AI Act.

Centre for Democracy and Technology Europe: Notes that residual systemic risks under the AI Act are undefined and calls for clearer risk categories and safeguards for GPAI governance.

The AI Act does not specify what these risks may be.

Meta Platforms Ireland Limited: Advocates a technology-neutral, use-case-focused approach and proposes removing GPAIM-specific rules, warning that fragmented enforcement hampers innovation.

In particular, the GPAIM focused rules of the AIA should be removed - especially those outlined in Chapter V - to make this a reality.

: Supports stronger GPAI transparency, reporting, and independent evaluations to manage upstream risks and improve accountability.

Pour Demain Europe: Argues the Omnibus should not alter GPAI provisions and emphasizes robust upstream obligations to protect downstream deployers.

Ministry of Industry and Trade of the Czech Republic - this entry represents the official position of the Czech Republic for the section "Targeted adjustments to the Artificial Intelligence Act to ensure the optimal application of the rules: Supports limited exemptions for open-source GPAI models while maintaining core upstream duties and safeguards.

Polish Confederation Lewiatan: Criticizes ambiguous compute-based thresholds for defining GPAI models and urges clearer, risk- and capability-based criteria.

International Federation of Reproduction Rights Organisations (IFRRO): Calls to strengthen GPAI implementation instruments—Code of Practice, transparency templates, and guidelines—to better protect IP and ensure compliance.

ITI - Information Technology Industry Council: Recommends a standardized model disclosure template to improve GPAI transparency and facilitate consistent compliance.

AI Standards Lab: Warns that compute-only thresholds and unclear provider responsibilities can misallocate obligations, urging alignment with Article 53 to avoid shifting policing downstream.

European Broadcasting Union: Urges maintaining and enforcing Article 53 transparency duties for GPAI to safeguard media interests and IP rights.

Sdružení pro internetový rozvoj (SPIR): Opposes any easing of AI Act copyright rules affecting GPAI and supports strong upstream transparency and IP protections.

Google: Proposes a capabilities-based process to identify high-impact GPAI models rather than relying solely on compute thresholds.

MVFP Medienverband der freien Presse e.V.: Rejects dilution of GPAI rules and argues current measures insufficiently protect IP, calling for stronger upstream safeguards.

AFME: Suggests assigning watermarking and provenance obligations to upstream model providers to ensure consistent safeguards across the ecosystem.

German Newspaper Publishers and Digitalpublishers Association (BDZV): Opposes dilution of GPAI provisions and seeks improved implementation to uphold IP rights and transparency obligations.

Seznam.cz, a.s.: Opposes easing AI Act copyright-related duties for GPAI and supports maintaining or strengthening Article 53 obligations.

CEN and CENELEC: Warns that GPAI Codes of Practice may conflate roles across the value chain, urging clarity to prevent improper burden shifting.

Middle Tech Europe: Calls to safeguard and strengthen the GPAI Code of Practice as a key governance tool for transparency and risk mitigation.

DIGITALEUROPE: Argues compute-only GPAI thresholds are insufficient and supports multi-factor, risk- and capability-based triggers for upstream duties.

Verband Österreichischer Zeitungen (VÖZ): Advocates robust IP protections in GPAI governance, including transparent disclosure of training content and respect for rights holders.

SaferAI: Opposes delaying GPAI requirements and urges timely rollout of upstream safeguards for high-risk capabilities.

2.8.10 Miscellaneous

This category captures miscellaneous viewpoints under AI governance, transparency, and high-risk safeguards that urge the EU to prioritize societal benefit over profit-driven models. Contributors advocate purpose-specific, high-value AI systems with tangible goals, aligning oversight with transparency and safeguards proportionate to risk. Consumer and professional bodies express trust in the European Commission to deliver the AI Act and broadly support EU leadership in AI regulation, reflecting consensus around responsible innovation, auditability, and consumer protection. Industry feedback notes that the AI Act is not the main barrier to AI deployment, suggesting that effective governance should remain targeted and enable innovation while addressing genuinely high-risk applications.

Therefore, the EU should NOT follow their path, but focus on creating high-value, purpose-specific AI systems that have tangible and specific impact and goals. ()

We remain at your disposal for a meeting and trust the Commission to deliver on the promise of the AI Act. (BEUC - The European Consumer Organisation)

The Big Tech companies in the US are evidently focusing on profit rather than on benefit. ()

: Urges the EU to reject the profit-first US Big Tech model and instead build purpose-specific, high-value AI with tangible societal impact, aligning governance with public benefit over scale.

Therefore, the EU should NOT follow their path, but focus on creating high-value, purpose-specific AI systems that have tangible and specific impact and goals.

BEUC - The European Consumer Organisation: Conveys confidence in the European Commission's implementation of the AI Act and readiness to engage, reinforcing support for strong governance and consumer protection.

We remain at your disposal for a meeting and trust the Commission to deliver on the promise of the AI Act.

Compagnie Nationale des Commissaires aux Comptes (professional organisation for statutory auditors): Affirms support for the AI Act and highlights EU leadership in AI regulation, signaling commitment to robust oversight and safeguards for high-risk systems.

kaiko.ai: Supports EU leadership in AI regulation, aligning with transparent governance and stringent standards for high-risk AI.

DIGITALEUROPE: Contends the AI Act is not the principal barrier to AI progress, implying other challenges dominate and advocating balanced governance to avoid unnecessary regulatory friction.

2.9 Sectoral Safety, Accessibility and Public Interest

The most compelling insight is that safeguarding the public requires sector-specific, risk-proportionate governance that elevates safety, accessibility, and sustainability alongside innovation, anchored in enforceable standards and continuous oversight. In health and workplaces, this means robust, fail-safe AI and devices with human oversight across the lifecycle, leveraging MDR and OSH frameworks while anticipating novel AI risks; protecting clinical context and preventing misuse of raw telemetry or e-prescription data; and balancing new AI rules with supply continuity and resilient care. Accessibility must be mandatory across products, services, and AI, mainstreamed through universal design, rigorous testing and enforcement, and continuous participation of persons with disabilities; retain platform and consumer safeguards, address social media harms (including child safety), ensure non-digital options, and invest in inclusive infrastructure and literacy backed by targeted finance. Environmental safety calls for aligning digital policy with the Green Deal via energy efficiency, life-cycle accountability, sustainable procurement, material traceability, and strong chemicals oversight, avoiding omnibus rollbacks and recognizing digital rights' biodiversity impacts. Critical infrastructure needs sustained, transparent, multi-level collaboration and investment, with tailored cybersecurity/OT rules and modernized, risk-calibrated licensing that protect public goods. Across domains, the throughlines are safety-by-design, enforceability, stakeholder inclusion, and data/context integrity. Co-designed, interoperable governance integrates social, environmental, and economic goals to deliver resilient, inclusive outcomes.

2.9.1 Critical Infrastructure and Public Interest Governance

This category integrates guidance for governing critical infrastructure and essential services with a public-interest lens. It emphasizes risk-proportionate, sector-aware regulation paired with sustained investment in secure, resilient digital infrastructure (e.g., broadband, 5G, AI). A recurring theme is the need for multi-level, public-private collaboration that recognizes the frontline role of local and regional governments, involves social security institutions, and protects public goods such as education, pensions, and cultural heritage. Regulatory simplification is welcomed only when it explicitly safeguards public values and policy objectives, with transparency and accountability serving as core governance principles. Operationally, the insights call for tailored cybersecurity and operational-technology rules (notably in rail and industrial control), stronger digital governance in regulated sectors (e.g., gas), and modernized licensing and safety regimes (e.g., digital firearms licensing, Vision Zero technologies). They also advocate calibrating compliance to real-world risk—avoiding undue burdens where systemic risks are minimal—while ensuring public-interest protections are not diluted. Together, these points outline a governance approach that is collaborative, sector-specific, locally informed, and anchored in public value, accessibility, and safety.

> *Achieving the Union's ambitious digital and economic objectives requires harnessing the complementary strengths of both sectors - the public sector's regulatory authority and commitment to the public interest, and the private sector's agility, innovation, and operational excellence.* (FEBIS)
>
> *Effective collaboration between these actors ensures that digital infrastructures such as EBW are not only secure and compliant, but also efficient, user-friendly, and responsive to market realities.* (FEBIS)
>
> *Additionally, it is critical to exempt intra-group financial services (e.g., treasury services for subsidiaries of a non-financial group) from the regulatory framework.* (Adigital (Asociación Española de la Economía Digital))
>
> *These services are currently subject to much of the regulatory burden-such as under the DORA Regulation-without being justified by any significant risk to the financial system.* (Adigital (Asociación Española de la Economía Digital))

FEBIS: Advocates strong public-private cooperation so critical digital infrastructures are both compliant and high-performing, aligning regulatory authority with private-sector agility to meet EU objectives.

> *Effective collaboration between these actors ensures that digital infrastructures such as EBW are not only secure and compliant, but also efficient, user-friendly, and responsive to market realities.*

Adigital (Asociación Española de la Economía Digital): Urges exempting low-risk intra-group financial services from broad frameworks like DORA to align oversight with actual systemic risk and reduce unnecessary compliance burden.

This represents an unnecessary compliance burden disconnected from real operational risk.

WKÖ - Austrian Federal Economic Chamber: Calls for increased investment in core digital infrastructure (5G, broadband, IPCEI AI) to keep Europe competitive and resilient.

We are therefore calling for more investment in digital infrastructure: from 5G and broadband expansion to further ambitious and accompanying measures such as an IPCEI AI, so that Europe can keep pace with digital competition.

ENSHPO - The European Network of Safety and Health Professional Organizations: Promotes accelerated adoption of Vision Zero-aligned safety technologies to reduce workplace harm across sectors.

DigitalTrade4.EU: Supports modernized digital regulation for the gas sector and the rollout of digital firearms licensing to strengthen safety, traceability, and oversight in sensitive domains.

European Public Service Union: Stresses that governance should prioritize the public interest and public good, reinforcing strong, accessible public services and protections.

Mafex – Spanish Railway Association: Argues for rail-specific cybersecurity and operational technology rules to safeguard railway systems as critical infrastructure.

REIF: Calls for the meaningful involvement of social security institutions in policy and governance processes affecting digital and sectoral systems to protect social welfare.

Association of Finnish Cities and Municipalities: Urges systematic assessment of local and municipal impacts when designing regulation, recognizing cities' central role in essential services and infrastructure.

Comitato Elettrotecnico Italiano - CEI: Advocates a tailored approach to regulating operational technology, avoiding one-size-fits-all rules to reflect sector-specific risks and needs.

EU DisinfoLab: Warns that current approaches risk overlooking key public policy objectives, such as countering disinformation, needed to protect the public interest.

Movement for an Open Web: Pushes for greater transparency and accountability in EU bank resolution and related processes to safeguard financial stability and the public interest.

Chair in Cyber Policy, University of Luxembourg: Emphasizes that regulatory simplification must explicitly protect public values like security, accountability, and democratic resilience, not just reduce burdens.

European Trade Union Committee for Education (ETUCE): Maintains that regulation is necessary to shield public education from profiteering, ensuring equitable access and quality.

PensionsEurope: Supports a pro-regulatory framework that encourages workplace pension membership and strengthens long-term governance for savers.

A regulatory environment encouraging workplace pension membership.

Culture Action Europe: Highlights digitized cultural heritage as enabling innovation, access, and societal value, positioning it as a public-interest digital asset.

Council of European Municipalities and Regions (CEMR): Seeks recognition and inclusion of local and regional governments as frontline actors in governing and delivering critical services and digital infrastructure.

2.9.2 Environmental Sustainability and Safety

This category synthesizes how environmental sustainability and safety are embedded across digital and sectoral policies. Core knowledge emphasizes aligning digital innovation with the European Green Deal through

mandated energy efficiency, sustainable procurement, and full life-cycle accountability for digital products and services. Regulatory incentives and funding are positioned to accelerate green tech uptake and climate-neutral digital infrastructures, framing decarbonization as both a policy imperative and a competitive opportunity. Complementary safeguards span multiple domains: better digital battery and recycled-material reporting to improve traceability and circularity; stronger oversight of hazardous chemicals; and reinforcement of plant health frameworks to protect ecosystems. Safety concerns extend to technical practices (e.g., restricting unsafe BMS resets), while civil society flags risks when omnibus reforms weaken environmental safeguards. Finally, the governance of digital rights is recognized as shaping biodiversity outcomes, underscoring that environmental protection, safety, and digital policy are interdependent and must be co-designed for public interest outcomes.

> *Di- gital innovation must align with the European Green Deal.* ()
>
> *Therefore, policymakers must mandate energy efficiency, sustainable procurement, and life-cycle accountability for digital products and services.* ()
>
> *We recall that the first omnibus proposal was already widely criticised5 for targeting environmental safeguards.* (BEUC - The European Consumer Organisation)
>
> **:** Calls for aligning digital innovation with the European Green Deal by mandating energy efficiency, sustainable procurement, and life-cycle accountability, supported by incentives and funding for climate-neutral infrastructure. Positions this as essential for climate goals and a business opportunity for EU companies.
>
> *Therefore, policymakers must mandate energy efficiency, sustainable procurement, and life-cycle accountability for digital products and services.*
>
> **BEUC - The European Consumer Organisation:** Warns that the first omnibus proposal undermined environmental protections, raising public-interest concerns. Urges safeguarding environmental standards rather than weakening them.
>
> *We recall that the first omnibus proposal was already widely criticised5 for targeting environmental safeguards.*
>
> **DigitalTrade4.EU:** Supports stronger sustainability and safety measures, including enhanced digital reporting for batteries and recycled content, reinforced plant health protections, and tighter oversight of hazardous chemicals. Emphasizes transparency and risk control to protect ecosystems and public health.
>
> **Japan Business Council in Europe (JBCE):** Flags safety risks from allowing unrestricted battery management system resets, indicating the need for controls to prevent hazardous operation. Advocates precautionary measures to uphold product safety.
>
> **Palombar - Associação de Conservação da Natureza e do Património Rural:** Connects digital rights and governance to biodiversity outcomes, urging environmental impacts be integrated into digital policy. Argues that data and access rules can affect habitat protection and rural heritage.

2.9.3 Healthcare and Occupational Safety Governance

Healthcare and Occupational Safety Governance centers on safety-first deployment of AI and digital systems in clinical and workplace settings. Core knowledge stresses robustness and reliability in hazard detection, automatic transition to safe states, and sustained human oversight throughout the device lifecycle. Existing medical-device frameworks (MDR) are favored for their clinical evaluation, post-market surveillance, and vigilance, while OSH perspectives highlight that AI introduces novel risks, that traditional foreseeability standards can misfit rapidly evolving AI, and that safety must take precedence over reducing administrative burden. Data and context governance are critical: removing safeguards around access to raw implant telemetry invites misinterpretation and patient harm; sector stakeholders warn the Data Act could erode clinical context; and access to e-prescriptions must not be construed as authorization for cross-border shipment of prescription medicines. Building public trust requires clear safety understanding and sector-specific guidance, with civil-society voices emphasizing people and safety over profit and criticizing reactive, inadequate safety responses—arguing for proactive, systemic protections. Finally, governance must balance innovation with supply continuity. There is concern that new AI rules could disrupt availability of long-proven medical devices and disproportionately affect devices with strong real-world performance. Industry backs updated machinery safety requirements and calls to prioritize MDR application, while health-system pressures—from backlogs to supply-

chain risks—underscore the need to align digital regulation with medicines strategy (e.g., leveraging EUTIR) and ensure resilient, safe care.

> *To ensure safety in this scenario, these AI Systems are subject to the Machinery Regulation and in this respect need to fulfil high reliability and robustness standards when detecting objects in critical areas (avoid false positive or false negative classifications).* (SIEMENS AG)
>
> *requesting raw telemetry from an implant could receive data that, without MDR or EHDS safeguards, is easily misread and poses patient-safety risks.* (Zimmer Biomet)
>
> *There's a significant risk that the availability of certain medical devices - many of which have been safely used for years, if not decades - could be disrupted after August 2, 2027.* (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)
>
> *Devices with a strong track record of safety and effectiveness, backed by extensive real-world data and post-market performance, may be disproportionately affected by the Al Act's requirements.* (COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry)

SIEMENS AG: Stresses that AI-driven machinery must meet Machinery Regulation robustness and reliability to avoid misclassification and automatically enter safe states that protect nearby people.

> *To ensure safety in this scenario, these AI Systems are subject to the Machinery Regulation and in this respect need to fulfil high reliability and robustness standards when detecting objects in critical areas (avoid false positive or false negative classifications).*

Zimmer Biomet: Warns that bypassing MDR/EHDS safeguards when accessing implant telemetry can lead to misinterpretation and patient-safety risks.

> *requesting raw telemetry from an implant could receive data that, without MDR or EHDS safeguards, is easily misread and poses patient-safety risks.*

PHOENIX group: Supports digital access to prescriptions but insists governance must prevent it being used to justify cross-border shipment of prescription medicines.

> *However, with an important safeguard: access to e-prescriptions or patient records must not be interpreted as authorization to ship Rx medicines across borders.*

COCIR - European Coordination Committee of the Radiological, Electromedical and healthcare IT Industry: Raises concern that AI Act requirements could disrupt long-standing, safe medical devices after 2027, threatening continuity of care despite proven safety records.

> *There's a significant risk that the availability of certain medical devices - many of which have been safely used for years, if not decades - could be disrupted after August 2, 2027.*

: Argues MDR already provides active human oversight and continuous surveillance in healthcare, and should be the primary regulatory framework.

> *Therefore, MDR regulation should be primarily applied.*

ENSHPO - The European Network of Safety and Health Professional Organizations: Highlights that AI brings new occupational safety and health risks, that foreseeability standards fit poorly for OSH AI, and that safety should trump administrative burden reduction.

: Emphasizes that public trust in health AI depends on clear understanding and assurance of safety.

DigitalTrade4.EU: Recommends leveraging EUTIR within the EU drugs strategy to align innovation with safety and effective governance of medicines data.

MedTech Europe: Cautions that Data Act–driven data access could strip clinical context, undermining patient safety and responsible use of health data.

Confindustria: Supports updated machinery requirements to ensure safer, more reliable AI-enabled equipment in workplaces.

The Center for Countering Digital Hate: Urges governance that prioritizes people and safety over profit and criticizes reactive, after-the-fact safety approaches as inadequate.

Siemens Healthineers AG: Warns that regulatory backlogs pose risks to healthcare supply and patient access, underscoring the need for predictable safety governance.

BioMed Alliance: Calls for sector-specific guidance for health AI with tailored mitigations addressing clinical risks and implementation challenges.

2.9.4 Digital Inclusion, Platforms and Consumer Protection

This category centers on making digital environments inclusive by treating accessibility as a mandatory, enforceable requirement across products, services, and AI systems. Streamlining the digital acquis must mainstream universal design, strengthen technical standards and codes of conduct, and be matched by robust testing, quality control, and enforcement. Participation by persons with disabilities and civil society throughout the regulatory cycle is emphasized to ensure legitimacy and relevance. Platforms and consumer protection feature prominently: maintaining DSA safeguards against illicit and counterfeit goods, regulating social media due to evidence of significant online harms and child-safety failures, and prioritizing safety over data sharing. Stakeholders call for differentiating B2B and consumer risks, preserving clear information duties while simplifying rules, offering non-digital service options, and investing in inclusive infrastructure and digital literacy to close the digital divide. To sustain inclusion, technologies should be harnessed for public-interest goals (e.g., SDGs), backed by supervised, enforceable financing, and earmarked public funding that catalyzes accessible innovation. Capacity-building includes embedding accessibility and inclusive design in university curricula, developing metrics for disability representation in innovation, and monitoring progress. The shared ethos reframes accessibility as a fundamental right and a driver of innovation, asserting that voluntary measures alone are insufficient without coherent law, standards, and accountability.

As more aspects of life move online, it is essential that all digital products and services meet minimum accessibility requirements. (European Disability Forum)

Simplification must integrate and strengthen universal accessibility requirements and design for all at the core of all digital legislation. (CERMI)

Article 16 of the AI Act explicitly references the Web Accessibility Directive and the European Accessibility Act, establishing accessibility obligations for high-risk AI systems. (European Disability Forum)

To improve the participation of people with disability in the innovation process, they suggest the creation of metrics on disability representation. (European Disability Forum)

European Disability Forum: Calls to maintain and strengthen mandatory accessibility requirements across digital products and services, with robust standards, quality control, and enforcement. Advocates funding and education to harness technology for inclusion, including metrics on disability representation and accessibility in curricula and AI governance.

The disability community knows from experience that voluntary measures have proven insufficient; mandatory and coherent legal requirements, underpinned by technical standards are necessary.

EFPIA: Urges online platforms to uphold DSA safeguards to protect consumers by preventing illicit and counterfeit medicines. Emphasizes strong procedures and technical standards for platform compliance.

Regarding the DSA, online platforms should maintain strong procedures and technical standards to prevent the sale of illicit and counterfeit medicines.

CERMI: Insists universal accessibility and design-for-all be core, strengthened requirements across digital legislation to ensure equal rights for persons with disabilities. Calls for formal mechanisms to involve persons with disabilities and their organizations throughout digital governance.

Simplification must integrate and strengthen universal accessibility requirements and design for all at the core of all digital legislation.

European Travel Retail Confederation (ETRC): Warns that mandatory on-pack labels can reduce consumer choice and may have unintended consumer protection impacts. Suggests more proportionate approaches to inform consumers without restricting access.

DigitalTrade4.EU: Advocates supervised, regulated, and enforceable access to financing to foster inclusive digital participation. Emphasizes consumer and SME protection through accountable financial mechanisms.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Critiques current accessibility responsibilities for digital systems and calls for stronger duties and testing to ensure inclusion. Urges more rigorous evaluation to prevent exclusion by digital platforms and AI.

Ecommerce Europe: Highlights the digital divide as a driver of exclusion, urging policies that ensure accessible digital services and support for vulnerable users. Stresses consumer protection measures that do not leave non-digital or less-skilled users behind.

: Advocates maintaining non-digital service channels to ensure no one is excluded from essential services. Emphasizes inclusive design that accommodates users who lack digital access or skills.

DOT Europe: Seeks deletion of the EECC contract summary requirement to reduce burdens on providers, arguing it does not improve consumer outcomes. Calls for streamlined rules that protect consumers without unnecessary administrative demands.

CECIMO - European Association of Manufacturing Technologies: Argues that B2B digital product risks differ from consumer contexts and should be regulated accordingly. Supports tailored safety and liability rules that maintain accessibility without overextending consumer-style obligations to industry.

The Center for Countering Digital Hate: Documents social media platforms' failures to protect children and other users from significant online harms. Calls for stronger regulation and platform accountability to safeguard consumers.

Orgalim - Europe's Technology Industries: Prioritizes product safety over expansive data-sharing mandates to protect users and innovation. Proposes limiting mandatory support periods to digital elements to balance consumer protection with feasibility.

Insurance Europe: Addresses suitability and conduct rules under the IDD, including the use of AI in advice, to ensure fair treatment and consumer protection. Supports clear standards for transparency, suitability, and oversight of digital sales and advice.

AMETIC: Identifies barriers that risk exclusion and calls for inclusive implementation of digital policies. Emphasizes removing obstacles and designing services that are accessible to all users.

Council of European Municipalities and Regions (CEMR): Promotes inclusive digital infrastructure and literacy initiatives so all residents can access online public services. Encourages local investments that bridge gaps in connectivity and skills for consumer protection and inclusion.

2.10 Fair Competition, Gatekeepers and Media Sustainability

Sustaining fair competition and media pluralism hinges on consistent, well-resourced enforcement of EU cornerstones (DMA, DSA, Data Act, AI Act) that curb gatekeepers' data-driven advantages while hardwiring interoperability and device neutrality. Dominant platforms exploit walled gardens and centralized consent; stakeholders seek symmetric obligations, broader analysis across privacy/security/labour/IP, tailored rules for Big Tech's cross-sector expansion, and firm remedies against repeat noncompliance. Fair, reciprocal data access must be preserved, with sector fixes in mobility (OEM data control) and finance, calibrated PIMS duties, protection of trade secrets, and practical governance (switching, reporting) that empowers SMEs and municipalities. Media viability depends on data-enabled, privacy-respecting advertising alongside subscriptions, with interoperable, timely measurement, standardized platform metrics, and support for IP and cultural funding. Communications markets need targeted ex-ante rules, net neutrality, fair HMI access, and strengthened cloud switching. Standards should embed PETs, FRAND SEP access, and APIs; procurement and vouchers help exit lock-in, backed by expanded conformity assessment and strategic de-risking without decoupling. Platform

transparency, oversight data, and proportionate anti-virality tools should avoid antitrust conflicts. AI governance should bolster open-source, fair creator terms, and monitor concentration beyond high-risk systems. The common threads are disciplining gatekeeper leverage through interoperability and data access, and making enforcement capable and proportionate. The strategic arc is sovereignty via openness: practical rules that preserve competition and a plural, sustainable media ecosystem.

2.10.1 Gatekeepers & Market Contestability

Gatekeepers & Market Contestability captures concerns that dominant platforms exploit walled gardens, centralized consent mechanisms, and vertical integration to entrench their positions, squeezing smaller publishers and service providers. Stakeholders call for a functional, consistent application of the Digital Markets Act across comparable services to preserve contestability, backed by symmetric, reciprocal obligations that prevent uneven compliance costs and regulatory arbitrage. They urge competition authorities to widen their analytical lens (e.g., security, privacy, labour, IP, industrial strategy) and invest in enforcement capacity. Cross-sector expansion of Big Tech—especially into financial and insurance services—raises risks from data advantages, concentration, and financial stability linkages that existing sectoral rules may not address, warranting tailored, possibly Big Tech–specific regulation. Some advocate firm remedies against noncompliant international actors, including bans to restore a fair marketplace, with the expectation that this would open currently monopolised niches to new local entrants.

> *Ensure a level playing field between gatekeeper platforms and other Search and Information Providers (SIPs), including clear scope and consistent application of the Digital Markets Act (DMA) where rules are necessary to preserve contestability.* (Siinda)
>
> *This fragmentation can advantage vertically integrated gatekeepers or create regulatory arbitrage.* (Siinda)
>
> *Such players would be banned, and that is what has to happen to regain a fair marketplace.* ()
>
> *The EU already has high levels of start-ups and similar levels of market entry as the US, however:* (AI & Partners B.V.)
>
> **:** Advocates broadening competition policy to adjacent domains and ramping up enforcement, including new tools like the Digital Markets Act, to secure fair, contestable markets. Stresses the need for significant resourcing to make this effective.
>
> *This new EU competition policy, including the enforcement of new laws such as the Foreign Subsi- dies Regulation and the Digital Markets Act, will require significantly increased hiring efforts.*
>
> **EMMA-ENPA:** Warns that centralised consent mechanisms entrench gatekeeper platforms, deepen data dominance, and distort advertising competition, while blocking publishers' direct consent relationships. Calls out the risk of creating new consent gatekeepers.
>
> *As mentioned above, we also believe that centralised consent would only further reinforce existing gatekeepers, consolidate their data hegemony and further distort competition in the advertising market in their favour - or establish the providers of centralised consent solutions as new gatekeepers.*
>
> **Unipol Assicurazioni S.p.A.:** Highlights risks that Big Tech's entry into finance could entrench data oligopolies and concentration, disadvantaging incumbents and undermining market contestability. Argues for a Big Tech-specific regulatory approach to address gaps and stability risks.
>
> *While we believe that competition promotes innovation and consumer welfare, we cannot ignore the potential risks associated with Big Tech firms utilising FISP authorisation to strengthen and enlarge their data oligopolies.*
>
> **Siinda:** Calls for a functional, consistent DMA application across similar services to preserve contestability and prevent arbitrage by vertically integrated gatekeepers. Urges symmetric obligations so rules do not entrench dominance through regulatory asymmetries.
>
> *Ensure a level playing field between gatekeeper platforms and other Search and Information Providers (SIPs), including clear scope and consistent application of the Digital Markets Act (DMA) where rules are necessary to preserve contestability.*

egta - the international trade body of multiplatform TV and audio businesses: Opposes browser-level consent that would hand control to gatekeepers, increase intermediation risks, and strip smaller players of service control. Urges the Commission to discourage centralised consent.

Introducing browser-level consent mechanisms would put control entirely in the hands of gatekeepers, leading to significant intermediation risks and depriving smaller players of any control over their services.

AI & Partners B.V.: Notes EU market entry is already high and that antitrust action against tech persists across political lines, suggesting ongoing scrutiny of gatekeeper power. Implies contestability concerns are recognized and acted upon.

The EU already has high levels of start-ups and similar levels of market entry as the US, however:

: Advocates banning noncompliant international players to restore a fair marketplace and enable local entrants to contest monopolised niches. Emphasizes that fair rules are a prerequisite for European firms to compete.

Such players would be banned, and that is what has to happen to regain a fair marketplace.

Digital Business Ireland: Calls for tailored DMA obligations and clear guidance to maintain contestability while reflecting sectoral realities. Seeks balanced rules that curb gatekeeper power without unintended burdens.

DigitalTrade4.EU: Urges modernized merger control to tackle consolidation by powerful digital players and keep markets open to challengers. Sees updated tools as key to preventing entrenchment.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Characterizes the Act as aspirational in promoting fairness and contestability, signaling intent to curb gatekeeper power. Suggests further concrete measures may be needed to realize these goals.

VDMA - Advancing Europe´s machinery industry: Warns that vague unfairness clauses and flexible rules can distort competition, creating contractual uncertainty and disadvantaging firms versus larger platforms. Calls for clarity to avoid entrenching dominant players.

European Public Service Union: Denounces deregulation framed as competitiveness, arguing it benefits dominant firms and undermines fair competition. Supports stronger safeguards to preserve contestability.

Federation of German Consumer Organisations (vzbv): Cautions that weakening protections and conflicting rules risks reinforcing dominant platforms and harming contestability. Points to structural deficits that impede competitiveness and fair markets.

Association des Constructeurs Européens de Motocycles: Criticizes mandates for single-platform reliance and rules modeled on large providers, which reduce choice and entrench gatekeepers. Calls for diversified access to sustain contestability.

ICMP - International Confederation of Music Publishers: Calls for strong enforcement targeting the largest global operators to curb abuses and protect fair access. Emphasizes leveling the playing field for smaller competitors.

Fastweb S.p.A.: Stresses that enforcement must avoid creating competitive disadvantages and should preserve a level playing field. Seeks balanced measures that do not favor gatekeepers.

SGI Europe: Highlights asymmetries and lock-in effects from Big Tech that constrain user choice and weaken contestability. Supports measures to counteract dependency on dominant platforms.

: Flags risks from consolidation and centralization that concentrate control with gatekeepers and erode market openness. Advocates vigilance against power aggregation.

ESYS Foundation: Notes high costs of concentration assessments for firms, which can deter challenges to dominant players. Warns this burden can hinder effective contestability oversight.

Cigref: Backs robust, enforceable rules to tackle unfair practices by dominant platforms and keep markets open. Argues strong governance is needed to preserve contestability.

CIO Platform Nederland: Argues persistent market issues necessitate regulation to limit gatekeeper power and protect contestability. Sees intervention as essential for fair competition.

noyb: Warns that deregulation mainly enriches Big Tech, worsening dominance and shrinking contestability. Supports maintaining strong protections against platform abuses.

European DIGITAL SME Alliance: Calls to preserve essential rules that safeguard SMEs from gatekeeper conduct and keep markets contestable. Emphasizes preventing abuse of bottleneck positions.

Verband Österreichischer Zeitungen (VÖZ): Urges clear differentiation between gatekeepers and media publishers so interventions target true bottlenecks without harming media sustainability. Seeks proportionate, competition-friendly rules.

Dutch Startup Association: Emphasizes guarding start-ups against platform gatekeeper control to sustain entry and innovation. Supports measures that secure fair access and competitive neutrality.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Observes procedural gaps in competition law that delay action against gatekeeper strategies, undermining contestability. Calls for improved processes to address digital market dynamics.

The Finnish Media Federation, Finnmedia: Calls for vigilance against gatekeeper dominance to protect media sustainability and maintain competitive conditions. Advocates policies that prevent bottleneck control over distribution and data.

2.10.2 Open Internet, Device Neutrality & Network Competition

This category centers on protecting an open internet and competitive communications markets by resisting premature deregulation and maintaining targeted ex-ante rules where significant market power persists. Stakeholders argue that moving away from ex-ante regulation (e.g., relying solely on the three-criteria test) is inadequate, as it risks entrenching incumbent advantages, overbuild strategies, and undermining consumer welfare. They call for clear, predictable obligations—rather than voluntary frameworks—and for ensuring telecoms are fully included in horizontal digital competition initiatives, warning that proposals like a Digital Networks Act must not dilute net neutrality or the level playing field. Device neutrality and fair access to user interfaces are likewise emphasized. Independent service providers seek non-discriminatory, standardized access to in-vehicle data, functions, resources, and human–machine interfaces (such as dashboards) to compete on merit—echoing broader concerns over OS- or browser-led centralization and the need for explicit safeguards. Interoperability and switching (e.g., cloud switching) should be preserved and strengthened to avoid lock-in, while narrowly tailored exemptions for security- and critical-infrastructure data remain necessary.

Only ex-ante regulation can break up market power and protect competition - especially in the interest of consumers. (Verband kommunaler Unternehmen e.V.)

However, for innovative & interactive automotive data-driven services, more is needed such as non-discriminatory access (compared to the vehicle manufacturer) to functions & resources, to the vehicle dashboard as the new communication interface with the consumer, or a mandatory standardized list of data for scalable services. (FIGIEFA aisbl)

Data from critical infrastructure and security-related sectors requires particularly high levels of protection and must not be shared under any circumstances. (Verband kommunaler Unternehmen e.V.)

Local public utilities continue to be confronted with the threat of overbuilding of their fibre networks by the company with significant market power. (Verband kommunaler Unternehmen e.V.)

Verband kommunaler Unternehmen e.V.: Opposes telecom deregulation and supports maintaining ex-ante regulation to curb dominant market power and ensure fair competition in fibre networks.

Criticizes reliance on the three-criteria test and calls for clear rules and data/cloud switching protections to avoid legal uncertainty.

Only ex-ante regulation can break up market power and protect competition - especially in the interest of consumers.

FIGIEFA aisbl: Calls for non-discriminatory, standardized access to in-vehicle data, functions, resources and the dashboard to enable competitive, data-driven aftermarket services. Emphasizes parity with vehicle manufacturers to ensure fair competition.

However, for innovative & interactive automotive data-driven services, more is needed such as non-discriminatory access (compared to the vehicle manufacturer) to functions & resources, to the vehicle dashboard as the new communication interface with the consumer, or a mandatory standardized list of data for scalable services.

Vodafone Group: Urges inclusion of the telecom sector in digital reforms to prevent entrenched market imbalances. Warns that excluding telecoms would undermine efforts to level the playing field.

Excluding the sector would be a missed opportunity that risks entrenching issues in the digital economy, as opposed to levelling the playing field.

VDMA - Advancing Europe´s machinery industry: Warns that imposing resale obligations before 2025 could distort markets and harm fair competition. Calls for careful timing and design to avoid unintended consequences.

BusinessEurope: Raises concerns that banning geoblocking across cross-border interfaces could impose high compliance costs and complexity. Suggests targeted approaches to preserve competition without undue burdens.

Agilitation: Warns that browser-led control over web capabilities risks centralization that undermines the open internet and device neutrality. Advocates preserving user choice and competitive access to platform features.

European Digital Rights (EDRi): Flags risks that the proposed Digital Networks Act could weaken net neutrality protections and the open internet. Calls for safeguards to ensure non-discriminatory traffic management and user rights.

Middle Tech Europe: Opposes centralized browser controls that could restrict access to web APIs and steer users, threatening device neutrality and competition. Supports measures to limit gatekeeper power at the browser level.

DIGITALEUROPE: Seeks clear definitions of OS exemptions and safeguards for operating system integrations to protect device neutrality. Emphasizes preventing self-preferencing and ensuring equal access for third parties.

2.10.3 Standards, Interoperability & Digital Sovereignty

This category focuses on deploying EU-level standards and interoperability obligations to curb vendor lock-in, dilute gatekeeper power, and advance digital sovereignty while sustaining fair competition. Stakeholders stress embedding privacy-enhancing technologies (PETs) and other critical components within harmonized standards, ensuring a level playing field and FRAND access to SEPs. Interoperability is framed broadly—spanning data portability, APIs, fair access to repair/maintenance, and preserving technical neutrality in decentralized systems (e.g., preventing centralized control from undermining blockchain neutrality). To operationalize sovereignty without sliding into protectionism, proposals combine pro-competitive rules with practical incentives: public procurement preferences (a “Buy European Tech” clause) to catalyze domestic capability; Technology Change Vouchers to help public authorities exit legacy lock-in; and stronger protection of trade secrets and IP. A resilient conformity-assessment ecosystem is essential—expanding accredited capacity and publishing recognized labs to avoid bottlenecks where a few entities control market access, inflate costs, and dampen competition. Some contributions call for excluding dominant gatekeepers from sensitive roles and requiring EU establishment for providers of critical services. Internationally, contributors warn Europe is losing ground and advocate targeted, limited de-risking—leveraging trusted third countries to diversify supply chains—over broad decoupling. Policymakers should avoid unintended barriers (including for open-source) or measures that could

exclude foreign firms, while noting that pressure to relax rules often comes from non-EU multinationals seeking easier entry. The goal is strategic openness: safeguard resilience and sovereignty without sacrificing interoperability, innovation, and cross-border competition.

> *Their effective introduction requires the establishment of clear EU-level standards, ensuring interoperability and preventing the risk that a dominant player could control PETs and render the industry dependent on a single provider.* (European Tech Alliance)
>
> *Embedding PETs in this way would ensure that data use remains privacy-preserving, interoperable, and consistent with EU standards, while avoiding undue reliance on any single provider.* (European Tech Alliance)
>
> *This is likely to be one option pursued by the upcoming Cloud & AI Development Act, though whether it will have the effect of excluding foreign firms from (part of) certain markets remains to be seen.* (AI & Partners B.V.)
>
> *Calls for substantive relaxation often come from large multinational firms outside the EU seeking lighter rules for easier market entry.* (AI & Partners B.V.)

: Advocates a Buy European Tech procurement preference and Technology Change Vouchers to reduce lock-in, strengthen interoperability, and bolster EU digital sovereignty in public sector tech.

> *The introduction of ‚Technology Change Vouchers' for public authorities would help to overcome severe lock-in effects.*

European Tech Alliance: Calls for EU-level standards for PETs to secure interoperability, a level playing field, and to prevent dominance or lock-in by a single provider.

> *Their effective introduction requires the establishment of clear EU-level standards, ensuring interoperability and preventing the risk that a dominant player could control PETs and render the industry dependent on a single provider.*

Finnish Food and Drink Industries´ Federation (ETL): Urges stronger protection of trade secrets to retain data-driven expertise within European firms, reinforcing digital sovereignty and competitive capacity.

> *Protection of trade secrets and retention of data-driven expertise within European companies must be strengthened.*

Entrust SAS: Warns that limited accredited laboratories create bottlenecks and market concentration, urging the EU to expand capacity and list recognized labs to uphold fair, interoperable compliance.

> *Without such measures, the market risks becoming concentrated in the hands of a few testing entities, undermining the Commission's objectives of competition and fairness.*

AI & Partners B.V.: Recommends targeted de-risking and selective reliance on trusted third countries to diversify supply chains without protectionism, while cautioning against rule relaxations driven by non-EU multinationals.

> *Greater reliance on trusted third countries may help provide more diverse and resilient supply chains without the EU or its Member States resorting to subsidising European or national champions.*

European Banking Federation: Supports guaranteeing FRAND access to standard-essential patents to maintain interoperability and fair competition across EU markets.

ESYS Foundation: Notes that supplier concentration raises disruption risks, underscoring the need for diversified, interoperable supply chains to protect digital sovereignty.

Digital Currencies Governance Group (DCGG): Argues that centralized control in blockchain ecosystems undermines neutrality, advocating open, interoperable standards to avoid new gatekeepers.

Prosus Group: Highlights Europe’s declining tech competitiveness and the need for interoperable standards and sovereign capabilities to regain ground.

European Savings and Retail Banking Group: Proposes excluding gatekeepers from certain roles and requiring EU establishment for critical services to reinforce sovereignty and fair competition.

Free ICT Europe Foundation: Calls to curb OEM control and harmonize access to repair data and tools, fostering interoperability, competition, and user sovereignty over devices.

Mistral AI: Warns that the open-source exemption as framed could create new barriers and entrench incumbents, urging adjustments to keep ecosystems open and interoperable.

WindEurope: Stresses safeguarding trade secrets and IP in wind technologies to sustain competitive, sovereign innovation aligned with EU standards.

2.10.4 Data Fairness, Access & Privacy

The insights converge on making data access fair, reciprocal, and privacy-preserving to sustain competition and media markets. Stakeholders see the EU Data Act as a cornerstone that should not be weakened, while calling for targeted, sectoral fixes where asymmetries persist. In mobility, OEM control over what vehicle data is recorded, made retrievable, and priced creates barriers to independent services despite FRAND principles, prompting calls for vertical, binding rules and clear guidance on reasonable compensation. In finance, one-way access proposals for financial information service providers are flagged as unbalanced and likely to entrench gatekeepers rather than promote competition. Media and civil society voices warn that third-party data controllers convert their structural visibility across the web into market-killing advantages by reusing publisher audiences elsewhere, draining revenue from quality journalism and rewarding low-quality content and AI spam. Centralized consent models and stricter cookie regimes, if poorly designed, can entrench gatekeepers and harm SMEs. There is parallel concern that privacy-friendly services face economic disadvantages, while user choice and compensation rights over data use should be strengthened, and PIMS duties for gatekeepers calibrated with meaningful limits. On governance, contributors urge preserving the integrity of key frameworks via the Digital Omnibus while making them practical: streamline or remove blanket Data Act reporting and cost-disclosure obligations that conflict with trade secrets and antitrust law; enforce DMA data-access duties to empower business users; and clarify Data Act switching and termination rules (including fair, exit-friendly penalty calculations for fixed-term SaaS under hybrid pricing). Additional priorities include safeguarding trade secrets, addressing consumer harms from price personalization, and ensuring a level playing field for municipalities and SMEs.

> *This, for instance, is true for the automotive sector, where the European Commission has conducted comprehensive in-depth studies3 which have identified a number of technical, legal and policy issues concerning access to vehicle-generated data and state that "policy makers could consider measures to promote more competition in these markets and reduce the OEMs monopolistic hold on car data and service delivery channels".* (ZVEI e.V.)

> *The Data Act, in particular, is a cornerstone for Europe's data economy: potentially weakening it would risk undermining fair competition and innovation in all data-driven sectors, including mobility.* (FIGIEFA aisbl)

> *In practice, this market structure in which the consumer-facing business doesn't re- tain exclusive control over its audience data is a tax on quality content, par- ticularly premium journalism, the proceeds of which are used to subsidise disinformation and AI slop farms.* ()

> *If they comply with the transparency obligation under the DA, they risk violating competition law.* (Bitkom e.V.)

ZVEI e.V.: Calls for applying the Data Act to correct access asymmetries in the automotive sector, reducing OEMs' monopolistic control over vehicle data to foster competition and fair data access.

> *This, for instance, is true for the automotive sector, where the European Commission has conducted comprehensive in-depth studies3 which have identified a number of technical, legal and policy issues concerning access to vehicle-generated data and state that "policy makers could consider measures to promote more competition in these markets and reduce the OEMs monopolistic hold on car data and service delivery channels".*

FIGIEFA aisbl: Warns that weakening the Data Act would undermine fair competition and innovation, urging preservation of coherent frameworks that establish baseline data access rights across sectors, including mobility.

The Data Act, in particular, is a cornerstone for Europe's data economy: potentially weakening it would risk undermining fair competition and innovation in all data-driven sectors, including mobility.

: Argues that third-party data controllers exploit cross-site data to the detriment of publishers and consumer-facing businesses, distorting markets and harming quality journalism, and calls to stop such practices.

In practice, this market structure in which the consumer-facing business doesn't re- tain exclusive control over its audience data is a tax on quality content, par- ticularly premium journalism, the pro- ceeds of which are used to subsidise disinformation and AI slop farms.

France Digitale: Seeks clarity on how the Data Act's termination rights interact with fixed-term SaaS contracts and whether early termination penalties are fair and permissible, especially under hybrid pricing models.

According to a certain interpretation of art. 25, however, the fixed-term contracts SaaS startups rely on would be incompatible with the new mandatory short-term termination rights.

Unipol Assicurazioni S.p.A.: Highlights unbalanced data-sharing regimes that disadvantage financial entities and service providers in mobility, urging sectoral rules to ensure FRAND access and limit OEM discretion over vehicle data and pricing.

Only a vertical regulatory act that restricts the carmaker's expected discretion in identifying the data to be shared (through direct or indirect access) will effectively guarantee all aftermarket service providers genuine access to vehicle data and resources under FRAND technical and economic conditions, thereby enabling operators to develop more innovative and competitive services for the benefit of the entire community and competition.

Bitkom e.V.: Criticizes Data Act reporting and cost-disclosure mandates as burdensome and potentially conflicting with competition law, proposing their removal in favor of standard legal redress mechanisms.

If they comply with the transparency obligation under the DA, they risk violating competition law.

WKÖ - Austrian Federal Economic Chamber: Emphasizes enforcing the Digital Markets Act so large platforms provide business users with data access, supporting fair competition and a level playing field.

In this context the application of Digital Market Acts is very important: large platforms need to provide data to their business customers

European Law Institute: Notes that price personalization tends to raise consumer costs, posing risks to data fairness and privacy and warranting regulatory attention.

Japan Business Council in Europe (JBCE): Advocates stronger safeguards for trade secrets within data-sharing frameworks to balance access with confidentiality and maintain fair competition.

Advertising Information Group: Contends that stricter cookie consent rules disadvantage SMEs in digital advertising, entrenching larger players and harming competitive balance and media sustainability.

MVFP Medienverband der freien Presse e.V.: Warns that centralized consent mechanisms can concentrate power with gatekeepers, limiting publishers' access to user data and weakening their market position.

The Center for Countering Digital Hate: Supports enhancing user choice, control, and compensation for data use to rebalance power with platforms and promote fair, sustainable digital markets.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Notes gatekeepers' obligations around PIMS while stressing practical limits, and observes that privacy-friendly services face structural economic disadvantages in current data markets.

Council of European Municipalities and Regions (CEMR): Calls for a level playing field in data access and sharing for municipalities and regions, preventing dominance by large platforms and enabling fair public-private data collaboration.

2.10.5 Platform Transparency, Regulation & Disinformation

Stakeholders converge on the need for robust, evenly enforced EU digital frameworks—especially the DSA and DMA—to secure a fair, open, and trustworthy online environment, protect smaller actors, and curb gatekeeper dominance. They warn that regulatory "simplification" must not dilute cornerstone safeguards, and highlight uneven enforcement that can privilege adtech intermediaries and tech monopolies while burdening SMEs and eroding sovereignty as platforms set de facto rules. To bolster platform transparency and counter disinformation, proposals include stronger data access for independent oversight, regulating social media like other high-impact industries, and product-level measures to dampen virality (e.g., limiting resharing) and remove perverse for-profit incentives. At the same time, transparency obligations must be calibrated to avoid conflicts with competition law (e.g., cost disclosure) and unnecessary duplication (e.g., certain P2B transparency duties). Calls also stress correcting a corporate-driven policy agenda and embedding rights- and accountability-based approaches as a path to sustainable competitiveness.

However, simplification must not come at the expense of essential safeguards or lead to the weakening directly or indirectly of cornerstone legislative acts such as the Digital Services Act (DSA) and the Digital Markets Act (DMA). (France Digitale)

These frameworks are critical to ensuring a fair, open, and trustworthy digital environment. (France Digitale)

We have certainly seen this dynamic at play with the GDPR, which seems to apply relatively stringently to small European actors while leaving the big global actors mostly untouched. ()

Regulating locally re- mains possible, but matching the power that digital infrastructure has to set rules is challenging, which in turn undermines sov- ereignty and makes regulation at best hard to apply in practice. ()

FIGIEFA aisbl: Supports EU digital legislative instruments to ensure a level playing field and spur innovation among platforms and market actors. Emphasizes rules that promote fairness and transparency in the digital ecosystem.

The EUs digital legislative instruments are essential to create a level playing field and stimulate innovation.

: Warns that current enforcement of digital rules disproportionately burdens small European actors while benefiting adtech intermediaries and tech monopolies. Notes that platforms' rule-setting power undermines sovereignty and makes local regulation hard to apply.

Unfortunately, the specific way in which they are enforced and implemented undermine this shared interest and only benefit adtech intermediaries, and primarily tech monopolies amongst those.

France Digitale: Urges that regulatory simplification must not weaken the DSA and DMA. Stresses these frameworks are essential to maintain a fair, open and trustworthy digital environment against gatekeeper power.

However, simplification must not come at the expense of essential safeguards or lead to the weakening directly or indirectly of cornerstone legislative acts such as the Digital Services Act (DSA) and the Digital Markets Act (DMA).

DOT Europe: Calls for removing P2B transparency requirements, suggesting they are unnecessary or overly burdensome. Argues streamlining obligations on platforms to reduce compliance friction.

Association des Constructeurs Européens de Motocycles: Argues that mandated cost transparency could conflict with competition law. Cautions that such disclosures may distort markets or expose sensitive data, undermining fair competition.

The Center for Countering Digital Hate: Highlights persistent transparency failures by social media platforms and advocates robust, enforceable data access and oversight. Calls for regulating social media like other industries and for decisive government action against disinformation.

European Digital Rights (EDRi): Criticizes a corporate-driven digital policy agenda that weakens democratic oversight. Calls for stronger, rights-based platform governance and transparency to protect the public interest.

Siemens Healthineers AG: Advocates limiting viral resharing and excluding for-profit influence in information flows to curb disinformation harms. Supports measures that reduce amplification incentives on platforms.

AI Accountability Lab (AIAL), Trinity College Dublin: Contends European competitiveness should be built on fundamental rights, transparency, and accountability. Supports regulatory approaches that align innovation with robust oversight of platforms.

2.10.6 Media Sustainability, Advertising & Measurement

Media sustainability hinges on financially viable models that blend subscriptions with advertising, underpinned by data processing and analytics. Press revenue relies heavily on personalised advertising to monetise non-subscribers and keep subscriptions affordable; contextual-only models are not currently scalable. Proposals for centralised consent or making consent harder would reduce publisher revenues, entrench gatekeepers' data advantages, and risk media pluralism and citizens' access to free, ad-funded news—undermining the press's democratic role. Advertising and measurement must be practical, transparent, and interoperable. Business users need standardised, machine-readable access to campaign, ranking, and reach metrics from gatekeeper platforms, while the real-world ad supply chain (notably affiliate networks) requires longer attribution windows and near-real-time reporting to validate transactions, optimise campaigns, and pay publishers on time. Calls for independent audience measurement frameworks, protections for IP and broadcaster revenues, and broader cultural funding support complement these measures to preserve a diverse, competitive media ecosystem.

A free press can only be free, if it can finance its operations in the market. (EMMA-ENPA)

With regard to the financing aspect, personalised online advertising is an essential source of revenues for press publishers, allowing them to monetise visits by users who do not have a subscription - and to keep the price of subscriptions more accessible. (EMMA-ENPA)

It is often said that we have yet to find a business model for online journalism but that is not true: the business model of online journalism is perfectly fine. ()

The PMC and ATA therefore both depend on universal publisher adoption, something that does not currently exist and likely will never exist. (Sheridans, on behalf of Awin AG)

: Argues that the online journalism business model is fundamentally sound but requires protection from policies or practices that would undermine it to maintain a thriving democratic media.

It is often said that we have yet to find a business model for online journalism but that is not true: the business model of online journalism is perfectly fine.

EMMA-ENPA: Press publishers stress that financial viability depends on data-driven, personalised advertising and site-level consent, warning that centralized consent or limits on targeting would slash revenues and harm pluralism.

With regard to the financing aspect, personalised online advertising is an essential source of revenues for press publishers, allowing them to monetise visits by users who do not have a subscription - and to keep the price of subscriptions more accessible.

Siinda: Calls for gatekeepers to provide standardized, machine-readable APIs and reciprocal access to performance data so advertisers and publishers can transparently measure and optimize campaigns.

Require gatekeepers to offer APIs for advertisers, publishers, and third-party providers to access business-relevant metrics (ad performance, ranking metrics, audience reach) in machine-readable, anonymised formats.

Sheridans, on behalf of Awin AG: Explains that PMC/ARA tracking and reporting frameworks are misaligned with affiliate marketing, relying on unrealistic direct publisher adoption, using too-short tracking windows, and delaying reporting that impairs optimization and payments.

Neither the PMC nor ARA offer a tracking period appropriate for the usual practice of affiliate marketing.

EuroGeographics: Notes that making data free can reduce the income of mapping and geospatial agencies, with implications for sustainable funding of public information services.

European Casino Association (ECA): Warns that deceptive advertising imitating licensed casino brands misleads consumers and diverts lawful revenues, undermining fair competition in ad markets.

European Broadcasting Union: Urges that simplification efforts must not weaken IP and copyright protections and should preserve public service media exemptions to safeguard sustainable content funding.

Advertising Information Group: Raises concern that regulatory changes could jeopardize media diversity by destabilizing advertising-funded models and measurement frameworks.

Fedoweb - Federazione Operatori Web: Emphasizes that reliable, comparable audience metrics are essential for allocating advertising spend and sustaining digital publishers.

ICMP - International Confederation of Music Publishers: Highlights the significant economic and cultural contribution of copyright-based industries in the EU, underscoring the need to protect their revenue streams in the platform economy.

MVFP Medienverband der freien Presse e.V.: Asserts that personalized advertising is vital to finance free press offerings and keep subscriptions affordable, supporting media sustainability.

German Newspaper Publishers and Digitalpublishers Association (BDZV): States that access to user data and advertising revenues underpin the ability of newspapers to provide free, pluralistic journalism.

noyb: Argues that loosening tracking rules can backfire on publishers by entrenching gatekeepers and damaging the economics of independent media.

Audience Measurement Coalition (AMC): Advocates a mandatory, independent and transparent cross-media audience measurement framework with clear definitions and thresholds to ensure fair competition and ad market efficiency.

European Publishers Council: Calls for strong enforcement of rightsholder and publisher rights to maintain fair value flows and compliance in digital advertising and distribution.

ACT (Association of Commercial Television and Video on Demand Services in Europe): Seeks protections against platform practices that erode broadcasters' and VOD services' advertising and data revenues, to sustain European media.

Culture Action Europe: Recommends EU budgetary support and fair remuneration rules to offset tech platforms' negative impacts on culture and ensure artists and cultural media are sustainably paid.

2.10.7 AI Governance & Competitive Neutrality

This category synthesizes calls for AI governance that preserves competitive neutrality by curbing gatekeeper power while enabling innovation and media sustainability. Stakeholders urge evidence-based policymaking that calibrates regulatory obligations to proven economic burdens, noting that early claims of competitiveness harm are speculative. They also argue that well-designed rules for general-purpose AI can bolster Europe's competitiveness rather than hinder it. Proposed levers include significantly ramping up support for open-source AI to avoid winner-takes-all dynamics; maintaining a level playing field under the AI Act for SMEs, publishers, and European competitors; and addressing contractual asymmetries vis-à-vis Big Tech providers. Further priorities are to monitor and mitigate concentration risks even among non-high-risk AI suppliers, ensure fair creator–AI platform terms with proper rights and compensation, and prevent current AI strategies from entrenching monopolies or inflicting broader societal harms.

> *We call for the support of Open Source AI technologies to be significantly intensified in order to counteract a 'winner-takes-all' dynamic in which a few companies dominate the market.* (WKÖ - Austrian Federal Economic Chamber)

Evidence-based policymaking requires regulatory obligations to be balanced with their economic burden based on empirical data. (Democracy Reporting International (DRI))

Given the current stage of implementation of AI obligations, claims that it is harming competitiveness remain speculative. (Democracy Reporting International (DRI))

We call for the support of Open Source AI technologies to be significantly intensified in order to counteract a 'winner-takes-all' dynamic in which a few companies dominate the market. (WKÖ - Austrian Federal Economic Chamber)

Democracy Reporting International (DRI): DRI argues that at this early stage, claims that AI rules harm competitiveness are unproven and urges evidence-based calibration of obligations against real economic burdens.

Given the current stage of implementation of AI obligations, claims that it is harming competitiveness remain speculative.

WKÖ - Austrian Federal Economic Chamber: WKÖ calls for significantly ramped-up support for Open Source AI to prevent winner-takes-all outcomes and preserve competitive neutrality against dominant firms.

We call for the support of Open Source AI technologies to be significantly intensified in order to counteract a 'winner-takes-all' dynamic in which a few companies dominate the market.

Pour Demain Europe: Pour Demain Europe contends that clear, harmonized rules for general-purpose AI can strengthen European competitiveness by fostering trust and a level playing field.

Intesa Sanpaolo: Intesa Sanpaolo urges addressing contractual asymmetries with Big Tech in AI services to safeguard bargaining power and fair competition for downstream users.

Corporate Europe Observatory: Corporate Europe Observatory warns that current AI strategies risk entrenching monopolies and harming the public interest, calling for stronger measures to curb market concentration.

German Newspaper Publishers and Digitalpublishers Association (BDZV): BDZV advocates maintaining a level playing field in the AI Act so gatekeepers cannot disadvantage publishers, supporting fair competition and media sustainability.

Seznam.cz, a.s.: Seznam.cz seeks balanced regulation between content creators and AI firms to ensure fair use terms, compensation, and competitive neutrality in digital markets.

ESYS Foundation: The ESYS Foundation highlights risks from supplier concentration even outside high-risk AI, recommending oversight to prevent dependencies that distort competition.

Culture Action Europe: Culture Action Europe calls for enforceable creators' rights, attribution, and compensation in AI to sustain cultural ecosystems and ensure fair competition with platforms.

2.10.8 Miscellaneous

This category aggregates cross-sector views that converge on maintaining a rules-based level playing field through proportionate, predictable regulation and inclusive policymaking. Stakeholder-driven simplification, ordo-liberal principles of efficient market oversight, and targeted obligations for large actors or gatekeepers (such as self-identification duties) are presented as tools to protect fair competition without unduly burdening smaller players. Strategically, contributors reject importing US-centric benchmarks, preferring a European social market approach aligned with globally successful, fairness-oriented economies. They stress real-economy nuances: tender-heavy, complex supply chains in rail; the need to prevent concession authorities from acting as market beneficiaries; risks that one-size-fits-all rules can erode agricultural competitiveness; and cautions that a business-first competitiveness agenda can harm communities and media sustainability. Overall, the insights advocate competitive neutrality coupled with social safeguards and resilient information ecosystems.

We strongly believe that the EU should continue to provide and guard rules that are aimed at providing a level- playing field for businesses. (European Tyres and Rubber Manufacturers' Association)

Instead, one should look at globally successful economies (Netherlands, the Nordic states, Switzerland) that are in line with the European model of social market economy and fair competition. (Democracy Reporting International (DRI))

We do not support the uncritical endorsement of the Draghi report that makes the US the measure of successful economics. (Democracy Reporting International (DRI))

European Tyres and Rubber Manufacturers' Association: The tyre industry urges that any regulatory streamlining involve all relevant stakeholders and that EU rules continue to safeguard a level playing field for businesses.

We strongly believe that the EU should continue to provide and guard rules that are aimed at providing a level- playing field for businesses.

Democracy Reporting International (DRI): DRI rejects making the US the benchmark for competitiveness and favors comparison with European-style social market economies aligned with fair competition.

Instead, one should look at globally successful economies (Netherlands, the Nordic states, Switzerland) that are in line with the European model of social market economy and fair competition.

European Law Institute: ELI highlights the need for a large-scale self-identification obligation for major actors to support oversight and fair competition in markets with gatekeeper dynamics.

Mafex – Spanish Railway Association: Mafex underscores the complexity of supply chains and tender-driven projects in rail, calling for competition and procurement rules that reflect these realities to ensure fair outcomes.

European Network Against Racism (ENAR): ENAR cautions that a business-first competitiveness agenda can harm marginalized communities and calls for safeguards to ensure fairness and social equity.

Enedis: Enedis proposes limiting concession authorities as beneficiaries to avoid market distortions and maintain competitive neutrality.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: The institutes advocate an ordoliberal, rules-based regulatory regime to promote efficient markets and restrain gatekeeper power while preserving fair competition.

Deutscher Bauernverband e.V.: The German Farmers' Association argues that regulatory burdens weaken agricultural competitiveness and urges easing them to maintain a level playing field.

2.11 SME Proportionality and Practical Compliance

The standout message: move from size-based carve-outs to coherent, risk-proportionate, simplified obligations with strong safeguards, delivered through harmonized standards, clear guidance, and realistic timelines. SMEs face heavy administrative drag—duplicative reporting, costly monitoring and conformity checks, extensive documentation and API upkeep, and tight transitions. Remedies include consolidation and once-only reporting via a single interface, interoperable tools, focusing assessments where they add value, shifting duties upstream (including producer liability), and exempting low-risk internal uses. Proportionality must be consistent across instruments and sectors, with timelines anchored to available standards, stakeholder participation, sector-specific guidance, and avoidance of misapplied platform-style burdens or disproportionate sanctions that entrench big tech. Safeguarded simplification keeps oversight and EU protections intact while streamlining processes, including in the public sector, and avoids SME-only carve-outs that backfire in supply chains. Practical support is essential: national support centers, sandboxes, shared repositories, standardized templates, tailored fees, and collective compliance—while acknowledging partner documentation demands and certification costs, and embedding inclusion, fair tech transfer, and digital sovereignty. Fragmentation across GDPR, ePrivacy, DSA and beyond chills innovation, especially for startups facing high-risk, cybersecurity and connectivity requirements. Priorities: end-to-end alignment, fair data access and cost-based compensation, addressing power asymmetries, coordinated implementation, and simple SME certification limited to genuine SMEs. Across sub-categories, the pattern is clear: risk-based proportionality, regulatory coherence, and

practical tooling—not exemptions—reduce burden without weakening safeguards. The shared goal is to cut bureaucracy so SMEs can comply efficiently and compete and innovate.

2.11.1 Regulatory Coherence & Harmonization

Regulatory Coherence & Harmonization under SME Proportionality and Practical Compliance calls for uniform, coordinated simplification across EU digital rules—GDPR, ePrivacy, DSA and related sectoral requirements—to reduce duplicative, overlapping obligations and fragmented national implementations. Stakeholders advocate clear, consistent guidance applicable to all companies, streamlined once-only reporting and a single reporting interface, as well as harmonized standards and certifications, so SMEs can comply efficiently without navigating conflicting frameworks. Coherence also means addressing structural interactions between instruments (e.g., ePrivacy with GDPR) and including missing pieces (e.g., DSA) in deregulatory reviews to ensure end-to-end alignment. Across insights, there is strong opposition to SME-specific exemptions or leniency: lowering obligations by firm size risks regulatory inconsistency, weakens accountability chains, and can backfire by pushing larger controllers to avoid SME processors, undermining competitiveness and innovation. The preferred path is uniform simplification—reduce administrative burden for everyone through coherent rules and practical compliance tools—rather than fragmented, size-based carve-outs.

> *The Commission can achieve its objective to reduce companies' administrative burdens by ensuring regulatory clarity through guidance applicable to all companies and consistency across Member States.* (Amazon)
>
> *While such a proposal would ease the disproportionate burden that the ePrivacy Directive currently places on businesses, it should only be understood as a transitional measure-a stop-gap solution to the deeper structural problem of how the Directive interacts with the GDPR.* (ACEA (European Automobile Manufacturers' Association))
>
> *Lower compliance standards for SMEs could heighten the risk of supply chain attacks that would impact data subjects' privacy and the wider economy.* (Amazon)
>
> *To protect themselves, larger controllers may avoid working with SMEs altogether or only work with SME processors that agree to adhere to the higher standards of data protection.* (Amazon)
>
> **Amazon:** Amazon cautions that lowering standards for SMEs would fragment accountability and discourage larger controllers from engaging them; instead, it recommends EU-wide guidance and consistency to reduce burdens while preserving security.
>
> *The Commission can achieve its objective to reduce companies' administrative burdens by ensuring regulatory clarity through guidance applicable to all companies and consistency across Member States.*
>
> **Seznam.cz, a.s.:** Seznam.cz urges the Commission to include the DSA in its deregulation review to harmonize digital rules and cut unnecessary administrative costs for local EU businesses, aligning changes with the Digital Omnibus.
>
> *Such changes would align with the goals of the Digital Omnibus, and we would therefore like to suggest including them in the upcoming proposal.*
>
> **ACEA (European Automobile Manufacturers' Association):** ACEA highlights incoherence between the ePrivacy Directive and the GDPR as a structural issue that creates disproportionate burdens, arguing that temporary fixes are insufficient and deeper alignment is needed.
>
> *While such a proposal would ease the disproportionate burden that the ePrivacy Directive currently places on businesses, it should only be understood as a transitional measure-a stop-gap solution to the deeper structural problem of how the Directive interacts with the GDPR.*
>
> **EVOLIS:** EVOLIS points to duplicative reporting obligations across frameworks that create redundant compliance work for manufacturers, calling for harmonized, once-only reporting to streamline oversight.
>
> **Federation of Austrian Industries:** They advocate consolidating and streamlining reporting through a once-only principle and interoperable systems to harmonize requirements across Member States and authorities.

IDEMIA: IDEMIA warns that SME-specific leniency would open loopholes and drive inconsistent implementation, urging coherent, uniform rules and enforcement across the EU.

Federation of German Consumer Organisations (vzbv): The Federation of German Consumer Organisations rejects SME or mid-cap exemptions, favoring coherent, uniform consumer protection obligations for all companies to avoid regulatory fragmentation.

Ecommerce Europe: Ecommerce Europe stresses that overlapping and inconsistent rules increase complexity and costs, disproportionately affecting SMEs, and calls for coherent alignment of digital regulations.

SMEs are disproportionately affected due to limited resources.

ITI - Information Technology Industry Council: ITI seeks coordinated simplification across EU and national levels to align requirements and reduce cumulative compliance burdens on SMEs.

CPME: CPME notes that fragmented standards and certifications hinder SME compliance and recommends harmonized frameworks to alleviate unnecessary burdens.

Brunel University of London: Brunel University of London finds that regulatory fragmentation undermines SME compliance and innovation, supporting greater coherence across regimes.

European Entrepreneurs CEA-PME: CEA-PME reports that inconsistent GDPR interpretations across Member States harm SMEs and growth, and calls for harmonized guidance and enforcement.

Free ICT Europe Foundation: Free ICT Europe Foundation proposes a single, harmonized reporting interface to simplify compliance for SMEs and reduce duplicative submissions.

2.11.2 Risk-Based, Proportionate & Sector-Tailored

This category argues for regulatory obligations that scale with risk and context rather than company size, rejecting one-size-fits-all approaches. It highlights the need for clear and consistent proportionality across digital and AI frameworks to avoid overlapping or duplicative requirements and disproportionate sanctions that deter innovation and strain SMEs. Implementation timelines should be realistic and anchored to the availability of harmonised standards so that small providers can actually adopt them; evidence-based policymaking should weigh compliance benefits against economic burdens. A sector-tailored approach is emphasized: provide sector-specific guidance, keep certification and documentation proportionate, and avoid imposing platform-style or subcontracting burdens on actors for whom they are ill-suited (e.g., peer-to-peer resale platforms or non-platform providers). Effective stakeholder participation is key to workable rules. Without proportionate implementation, cooperative and mid-sized local institutions can be disadvantaged relative to big tech, risking market concentration and reduced local innovation.

That requires realistic implementation timelines tied to the availability of harmonised standards, standards-based conformity that companies can actually use in practice, and SME-appropriate documentation and reporting so effort scales with risk and not with company size. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

GPSR introduces new obligations for digital platforms without differentiating by size or function. (Adigital (Asociación Española de la Economía Digital))

Furthermore, the proposed sanctions for non-compliance are disproportionately high, even exceeding those under GDPR, which adds another layer of financial risk. (Unipol Assicurazioni S.p.A.)

For instance, without clearer guidance, SMEs in the financial sector could face a double regulatory burden (DORA and AIFMD9) that stifles their capacity for innovation. (FERMA - Federation of European Risk Managers Associations)

FERMA - Federation of European Risk Managers Associations: FERMA warns that the EU's digital framework lacks consistent application of proportionality, leading SMEs—especially in finance—to face overlapping burdens that hinder innovation. It calls for clearer, sector-aware guidance to align obligations with risk and capacity.

FERMA also sees shortcomings when it comes to the application of the proportionality principle throughout the EU digital framework, especially when it comes to SMEs.

Volkswagen Group: Volkswagen Group urges proportionate timelines that reflect overlapping horizontal and sectoral data rules, giving industries such as automotive sufficient lead time for practical compliance. This avoids undue strain across businesses of different sizes.

Further, sufficient lead time has to be allowed, taking into consideration that various horizontal and sectoral legislations with respect to data have recently been introduced with a considerable impact on large, medium and small businesses as well as Startups in one of Europe's key industries: Auto- motive.

FEBIS: FEBIS argues that inclusive stakeholder participation is essential to crafting proportionate, workable rules tailored to sector realities and SME capacities. This ensures legislation is both effective and practical.

Effective stakeholder participation is key to building proportionate and workable legislation.

Unipol Assicurazioni S.p.A.: Unipol Assicurazioni cautions that ambitious timelines and excessive sanctions create disproportionate burdens, undermining feasible compliance. It calls for calibrated enforcement aligned with market realities and risk.

Furthermore, the proposed sanctions for non-compliance are disproportionately high, even exceeding those under GDPR, which adds another layer of financial risk.

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): The German AI Association advocates effective, proportionate AI Act implementation with realistic timelines tied to harmonised standards and SME-appropriate documentation. Effort should scale with risk, not company size, to keep compliance feasible for startups and SMEs.

That requires realistic implementation timelines tied to the availability of harmonised standards, standards-based conformity that companies can actually use in practice, and SME-appropriate documentation and reporting so effort scales with risk and not with company size.

Democracy Reporting International (DRI): DRI promotes evidence-based proportionality, requiring obligations to be balanced with their economic burden using empirical data. This supports risk-based, practical compliance for smaller actors.

Evidence-based policymaking requires regulatory obligations to be balanced with their economic burden based on empirical data.

Adigital (Asociación Española de la Economía Digital): Adigital highlights disproportionate B2C-style obligations applied to small peer-to-peer platforms and urges size- and function-sensitive rules, especially under GPSR. This protects sustainable reuse models and reduces fragmentation and operational burdens.

GPSR introduces new obligations for digital platforms without differentiating by size or function.

European Associations of Co-operative Banks (EACB): EACB warns that AI Act burdens weaken cooperative banks' ability to innovate and risk concentrating services in big tech. It calls for proportionate implementation for cooperatives and mid-sized institutions to preserve local competition.

Proportionality in implementation must therefore be ensured for cooperative and mid-sized institutions, which play a vital role in Europe's local economies.

: This document supports risk-based, targeted restrictions over blanket bans to avoid unnecessary burdens. It emphasizes proportionate, sector-tailored approaches for practical compliance.

Deutscher Caritasverband e.V.: Deutscher Caritasverband seeks sector-specific compliance guidance so social services can meet obligations proportionately. Tailored support helps SMEs and nonprofits implement rules feasibly.

European Law Institute: The European Law Institute stresses calibrated obligations, preserving simplified regimes for small controllers and exemptions for hosting-only processors. This maintains proportionality and avoids undue compliance costs.

Telekom Austria AG: Telekom Austria urges avoiding platform-style burdens for non-platform telecom providers. Proportionate, sector-aware rules should reflect differing roles and risk profiles.

Federation of Austrian Industries: The Federation of Austrian Industries calls for certification requirements that are proportionate and scalable to company size and sector risk. This ensures feasible, risk-based compliance.

Confederation of Industry of the Czech Republic: The Czech industry confederation recommends removing disproportionate subcontracting obligations and excluding small marginal funds. Aligning rules with risk and scale improves practicality.

International Federation of Reproduction Rights Organisations (IFRRO): IFRRO supports differentiated obligations that reflect sector roles and sizes, avoiding one-size-fits-all burdens in copyright ecosystems. Proportionate frameworks ensure workable compliance.

MedTech Europe: MedTech Europe advocates a balanced, proportionate regulatory approach with sector-specific considerations for medical technologies. Tailored rules enable practical compliance and innovation.

AI Standards Lab: AI Standards Lab calls for necessary and proportionate burdens aligned with actual risk and warns of liability designs that may unduly affect mid-scale providers. Calibration prevents unintended consequences.

Verband der Automobilindustrie e.V.: The automotive association criticizes broad cross-sector Data Act obligations as disproportionate for components and systems. It urges sector-tailored requirements to avoid overburdening manufacturers.

Confederation of European Security Services (CoESS): CoESS warns that strict interpretations can impose disproportionate burdens on security services. Pragmatic proportionality should guide implementation to fit sector realities.

Association des Constructeurs Européens de Motocycles: The motorcycle industry notes that low-sales exemptions often fail to reflect sector realities, leading to disproportionate demands on small-volume manufacturers. Better tailoring is needed.

European Broadcasting Union: EBU argues for rules calibrated to SME capacities in broadcasting, preventing excessive burdens while maintaining accountability. Proportionate application supports sector diversity.

EU DisinfoLab: EU DisinfoLab highlights risks of unequal laws by company size and prefers risk-based proportionality over arbitrary thresholds. Tailored obligations improve fairness and effectiveness.

Plateforme de la filière Automobile: The automotive platform opposes blanket extensions of SME exemptions to mid-caps, favoring precise, risk-based tailoring. This keeps incentives aligned without undermining proportionality.

Danish Institute for Human Rights: The Danish Institute for Human Rights supports proportionate HRDD for SMEs, scaled by risk and sector context. This ensures feasible compliance while upholding rights.

Orgalim - Europe's Technology Industries: Orgalim calls for simplified documentation for benign, non-critical product data environments, aligning effort with risk. This avoids unnecessary burdens on low-risk use cases.

European Federation for Market Research Organisation (EFAMRO): EFAMRO warns that one-size-fits-all rules oversimplify diverse market research practices. Proportionate, tailored regulation better matches sector heterogeneity.

Siemens Healthineers AG: Siemens Healthineers critiques approaches that ignore sector-specific needs and promotes lean, proportionate regulation for health technologies. Tailoring improves compliance and innovation.

INVERCO: INVERCO finds ICT subcontractor record-keeping obligations disproportionate for investment firms. Risk-based adjustments would reduce unnecessary burdens.

Computer & Communications Industry Association (CCIA Europe): CCIA Europe rejects one-size-fits-all and warns against generalising cybersecurity rules across sectors. Proportionate, context-aware obligations are needed.

European Savings and Retail Banking Group: The European Savings and Retail Banking Group commits to a consumer-oriented yet proportionate framework for savings and retail banks, including smaller institutions. Tailoring supports feasible compliance.

APPLiA (Home Appliance Europe): APPLiA supports self-assessment as a practical, proportionate compliance route for appliance manufacturers. This reduces unnecessary burden while maintaining accountability.

2.11.3 Safeguarded Simplification

Safeguarded Simplification means making compliance simpler without diluting protections. The aim is to remove redundancies, inconsistencies, and procedural complexity while preserving clarity, usability, and high standards for sustainability, transparency, consumer and data protection. Measures should be proportionate and risk-based, reduce costs and bureaucracy, and avoid expanding obligations. Oversight and accountability must remain strong—supported by social dialogue and appropriate supervision—to maintain trust. Where appropriate, simplifications can extend to the public sector as well. A balanced approach should uphold European values and safety frameworks while enabling innovative business models and fair competition, particularly supporting SMEs by easing how obligations are met rather than lowering the bar. Evidence-based simplification should not shield providers from responsibility nor weaken safeguards or adoption; it should focus on streamlining processes and practical compliance. Caution is urged against SME-only carve-outs that can create weak links and supply chain risks, deter partnerships with SMEs, and ultimately harm competitiveness and innovation.

It is crucial to emphasize that regulatory simplification should not be equated with deregulation or a weakening of the protection of fundamental values. (Adigital (Asociación Española de la Economía Digital))

However, we would like to highlight that simplification should not come at the cost of clarity and usability. (FEBIS)

However, limiting simplification efforts to SMEs, while well intended, risks creating regulatory uncertainty, triggering unintended consequences across broader supply chains and undermining the GDPR principle of accountability. (Anitec-Assinform)

Lower compliance standards for SMEs could create weak links, heightening the risk of supply chain attacks that would impact data subjects' privacy and the wider economy. (Anitec-Assinform)

FEBIS: Calls for simplification that preserves clarity and usability, ensuring streamlined rules remain understandable and practical for compliance.

However, we would like to highlight that simplification should not come at the cost of clarity and usability.

Adigital (Asociación Española de la Economía Digital): Argues that simplification should remove redundancies without weakening fundamental protections, balancing European values with operational viability, especially for SMEs. It stresses that regulation must maintain high sustainability and transparency standards while minimizing disproportionate burdens on smaller firms.

It is crucial to emphasize that regulatory simplification should not be equated with deregulation or a weakening of the protection of fundamental values.

Anitec-Assinform: Warns that SME-targeted simplifications can erode accountability and introduce supply-chain risks, potentially discouraging partnerships with SMEs and undermining competitiveness.

However, limiting simplification efforts to SMEs, while well intended, risks creating regulatory uncertainty, triggering unintended consequences across broader supply chains and undermining the GDPR principle of accountability.

Deutscher Caritasverband e.V.: Supports easing compliance while maintaining protections for beneficiaries and data subjects, ensuring simplification does not reduce safeguards.

European Law Institute: States SME exemptions should not shield providers from accountability or safety obligations, keeping core responsibilities intact.

FINANSFORBUNDET (CVR 15320613): Advocates that any simplification be developed through social dialogue to safeguard workers, consumers, and financial stability.

Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs (VÖWG): Calls for balanced simplification with clear safeguards and oversight, avoiding unintended consequences in public services and the social economy.

Federation of German Consumer Organisations (vzbv): Contends that lowering protection thresholds harms SMEs and hinders adoption, urging simplification that preserves consumer rights and trust.

CENTR - Council of European Top Level Domain Registries: Urges avoiding added procedural complexity when simplifying, focusing on reducing administrative overhead without creating new burdens.

Ireland - Department of Enterprise, Tourism and Employment: Promotes evidence-based simplification that identifies harmful obligations and removes them without compromising outcomes or creating risks.

epicenter.works - for digital rights: Supports streamlining processes and cutting bureaucracy while keeping strong safeguards intact, prioritizing effective regulation over administrative formalities.

SGI Europe: Endorses simplification with safeguards and proportionate oversight, and insists streamlining must not expand obligations for service providers.

Cigref: Seeks cost reduction through simplification without lowering standards, enabling efficient compliance for enterprises.

Trans Sped: Favours simplicity that preserves trust and reduces bureaucracy, maintaining robust security and reliability in digital services.

SPMS – Shared Services of the Ministry of Health: Advocates intelligent simplification that improves efficiency without deregulation, preserving safety and accountability in health services.

BioMed Alliance: Supports balanced simplification within safety frameworks and recommends extending pragmatic compliance approaches to the public sector.

AMETIC: Calls for a balance between simplification, security, and consumer protection, warning that SME-focused deregulation would be counterproductive.

Council of European Municipalities and Regions (CEMR): Backs simplification that reduces burdens without weakening safeguards, ensuring resilient, compliant local and regional services.

The European Network of Expertise on Omics: Affirms that simplification should streamline compliance rather than deregulate, preserving scientific integrity and data protection.

2.11.4 Compliance Burden & Admin Relief

Stakeholders across sectors report that compliance regimes often impose significant administrative and technical burdens that raise costs, drain resources, and slow or even halt innovation. These include costly monitoring and frequent conformity assessments, extensive documentation and logging, repeated reporting with limited added value, building and maintaining endpoints/APIs and uptime processes, and applying consumer-facing obligations (e.g., content moderation and transparency) to low-risk intra-group operations. Tight deadlines, short transition periods, and duplicative requirements across frameworks increase the risk of non-compliance, while SMEs, startups, and mid-sized firms frequently lack the budget and expertise to meet complex demands. To improve SME proportionality and practical compliance, respondents advocate targeted administrative relief and simplification: streamline and consolidate obligations, avoid duplicated documentation/reporting, provide practical support and clear guidance, grant realistic timelines and forbearance, calibrate duties to risk and shift responsibilities toward providers rather than users/deployers, and exempt internal corporate environments where public-facing risks are absent. Proposed measures include introducing producer liability to reduce red tape, focusing conformity assessments where they add value, interoperable solutions that lower overhead, and targeted exemptions. Without such adjustments, Europe risks losing ideas and investment to jurisdictions with simpler pathways while burdening organizations without commensurate safety benefits.

> *Despite the AI Act being a solid foundation, it is viewed as overly complex and expensive for many creators, especially individuals working independently, small businesses, and tiny teams.* (2Dyles Services)
>
> *Requiring compliance with the DSA for intra-group hosting imposes unnecessary administrative and financial burdens on companies.* (Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries)
>
> *The associated costs and logistical challenges are such that we would have no viable alternative but to terminate the project.* (Airbus)
>
> *This approach has proved counterproductive in the implementation of the GDPR and should not be replicated for the AI Act.* (ENGIE)
>
> **Airbus:** Airbus warns that stringent compliance requirements would create high costs and iterative assessments that slow innovation. Low thresholds for substantial modification could trigger constant reevaluation and risk project viability.
>
> *Frequent, iterative conformity assessments will inevitably hinder future innovation.*
>
> **Amazon:** Amazon notes regulatory changes may add operational complexity for EU companies and those expanding internationally. This increased burden can hinder cross-border growth.
>
> *Such changes could add complexity to both European businesses seeking international expansion and companies operating within the EU.*
>
> **ENGIE:** ENGIE cautions that the AI Act places disproportionate compliance obligations on deployers and users rather than providers. They argue this design risks repeating counterproductive patterns seen under GDPR.
>
> *As regards the AI Act specifically, while acknowledging the valuable framework it provides to the safe deployment of AI across sectors, the current architecture risks putting excessive burden on the deployers/users of AI models and systems when it comes to compliance rather than incentivising providers to offer compliant and safe technologies.*
>
> **Sheridans, on behalf of Awin AG:** Requirements would force advertisers to build and maintain unfamiliar technical infrastructure, creating significant cost and operational burdens. Fragmented implementations would also strain networks through disparate data ingestion.
>
> *Few advertisers are equipped to manage this infrastructure, which involves maintaining a compliant server endpoint, ensuring uptime, handling retries, and staying current with browser specification changes.*
>
> **:** The proposal would duplicate administrative tasks for high-risk medical device manufacturers without improving safety beyond MDR. This adds unnecessary paperwork and compliance costs.

only duplicate the administrative burden for manufacturers of high-risk class IIb and III medical devices, without increasing the level of safety beyond the already established and comprehensive MDR system.

2Dyles Services: 2Dyles argues the AI Act is overly complex and expensive for small creators and micro teams. Without practical support, Europe may lose innovation to regions with simpler regulatory pathways.

Despite the AI Act being a solid foundation, it is viewed as overly complex and expensive for many creators, especially individuals working independently, small businesses, and tiny teams.

Bundesverband der Deutschen Industrie (BDI) / Federation of German Industries: BDI contends applying DSA obligations to intra-group hosting imposes unnecessary administrative and financial burdens ill-suited to internal environments. They highlight redundancy of public-facing safeguards for internal services.

Requiring compliance with the DSA for intra-group hosting imposes unnecessary administrative and financial burdens on companies.

American Chamber of Commerce to the EU: AmCham EU warns that the Cyber Resilience Act's complexity risks overloading businesses with compliance tasks. They call for clearer guidance or temporary forbearance to ease implementation.

: They propose introducing producer liability for tech companies to alleviate compliance documentation burdens on EU businesses. This shift would free resources for more meaningful work.

If you seriously want to reduce red tape for EU businesses with regard to the GDPR and other digitalisation laws, you will introduce producer liability for tech companies.

European Travel Retail Confederation (ETRC): ETRC argues national labelling rules create unnecessary compliance and packaging burdens for suppliers in travel retail. Harmonization is needed to prevent fragmentation-driven costs.

ENSHPO - The European Network of Safety and Health Professional Organizations: ENSHPO highlights that small OSH firms face heavy requirements for compliance documentation, logging, and reporting. Simplifications would help SMEs manage obligations sustainably.

Gen Digital: Gen Digital notes extensive documentation obligations consume resources without clear benefits. They urge focusing on high-value compliance activities.

Ingka Group IKEA: IKEA emphasizes the significant costs and operational complexity of transitioning to new regulatory frameworks. They seek phased approaches to avoid disrupting business processes.

Bundesministerium für Inneres: The ministry warns of rising administrative expenses from new rules and the need for expensive technical adaptations. They urge proportionate requirements to avoid undue burdens.

Telekom Austria AG: Telekom Austria argues DSA reporting and compliance obligations are excessively demanding for providers. Streamlining would reduce unnecessary administrative workload.

IDRS Platform: IDRS claims its approach can reduce compliance overhead for regulated entities. Simplified processes and tools can ease administrative tasks.

BusinessEurope: BusinessEurope warns mandatory conformity assessments create significant costs and delays, especially for SMEs. They advocate risk-based, proportionate procedures.

Confederation of Norwegian Enterprise (NHO): NHO points out that maintaining compliant user interfaces under geoblocking rules imposes ongoing technical and administrative burdens. Flexibility is needed to limit maintenance overhead.

Ecommerce Europe: Ecommerce Europe stresses that certain proposals require substantial technical changes and investments. These burdens could strain online businesses, particularly smaller players.

CENTR - Council of European Top Level Domain Registries: CENTR urges realistic timelines to avoid inadvertent non-compliance driven by tight deadlines. Longer transitions would mitigate administrative stress.

ITI - Information Technology Industry Council: ITI recommends extended transition periods to allow companies to implement requirements without excessive burden. This supports practical compliance and reduces risk.

REIF: REIF highlights that compliance obligations entail significant financial costs for firms. Relief measures could improve feasibility and competitiveness.

IAB Europe: IAB Europe notes that growing compliance costs divert resources from innovation and service improvements. They call for proportionate, streamlined rules.

Association des Constructeurs Européens de Motocycles: ACEM warns that new registration, update processes, and reporting duties would impose heavy administrative burdens on manufacturers. Simplification and clear mechanisms are necessary.

CLEPA: CLEPA stresses that limited implementation timelines hamper practical compliance for automotive suppliers. Additional time would reduce administrative pressure.

CSC - IT Centre for Science: CSC advocates simplifying incident reporting obligations for SMEs to avoid disproportionate administrative loads. Tailored requirements can maintain security without excessive paperwork.

European Fund and Asset Management Association (EFAMA): EFAMA argues extensive data collection duties offer limited supervisory value while increasing administrative effort. Targeted reporting could reduce burden.

Orgalim - Europe's Technology Industries: Orgalim believes proposed SMC simplifications under Omnibus IV do not adequately reduce administrative burdens for technology industries. More ambitious red-tape reduction is needed.

Association of German Cities: German cities warn that new mandates could overwhelm limited municipal resources. Proportional obligations and funding are needed to avoid undue burdens.

Middle Tech Europe: Middle Tech Europe cautions that overlapping regulatory requirements cumulatively strain mid-sized technology companies. Streamlined, coherent rules would alleviate pressure.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: They propose simplifying application and administrative processes to cut bureaucracy for participants. Clearer procedures would lower compliance overhead.

Adyen: Adyen warns that stringent EU regulations can burden startups and scale-ups, limiting growth. Proportionate, innovation-friendly compliance is needed.

Confederation of Swedish Enterprise: They report GDPR-related compliance generates high administrative costs for businesses. Relief and simplification would free resources for productive activities.

2.11.5 SME Support & Capacity Building

SME Support & Capacity Building centers on making compliance proportional and practical: keep obligations intact while cutting bureaucratic load, harmonizing reporting across regulations, and providing accessible, cost-efficient tools, guidance, and platforms. Proposed measures include dedicated AI support centers in national authorities, regulatory sandboxes and shared repositories, co-designed capacity-building with government,

tailored fees, and collaborative or collective compliance models that help SMEs overcome limited resources, governance gaps, and startup uncertainty. The aim is to enable experimentation and innovation while ensuring SMEs can meet obligations efficiently and fairly. The category also flags constraints and unintended effects that capacity-building must address. SME exemptions often yield minimal real-world relief because larger partners still demand full documentation; voluntary certifications, though helpful, can exert market pressure and add costs; and simplification must embed social safeguards—prioritizing inclusion, equitable technology transfer, and digital sovereignty—so innovators, including African SMEs, can participate fully in EU digital markets. Prioritizing SMEs, practical guidance, and standardized tools reduces compliance friction and mitigates risks of unequal exclusion.

> *Smaller operators should be supported through accessible and cost-efficient compliance platforms to ensure fair participation in the digital environment.* (Union of Entreprenuers and Employers)
>
> *Companies should receive comprehensive support, e.g. through a dedicated AI support centre within the national authorities that can be easily contacted in case of uncertainties or when advice is needed.* (WKÖ - Austrian Federal Economic Chamber)
>
> *Larger companies, which are not covered by the exemptions, will still need to demand full documentation from their service providers and partners-even if those partners qualify for exemptions - in order to meet their own accountability obligations under Article 5(2) GDPR.* (Volkswagen Group)
>
> *Simplification must prioritise inclusion, capacity building, and equitable technology transfer, enabling African innovators and SMEs to participate fully in EU digital markets while safeguarding digital sovereignty.* ()
>
> **:** Advocates keeping obligations intact while reducing SME bureaucracy by aligning regulatory requirements and enabling one-stop reporting, so SMEs can focus on practical compliance and innovation.
>
> *The regulations should be simplified ONLY if this means alignment in terms of bureaucratic load and less burden for SMEs (e.g. allowing companies to generate one report that covers multiple regulations).*
>
> **Volkswagen Group:** Warns that proposed SME exemptions yield limited practical relief because larger partners will still require full documentation from exempt SMEs to meet their own accountability obligations.
>
> *Larger companies, which are not covered by the exemptions, will still need to demand full documentation from their service providers and partners-even if those partners qualify for exemptions - in order to meet their own accountability obligations under Article 5(2) GDPR.*
>
> **:** Argues that any simplification must embed inclusion, capacity building, and equitable technology transfer so African innovators and SMEs can fully participate in EU digital markets without undermining digital sovereignty.
>
> *Simplification must prioritise inclusion, capacity building, and equitable technology transfer, enabling African innovators and SMEs to participate fully in EU digital markets while safeguarding digital sovereignty.*
>
> **Union of Entreprenuers and Employers:** Calls for accessible, cost-efficient compliance platforms to help smaller operators participate fairly and meet obligations at lower cost.
>
> *Smaller operators should be supported through accessible and cost-efficient compliance platforms to ensure fair participation in the digital environment.*
>
> **WKÖ - Austrian Federal Economic Chamber:** Notes that while standards and certifications can reduce effort, even voluntary schemes can pressure SMEs and add costs; recommends dedicated, easily reachable AI support centres and tailored support measures for SMEs.
>
> *Companies should receive comprehensive support, e.g. through a dedicated AI support centre within the national authorities that can be easily contacted in case of uncertainties or when advice is needed.*
>
> **European Law Institute:** Suggests enabling collective delegation of compliance obligations to reduce burdens, letting associations or intermediaries support SMEs in meeting requirements efficiently.

Pour Demain Europe: Highlights heightened liability risks for SMEs in digital regulation and urges mitigation measures to avoid chilling participation and innovation.

Healthtech Finland: Stresses that SME concerns in healthtech require targeted, sector-specific solutions and support to achieve practical compliance.

Federation of German Consumer Organisations (vzbv): Advocates practical tools and clear guidance to help SMEs implement obligations effectively and proportionately.

Brunel University of London: Recommends government support and co-designed capacity-building initiatives to address weak governance and compliance gaps that hinder SMEs.

EFCA - European Federation of Engineering Consultancy Associations: Points out that many SMEs lack the resources and capacity for compliance, calling for proportionate requirements and supportive measures.

Digital Currencies Governance Group (DCGG): Emphasizes that authoritative guidance can reduce compliance friction and enable SMEs to navigate obligations more smoothly.

Danish Entrepreneurs: Notes startups face significant compliance uncertainty and need clarity, simple processes, and scaled obligations to innovate safely.

Free ICT Europe Foundation: Urges simplification of AI Act compliance for SMEs through proportionate obligations and supportive resources that limit administrative burden.

European network of equality bodies (Equinet): Prefers non-legislative support—guidance and capacity-building—over amendments to help SMEs achieve compliance in practice.

STM: Promotes practical compliance tools and templates to make SME adherence cost-effective and straightforward.

AI Accountability Lab (AIAL), Trinity College Dublin: Observes that SME exemptions deliver minimal real-world relief because ecosystem demands persist, indicating the need for alternative support mechanisms.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Proposes sandboxes and joint repositories to lower entry barriers, acknowledges SMEs are disadvantaged by regulatory complexity, and urges prioritization with tailored fees.

Council of European Municipalities and Regions (CEMR): Calls for addressing unequal exclusion of SMEs from markets and public services by mitigating compliance complexity and offering support.

: Recommends assisting companies with concrete compliance tools and help, with emphasis on SME practicality and efficiency.

2.11.6 Innovation, Competition & Data Access

Stakeholders emphasize that well-calibrated regulation can foster innovation, but the sheer proliferation and fragmentation of EU digital rules have imposed disproportionate burdens on SMEs. Startups, lacking in-house legal resources, face overlapping filings and significant upfront costs—especially for high-risk systems—that can effectively exclude them from regulated markets. Without clearer alignment and practical guidance, even pro-innovation measures like the Data Act risk becoming compliance obstacles. Additional monitoring, connectivity, and cybersecurity requirements further hinder deployment in practice, chilling innovation in sectors from safety and health to agriculture and local government. To preserve competition and unlock data-driven innovation, contributors call for SME-proportionality in both obligations and data access: streamlined and harmonized compliance, cost-based data compensation, fair access and reuse arrangements, and attention to power asymmetries that disadvantage smaller firms. A consistent theme is protecting the integrity of SME relief by maintaining a sup-port tailored measures and avoiding their extension to mid-caps; introducing simple SME certification to speed up access to exemptions; and improving coordination to reduce fragmentation. Together, these steps seek to lower barriers while sustaining a level playing field for genuine SMEs.

While carefully designed regulatory intervention can foster innovation, the EU's legislative maze, comprising in early 2025 exactly 101 adopted di- gital laws, has often constrained growth, especially for European SMEs that face disproportionate compliance costs compared to global giants (see FIGURE 5). ()

The financial impact is significant: for high-risk AI systems, compliance preparation alone can absorb tens of thousands of euros, effectively excluding smaller innovators from regulated markets. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

We call for a coordinating body, cost-based data compensation, and SME certification, but oppose mid-cap exemptions. (ACEA (European Automobile Manufacturers' Association))

Without clearer alignment and practical guidance, the Data Act's promise to foster innovation may instead create compliance burdens that small companies cannot realistically manage. (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association))

: Carefully designed regulation can spur innovation, but the EU's sprawling digital rulebook imposes disproportional compliance costs on SMEs, constraining their growth relative to large players.

While carefully designed regulatory intervention can foster innovation, the EU's legislative maze, comprising in early 2025 exactly 101 adopted di- gital laws, has often constrained growth, especially for European SMEs that face disproportionate compliance costs compared to global giants (see FIGURE 5).

Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. (German AI Association): Existing EU digital rules create heavy compliance and data-access burdens that small AI firms cannot absorb, diverting scarce resources from development and effectively shutting SMEs out of regulated markets.

The financial impact is significant: for high-risk AI systems, compliance preparation alone can absorb tens of thousands of euros, effectively excluding smaller innovators from regulated markets.

ACEA (European Automobile Manufacturers' Association): SME-focused exemptions should remain exclusive to genuine SMEs to preserve fair competition; a certification mechanism can streamline verification while preventing mid-caps from benefiting.

Exemptions provided to SMEs under digital legislation such as the Data Act should not be extended to mid-cap companies, as this would distort competition and dilute support for genuine SMEs; rather, a certification mechanism for SMEs should be created so that they can demonstrate their status, to simplify verification and ensure SMEs can swiftly avail of these exemptions.

ENSHPO - The European Network of Safety and Health Professional Organizations: Cumulative regulatory demands in safety and health risk chilling innovation, as smaller organizations struggle to comply while experimenting with new approaches.

CPME: Policies should ensure equitable SME access to data, addressing power imbalances so smaller firms can compete and innovate.

Local Government Denmark: Continually expanding digital regulations strain SMEs' capacity to innovate, as compliance obligations outpace practical capabilities.

Digital Currencies Governance Group (DCGG): Strict monitoring and connectivity mandates hinder deployment of new solutions, imposing overhead that particularly slows SME innovation.

OpenMined: Model cards and similar transparency tools can disadvantage SMEs by overlooking power asymmetries, reinforcing perceptions that regulation is anti-innovation.

Deutscher Bauernverband e.V.: Complex, overlapping rules hamper SME innovation by increasing administrative load and slowing practical implementation.

2.12 Miscellaneous

Durable digital progress hinges on trustworthy, evidence-based governance and disciplined execution that earn public confidence while enabling innovation. Stakeholders call for transparent, broadened participation, proportionality, and accountability, resisting blanket deregulation and emphasizing early scrutiny and fitness checks to safeguard legitimacy. Adoption depends on a people-first risk approach, credible assurance mechanisms, and operational readiness; codes of practice and supportive EU digital laws can catalyze uptake if backed by verifiable compliance. Administrative simplification should be targeted and resourced—cut legacy bureaucracy, prioritize substance over form, improve digital workflows, and preserve legal certainty—with caution toward centralization that isn't tied to user needs. Strategy must convert into delivery: align funding tools and eligibility, build capacity and skills, and pair rights-preserving protections with market-shaping instruments to strengthen competitiveness amid leadership risks. Sustainability is being integrated across trade, digital, and corporate governance, linking CBAM to broader architectures and anchoring climate criteria in new domains, while guarding against omnibus dilution and ensuring enforceability. Across sub-categories, the common threads are balance, integrity, and execution: stakeholder engagement, outcome-based reforms, and coherent instruments that build trust, protect users, and scale innovation responsibly.

2.12.1 Digital Strategy, Leadership & Competitiveness

A winning EU digital strategy requires more than an overarching vision: it needs a second, tightly coupled step of execution—aligning investment tools and rules with strategic priorities, building capacity and skills, and ensuring broad, predictable eligibility for EU funds. Stakeholders flag gaps such as InvestEU's limited digital relevance and an under-ambitious Digital Omnibus, while calling for coherent protections and incentives that enable sectors from health research to creative industries to digitize at scale and responsibly. AI strategies are framed around expansion and adoption, but must be matched with operational enablers. From a leadership and competitiveness standpoint, Europe's position is not assured: digital rights groups warn EU leadership is at risk, US industry headwinds illustrate the value of resilient, balanced frameworks, and the premise that liberal democracies enjoy an intrinsic edge over authoritarian rivals is challenged. The policy imperative is pragmatic: pair rights-preserving protections with market-shaping instruments, execution discipline, and targeted financing to convert strategic intent into competitive advantage.

> *However, introducing an overall vision to each of the EU's digital policy activities is still not enough.* ()
>
> *It can only be the first of two crucial as well as interconnected steps.* ()
>
> *The assumption that the EU has an advantage in competing with actual or quasi-dictatorships is terminally flawed.* ()
>
> *However, introducing an overall vision to each of the EU's digital policy activities is still not enough.* ()
>
> **:** Introducing an overarching vision for EU digital policy is necessary but insufficient for leadership. It requires a second, interconnected step focused on execution to deliver results.
>
> *However, introducing an overall vision to each of the EU's digital policy activities is still not enough.*
>
> **:** The belief that the EU holds a structural advantage against authoritarian competitors is flawed. Acknowledging this is vital to recalibrate strategy and strengthen competitiveness.
>
> *The assumption that the EU has an advantage in competing with actual or quasi-dictatorships is terminally flawed.*
>
> **DigitalTrade4.EU:** It criticizes InvestEU for lacking relevance to digital priorities and failing to bolster EU digital trade leadership. The program's design should be aligned with strategic digital competitiveness goals.
>
> **Palombar - Associação de Conservação da Natureza e do Património Rural:** It notes AI strategies that prioritize expansion can overshadow sustainability and governance. This focus risks undermining responsible leadership and long-term competitiveness.
>
> **REIF:** It calls for guaranteeing eligibility for EU funds to ensure key digital initiatives can access financing. Predictable access would accelerate strategic capacity and competitiveness.

ICMP - International Confederation of Music Publishers: Industry headwinds in the US illustrate the value of resilient frameworks and supportive policy. The EU should apply lessons to reinforce its digital competitiveness in creative sectors.

European Digital Rights (EDRi): It warns the EU's digital leadership is at risk without rights-respecting policy choices. Centering fundamental rights is essential for sustainable competitiveness.

BioMed Alliance: It urges investment in capacity building to strengthen digital capabilities across sectors. Building skills and infrastructure is key to leadership and competitiveness.

STM: It argues strong protections such as IP and data safeguards are essential to sustain digital leadership. Clear, enforceable rules underpin competitive innovation ecosystems.

Deutscher Bauernverband e.V.: It criticizes the Digital Omnibus for lacking the ambition needed to drive transformation. Greater scope and clarity are needed to support competitiveness in agriculture and beyond.

2.12.2 Governance, Evidence & Process Integrity

Across submissions, governance, evidence, and process integrity are emphasized over expedient simplification. Stakeholders warn against non-evidence-based changes, unsubstantiated cost-saving claims, and outdated risk metrics; they call for fitness checks, addressing root causes rather than blaming bureaucracy, targeted and coordinated adjustments instead of blanket deregulation, and, where needed, regulatory pauses with early scrutiny to ensure proportionality and accountability. Process integrity hinges on transparent, broadened consultations and structured participation: civil society and social partners, municipalities, researchers, and industry should be involved through mandatory procedures, researcher-focused dialogues, collaborative case studies, and practical guidelines/codes. Effective governance requires stakeholder alignment, recognition of trade-offs, and careful political/operational balancing, with clarity on management duties and AI role transitions/model versioning, and dialogue and cooperation before any changes. These safeguards are cast against a backdrop of declining open democracies, underscoring the need to reinforce trust and legitimacy in decision-making.

Each of the proposed initiatives involves trade-offs among different stakeholders, thus requiring a certain level of compromise. (European Cyber Security Organisation)

Both the political and operational aspects will need to be carefully considered to strike a balance between concerns and priorities. (European Cyber Security Organisation)

Only 3.5 % of people still live in open systems that are democratically oriented. ()

: Highlights the global erosion of open, democratic governance, underscoring the urgency of evidence-based safeguards and accountability.

Only 3.5 % of people still live in open systems that are democratically oriented.

European Cyber Security Organisation: Emphasizes that governance reforms must balance stakeholder trade-offs and weigh both political and operational considerations to maintain process integrity.

Each of the proposed initiatives involves trade-offs among different stakeholders, thus requiring a certain level of compromise.

: Endorses a joint civil society position, signaling support for collective, transparent governance advocacy.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: Argues for instituting early scrutiny with a clear business case to improve accountability and risk management in decision-making.

Deutscher Gewerkschaftsbund: Urges a permanent procedure for social partner involvement to institutionalize inclusive and predictable governance.

Palombar - Associação de Conservação da Natureza e do Património Rural: Questions the proposal's rationale and calls for clearer justification grounded in evidence and necessity.

Polish Confederation Lewiatan: Criticizes reliance on outdated systemic risk metrics and urges updating indicators to reflect current governance realities.

Federation of German Consumer Organisations (vzbv): Contends bureaucracy is not the main cause of declines and urges tackling root causes for durable, evidence-based improvements.

AI Standards Lab: Identifies governance gaps around role transitions and model versioning, calling for clear traceability and change-control processes.

Association des Constructeurs Européens de Motocycles: Supports mandatory management training but flags unclear requirements that could impede consistent, accountable implementation.

secunet Security Networks AG: Calls for stakeholder alignment and balanced collaboration to ensure coherent, legitimate policy processes.

EWE AG: Advocates targeted, coordinated adjustments rather than broad changes to preserve effectiveness and process integrity.

German Newspaper Publishers and Digitalpublishers Association (BDZV): Warns against non-evidence-based changes and notes claimed cost savings are unsubstantiated, urging rigorous analysis.

Danish Institute for Human Rights: Stresses the need for transparent, rights-compliant consultations throughout policymaking to uphold legitimacy.

European Federation for Market Research Organisation (EFAMRO): Proposes leveraging guidelines and professional codes to pragmatically resolve governance and implementation challenges.

EUROCINEMA: Urges dialogue and cooperation with stakeholders before changes, reinforcing participatory process integrity.

Association of German Cities: Emphasizes crucial municipal involvement early in processes to ensure legitimacy and practical feasibility.

European Digital Rights (EDRi): Critiques premature simplification as lacking an evidence base and risking erosion of necessary safeguards.

Computer & Communications Industry Association (CCIA Europe): Calls to broaden consultations to include more stakeholders, improving balance and information quality.

PensionsEurope: Supports mandatory participation mechanisms for stakeholders to ensure completeness and fairness in governance.

Eurosmart: Supports collaborative case studies to inform policy and criticizes the Commission's approach as insufficiently reflective of real-world complexity.

STM: Endorses balanced simplification that preserves process integrity and supports an evidence-based fitness check.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Notes repeated concerns voiced by a major platform actor, underscoring the need to document and address stakeholder input.

Association Française des Entreprises Privées: Advocates a regulatory pause and review to reassess impacts with robust evidence before proceeding.

International Federation of Library Associations and Institutions: Calls for rigorous critique and structured, researcher-focused dialogues to strengthen evidence and governance quality.

2.12.3 Simplification & Administrative Efficiency

This category emphasizes pragmatic streamlining of administrative systems to unlock innovation and improve user experience. Core lessons include cutting legacy bureaucracy and manual processes, prioritizing substance over form, and tackling structural sources of complexity rather than cosmetic fixes. Effective simplification relies on adequate resourcing—especially for digital document workflows and guidance—to remove friction where it actually occurs. Centralized solutions (such as a single hub) should be approached cautiously, as they may yield limited benefits unless clearly tied to concrete user needs and interoperable processes. Simplification is framed as a disciplined, even constitutional, commitment: keep changes bounded, preserve legal certainty and quality, and focus relentlessly on tangible outcomes. The aim is administrative efficiency that measurably improves service delivery and economic activity without hollowing out safeguards, achieved through targeted reforms, structural clarity, and outcome-based evaluation.

Others Italy and beyond still struggle with legacy bureaucracy that slows innovation and frustrates citizens. ()

: Entrenched bureaucratic systems hinder innovation and frustrate citizens, underscoring the need to modernize and streamline administration.

Others Italy and beyond still struggle with legacy bureaucracy that slows innovation and frustrates citizens.

Intesa Sanpaolo: Advocates administrative simplification that prioritizes substantive outcomes over formalities to reduce paperwork and complexity.

MVFP Medienverband der freien Presse e.V.: Argues simplification should be carefully bounded to preserve necessary detail and safeguards in complex domains.

European Fund and Asset Management Association (EFAMA): Maintains a proposed central hub should be deferred due to limited benefits, redirecting focus to more effective efficiency measures.

Bocconi University: Positions simplification as a constitutional discipline that guides rulemaking to curb excess formalism and improve administrative practice.

Chair in Cyber Policy, University of Luxembourg: Calls for simplification that targets structural causes of inefficiency rather than superficial changes for lasting impact.

Österreichische Notariatskammer: Urges allocating adequate resources and infrastructure for digital document workflows to streamline administration.

Wolt: Highlights inefficiencies from manual processes and supports automation to improve speed and accuracy.

The European Network of Expertise on Omics: Insists simplification efforts deliver tangible, measurable outcomes rather than merely procedural changes.

2.12.4 Innovation, Trust & Adoption

Innovation, Trust & Adoption centers on the idea that technological progress must be matched by reliability and human-centered risk management to earn public confidence. Consumer trust is both essential for uptake and currently fragile—marked by high concern, declining confidence, and blind spots in human–machine interactions. A people-first approach, meaningful engagement, and clear accountability are emphasized as key correctives to these trust gaps. Governance is positioned as an enabler, not a brake: widely endorsed Codes of Practice, benefits flowing from EU digital laws, and regulation designed to support innovation and business are cited as catalysts. At the same time, past certification schemes have failed to provide credible assurance, underscoring the need for more effective, verifiable mechanisms and operational readiness for compliance. A balanced, measured approach to digitalisation that demonstrably protects users while enabling progress is presented as the path to sustainable adoption.

In the long run, the success of this shift will depend on balancing innovation with reliability. (Union of Entreprenuers and Employers)

Union of Entreprenuers and Employers: Emphasizes that sustainable adoption depends on combining cutting-edge innovation with dependable performance to maintain user trust. Calls for aligning novel features with reliability to ensure long-term success.

In the long run, the success of this shift will depend on balancing innovation with reliability.

FINANSFORBUNDET (CVR 15320613): Argues that a trust-based governance framework unlocks innovation by creating the confidence needed for responsible development and uptake.

Pour Demain Europe: Notes that broad endorsement of a Code of Practice fosters shared standards, strengthening trust and supporting wider adoption of innovative solutions.

Federation of German Consumer Organisations (vzbv): Warns that rising consumer concerns and declining trust jeopardize adoption and growth. Stresses that rebuilding consumer trust is essential for market uptake and sustainable innovation.

AI Standards Lab: Signals readiness to handle compliance tasks, helping organizations meet standards that underpin trusted innovation and smoother adoption.

Danish Institute for Human Rights: Advocates a people-first approach to risk management and engagement to secure legitimacy and trust, enabling socially responsible innovation.

European Digital Rights (EDRi): Asserts that robust EU digital laws can deliver tangible public benefits, reinforcing trust and guiding responsible innovation and adoption.

Prosus Group: Maintains that well-designed regulation can simultaneously enable innovation and support business viability while building consumer trust.

: Highlights that framing AI in simplistic human–machine dichotomies creates blind spots that undermine trust and adoption, calling for more nuanced approaches.

Österreichische Notariatskammer: Urges a balanced digitalization strategy that safeguards reliability and legal certainty to maintain trust while enabling innovation.

Alexander von Humboldt Institute for Internet and Society / University of the Arts: Observes that previous certification programs failed to deliver trust or safety, implying the need for more effective accountability mechanisms to support adoption.

2.12.5 Sustainability & Climate Integration

This category captures how sustainability and climate objectives are being embedded across EU policy and governance. On the proactive side, proposals link trade and digital frameworks to climate delivery—for example, integrating the Carbon Border Adjustment Mechanism (CBAM) into a broader EUTIR architecture to mobilize green financing and align digital–climate objectives. Such integration aims to mainstream decarbonization incentives across market rules, finance, and data flows. Counterbalancing this, the insights warn about institutional pathways that can weaken ambition: omnibus lawmaking that dilutes corporate sustainability duties and raises procedural concerns serious enough to trigger Ombudsman scrutiny. They also highlight the importance of legal anchoring—e.g., using Article 95-type provisions to require sustainability-oriented assessments in emerging domains (such as AI)—so that climate impacts become a routine criterion in regulatory design. The throughline is climate integration across trade, digital, and corporate governance, coupled with vigilance to preserve integrity and enforceability.

The first omnibus package framework presented by the European Commission this year significantly diluted the reach and impact of EU corporate sustainability laws, undermining their core purpose and prompting an ongoing investigation by the European Ombudsman into procedural failings. (BEUC - The European Consumer Organisation)

The first omnibus package framework presented by the European Commission this year significantly diluted the reach and impact of EU corporate sustainability laws, undermining their core purpose and

prompting an ongoing investigation by the European Ombudsman into procedural failings. (BEUC - The European Consumer Organisation)

BEUC - The European Consumer Organisation: The organization warns that the European Commission's first omnibus package weakened EU corporate sustainability laws, undermining their core objectives and triggering oversight scrutiny. It flags potential procedural failings that jeopardize effective sustainability enforcement.

The first omnibus package framework presented by the European Commission this year significantly diluted the reach and impact of EU corporate sustainability laws, undermining their core purpose and prompting an ongoing investigation by the European Ombudsman into procedural failings.

DigitalTrade4.EU: The paper argues that integrating the Carbon Border Adjustment Mechanism within the EUTIR can channel green financing and align incentives for decarbonization. It promotes using EUTIR to jointly advance digital trade and climate objectives.

Leverhulme Centre for the Future of Intelligence at the University of Cambridge: The centre highlights the need to embed sustainability considerations into assessments under Article 95, linking governance requirements with environmental responsibility. It suggests formalizing sustainability criteria within evaluation processes.