
ITI
Promoting Innovation Worldwide
Simplifying the EU's Tech Rulebook
www.itic.org

Contents

Executive Summary

Europe's Ever-Expanding Digital Regulatory Framework and the Need for Simplification

Europe's expanding digital regulatory framework, covering areas like platform rules, privacy, AI, and cybersecurity, has created a complex environment with overlapping obligations and fragmented application across Member States. In this context, it adds difficulty for industry to successfully operate in the EU.

This complexity leads to legal uncertainty and administrative burdens, potentially discouraging investment, delaying product innovation, and hindering the adoption of new technologies within the European Single Market.

As highlighted by Enrico Letta and Mario Draghi in 2024, simplifying the EU rulebook will be key to strengthen Europe's competitiveness. Simplification is ultimately for the benefit of both business and consumers.

The EU should conduct an ambitious assessment of legislation, including tech rules – both passed and proposed – with the aim of mapping and simplifying legal overlaps and potential enforcement conflicts. Efforts to simplify the regulatory framework should also adhere to better regulation principles, ensuring clarity, proportionality, transparency, and stakeholder engagement.

The following pages present ITI's concrete proposals for simplifying and streamlining the current EU rules affecting tech and digital industries.

Overarching Guidance:

→ Implementation and Enforcement:

- Ensure regulatory authorities are ready before new EU rules become enforceable.
- Introduce statutory duties for Member State regulators to consider innovation, competition, and growth.
- Promote dialogue and coordination between different authorities to prevent regulatory conflicts.
- Adjust timelines and implement stop-the-clock mechanisms, allowing sufficient transition times for new legislation.

→ Standards and conformity assessment:

- Leverage global standards to simplify compliance, reduce redundancies and facilitate trade.
- Recognize Conformity Assessment Bodies in third countries to streamline compliance procedures.

→ National level simplification:

- Include proactive clauses in EU laws that require Member States to remove equivalent provisions in national law and do not reintroduce comparable provisions in the cases that they are removed from the EU acquis.

Issue-Specific Recommendations:

Cybersecurity:

- **Create national single reporting entry points** that consolidate obligations under NIS2, CRA, DORA, ePD, and GDPR, enabling streamlined and cross-framework reporting.
- **Clarify inter-framework exemptions** by ensuring that incidents reported under NIS2 fulfill corresponding obligations under the CRA when applicable.
- **Enhance coordination and standardization** by empowering ENISA, CSIRTs, and competent authorities to align taxonomies and reporting templates, and formalize ENISA's support role in harmonizing practices.
- **Introduce liability protections within reporting frameworks to encourage timely and comprehensive** reporting by providing legal clarity and reducing risk for companies.
- **Harmonize establishment rules** to ensure consistent oversight of data and cybersecurity obligations in a company's Member State of establishment.
- **Harmonize security requirements** across the CRA, DORA, and NIS2 and establish reciprocity for audits, testing, and certifications across those frameworks.
- **Extend the CRA's applicability timeline** to account for delays in standardization and give industry sufficient time to integrate harmonized standards into product development.

Artificial Intelligence:

- **Simplify the enforcement mechanism of the AI Act and mandate regulators to promote innovation** to align with the AI Act and the AI Continent Action Plan.
- **Ensure AI Act secondary legislation, guidance and compliance tools** such as the Codes of Practice are practical, proportionate, and developed in close consultation with industry.
- **Postpone application of certain AI Act requirements** where harmonized standards are delayed, using mechanisms like a regulatory stop-the-clock.
- **Simplify and streamline inconsistencies** between GDPR and AI Act obligations.

Data Governance and Privacy:

- **Provide clear, practical guidance** on the Data Act, including on its scope and key definitions.
- **Simplify burdensome provisions** in the Data Act such as those related to data transfers and trade secrets.
- **Issue practical guidance to reconcile the Data Act with obligations under the GDPR .**
- **Promote flexible, interoperable data transfer rules** by referencing international standards like OECD Guidelines and cross border privacy rules, and ease GDPR adequacy requirements to reduce burdens on companies, especially SMEs.
- **Repeal the ePrivacy Directive** and rely on the GDPR as the sole framework for personal data in electronic communications, including cookies, traffic, and location data.

Sustainability:

- **Accelerate the digitization of regulatory information** by recognizing digital formats as valid alternatives to physical labeling.
- **Ensure alignment across sustainability laws** by recognizing CSRD disclosures as valid under other pieces of legislation and coordinating new initiatives.
- **Align EU and international rules on waste and circular economy**, harmonizing timelines and interpretations to reduce market fragmentation and support a coherent Single Market for second-use materials.
- **Review data center reporting rules** to ensure alignment with AI and digitalization goals, and tailor obligations to reflect technical feasibility and shared responsibilities.

ITI, the Information Technology Industry Council, is the global trade association of the technology industry, representing 80 of the world's most innovative tech companies. Our membership spans across the entire spectrum of technology, including global leaders on software, hardware, cloud, cybersecurity and semiconductors.

Europe has a substantial and growing digital regulatory framework ranging from platform rules and privacy frameworks to AI, cybersecurity and sector specific legislation. This results in a complex regulatory environment marked by overlapping obligations, diverging requirements across different sets of rules, and fragmented application across Member States. The design and implementation of the EU digital rulebook has raised a number of issues, including a lack of legal clarity and administrative burden, which can unnecessarily disincentivize investment, delay innovative product launches and hinder the uptake of emerging technologies for firms doing business in the European Single Market.[1]

Simplification is therefore not just a technical exercise; it is a key element of strengthening Europe's competitiveness for the benefit of businesses and consumers in Europe. The EU Competitiveness Compass set the objective to simplify the EU regulatory landscape by reducing burden and complexity. **As a next step, the EU should conduct an ambitious assessment of tech legislation – both passed and proposed – with the aim of identifying and mapping legal overlaps and potential enforcement conflicts.**

The results of this assessment should be used to:

1. *Provide further guidance to businesses and authorities where needed;*
2. *Increase coordination of different enforcement authorities where potential conflicts arise; and*
3. *Inform future EU policymaking in pursuit of regulatory simplification and the goal of cutting 25% of recurring administrative costs for all companies, e.g., in the announced Digital package or other Omnibus simplification packages.*[2]

Efforts to simplify the regulatory framework should **also adhere to better regulation principles, ensuring clarity, proportionality, transparency, and stakeholder engagement.**

This report presents ITI's concrete proposals for simplifying and streamlining the current EU acquis affecting tech and digital industries.[3] More broadly, businesses operating in the EU face a variety of structural regulatory challenges which contribute to complexity. In order to tackle these challenges, ITI makes the following overarching policy recommendations, especially concerning **implementation and enforcement, timelines, standards, and better regulation principles for future legislation.**

A Streamlined Approach: Overarching Guidance

Implementation and Enforcement

- EU laws generally enter into effect and become enforceable before the necessary oversight structures and tools are in place. For example, there may be delays in member states legislators transposing EU rules into national law or the regulator not yet being fully staffed or resourced; EU rules can become legally binding before the relevant regulator (a member state regulator, EU-level body or the Commission) has drafted and consulted on actionable and workable guidance that supports company compliance. To avoid the legal uncertainty and contention this causes, the European Commission and Member States should work together to ensure the readiness of regulatory authorities and, where necessary, carefully sequence the entry into effect of new EU rules to avoid adverse effects on companies and ensure continuity of business operations.

- For the vast majority of companies operating in the Single Market, their day-to-day interaction with EU regulation is via Member State regulators. While the Commission has set out how it will simplify the application and oversight of regulation where it acts as a regulatory authority, it is unclear what steps Member State regulators will take to support the EU's simplification and competitiveness objectives. The Council should consider introducing statutory duties on these regulators to have regard to innovation, competition and growth in implementing and enforcing regulation and, as a first step, should task them to develop individual action plans setting out what steps they will take to simplify EU rules, including via stakeholder consultation, revised guidance or exploration of codes to aid compliance.

- The significant expansion of the EU's digital rulebook has increased the number of regulators overseeing and enforcing intersecting regulatory frameworks at national and European level – each with narrow mandates and which do not necessarily cooperate with each other. This creates two challenges contributing to regulatory complexity:

1. **Fragmentation across the Single Market** when national authorities take different interpretations of a particular framework and take different enforcement actions. This risk is also exacerbated in case of incoherent or delayed national transposition of EU rules. To address these challenges, the EU should also review and strengthen the functioning of the TRIS (Technical Regulations Information System) notification process. Ensuring that national laws are consistently and promptly notified would allow early identification of potential barriers to the Single Market, and reduce the risk of divergent approaches.

2. **Potential inconsistencies between regulatory frameworks** when over-lapping rules are applied in divergent ways by different authorities.

- To prevent this, **the EU must encourage the development of structures and ways of working that promote dialogue and coordination between different authorities enforcing EU digital legislation.** For example, Member State authorities should coordinate and collaborate on intersecting areas of regulation; EU-level bodies – such as those gathering Member States or national authorities - could form ad-hoc fora to collaborate on and coordinate the interpretation and implementation of the EU AI Act, DSA, DMA, GDPR, GPSR and cybersecurity legislation. Both these approaches could help prevent regulatory conflicts, and strengthen the cohesion of the Single Market. Both should also be informed by open consultation with regulated companies and other relevant stakeholders to fully understand their concerns and needs with a view to facilitating information sharing, coordinating on shared issues, and aligning policies and legal interpretations, with a particular focus on areas where the EU digital regulations intersect. Such fora must follow better regulation principles, in particular transparency and proportionality.

- **Joint guidance from relevant authorities, harmonized at EU level, can help companies navigate complex regulatory landscapes.** Actionable and workable guidance that supports business continuity and a smooth transition to a new regulatory framework would ensure that legal frameworks around digital policy areas are clear, agile, and streamlined - avoiding overlaps and conflicts. In particular, clear and timely guidance is needed on the **interplay between different regulations**, and on how key principles intersect and potentially overlap and how companies can consistently comply. This approach will promote a consistent understanding and application of regulations, reducing uncertainty for businesses across different regulatory frameworks. All guidance documents issued by national authorities and relevant EU-level regulatory bodies must be informed by **mandatory public consultation**, leaving sufficient and reasonable response deadlines and ensuring that perspectives from industry, civil society, and other stakeholders are taken into account, and that guidance is pro-competitive, practical and effective by design.

- ITI recommends Member State regulators and the European Commission **apply a risk-based approach and Better Regulation principles** to enforcement across the digital policy landscape. Ensuring that enforcement is proportionate, evidence-based, and taking into consideration business models and impact on security and privacy will be key to effective implementation.

Timelines

- When implementing new rules, especially for hardware products, it is crucial for new legislation to **allow for sufficient transition times to minimize business disruption**. Implementation timelines should take into account **product development lifecycles** and there should be **early and clear communication** on what industry stakeholders can expect in terms of requirements for compliance. This should also apply to guidelines, model contracts and harmonized standards which need to be provided well ahead of implementation deadlines, e.g., for compliance with CRA requirements in hardware and software products; or for interoperability standards in the Data Act.

- Before the adoption of new legislation, allowing for enough time for impact assessments and public consultations is critical. Consultation response windows should be lengthened, and initial impact assessments need to be concluded well before public consultations start in order to inform stakeholders' feedback.

- As part of the mission to boost EU competitiveness, we recommend **reusing the 'Stop-the-clock' mechanism applied in the Omnibus I sustainability package** for the field of technology legislation. Postponing the dates of application of certain requirements in the AI Act, the CRA – especially where relevant standards are not yet available - and other recently passed legislation would provide companies in the EU with legal certainty and a way to properly structure their compliance.

Standards and Conformity Assessment

- **Global standards** simplify the EU's regulatory framework by offering a clear, universally accepted method for demonstrating compliance. Shaped by leading pieces of legislation like those developed in the EU, global standards incorporate developments and provide a presumption of conformity with EU rules. This reduces redundancies, helps companies comply across borders, and ensures they meet global compliance expectations, ultimately making international operations more efficient and less burdensome. However, there is growing concern around regionalization of standards, which can be duplicative and unnecessary and undermines their global nature and the benefits they provide. To maintain harmonization and global competitiveness, **the EU should more actively participate in international standardization fora, prioritizing open, transparent, and industryled standards** that involve diverse global stakeholders.

- **Mutual recognition of existing internationally recognized standards** will also contribute to simplification and to reducing burdens in the EU Single Market. Especially where EU harmonized standards are not available or delayed – for example in the cases of the CRA, the RED Delegated Act and AI Act – existing international standards offer a practical and clear avenue for compliance. The Commission should increase recognition of such global standards for the purpose of compliance with EU regulations. This approach ensures inclusivity, facilitates interoperability, and prevents the development of isolated regional standards that could undermine international cooperation.

- **Mutual recognition of Conformity Assessment Bodies (CABs)** in third countries offers a pragmatic alternative to mutual recognition of standards to streamline compliance procedures. By allowing trusted CABs in third countries to certify products against EU requirements, and vice versa, without duplicative testing, this approach can significantly reduce administrative burdens, lower costs, and accelerate time-to-market for companies. Therefore, we invite the Commission to consider the mutual recognition of CABs as a practical simplification tool to enhance the efficiency of the conformity assessment system, particularly in the context of tight timelines of certain pieces of legislation as highlighted throughout this paper.

National Level

- **Remove provisions at national level, too.** When provisions or whole laws are removed from the EU acquis it is important to follow this through at the national level, particularly for Directives, which require national laws to implement them. An example of this is the Data Retention Directive, where approximately half of Member States retained amended national laws after it was taken down in the CJEU Digital Rights Ireland case. Therefore, proactive clauses should be included that require Member States to remove equivalent provisions in national law and not reintroduce comparable provisions.

Simplification in Detail: Issue-Specific Recommendations

EU Cybersecurity Rules

The adoption of frameworks such as NIS 2, the Cyber Resilience Act (CRA), and DORA has strengthened the EU's security but has also resulted in overlapping obligations and divergent implementation across Member States. This diverts some resources away from concrete cybersecurity improvements and toward legal compliance, which may ultimately undermine the overarching goal of raising the EU's cyber resilience. We support the European Commission's commitment to work on an omnibus simplification package for cybersecurity. As announced, this initiative will form part of the upcoming review of the Cybersecurity Act (CSA), and offers an important opportunity to address complexity, duplication, and fragmentation in the current regulatory landscape.

We recommend a comprehensive mapping of existing cybersecurity obligations spanning horizontal (NIS2, CRA), sector-specific (e.g., DORA, NCCS), national, EU-level, and international policies (e.g., cybersecurity standards, certification schemes, SBOM frameworks). The mapping should also consider linkages and overlaps with related regulations, such as the GDPR and the ePrivacy Directive, which can also help avoid adding new duplicative provision for example in the forthcoming Digital Fairness Act. This effort should aim not only to simplify incident reporting and information sharing but also to rationalize risk management obligations. The following are ITI's key recommendations:

Streamline Incident Reporting (NIS2, DORA and the CRA; ePrivacy Directive and GDPR)

Challenge

NIS2, DORA, and the CRA each mandate incident reporting, but they do so with different criteria and scopes. This can create a duplication burden for entities that need to report the same incidents multiple times under different frameworks, increasing operational costs and complexities without necessarily improving response effectiveness. Similarly, reportable incidents under these frameworks may also be reportable under the ePrivacy Directive (ePD) and GDPR.

Overlapping reporting requirements have many adverse effects on in-scope companies. For example, they introduce a heavy administrative burden on companies reporting one incident to multiple authorities. This complexity can ultimately cause businesses to move resources away from mitigation, response and recovery from the incident itself to compliance, in turn, weakening the EU's cyber resilience.

Moreover, deadlines for reporting incidents can be very short (as little as 24 hours in some cases) and information about incidents is dispersed across multiple different agencies (data protection authorities, cybersecurity agencies etc.).

This can result in a lack of situational awareness for governments and delayed incident responses. In addition, different incident reporting formats and technical and language requirements across frameworks can complicate the process especially for entities that operate in multiple jurisdictions all while managing cyber incident response and recovery. For providers of some services, incident reporting can be further fragmented not only across different regulators within a member state but also across multiple EU jurisdictions due to varying establishment rules or the application of the country of origin rule in some frameworks and country of consumption in others.

Recommendations

1 **Establish national single reporting entry points.** We recommend that each Member State establishes at national level a single reporting entry point covering all relevant frameworks including NIS2, the CRA, DORA, ePD, and the GDPR to reduce fragmentation and simplify processes for companies. This entry point would be responsible for ensuring that relevant reports are transmitted to the right authority. Efforts should also be made to ensure it is feasible for companies to comply with reporting obligations within the statutory deadlines, for example by permitting a single report for multiple frameworks and allowing reports to be provided in one language. In the longer term, a technical solution, such as ENISA's single reporting platform, could help route reports to the relevant national or EU authorities, while preserving national entry points and avoiding the creation of a single point of failure.

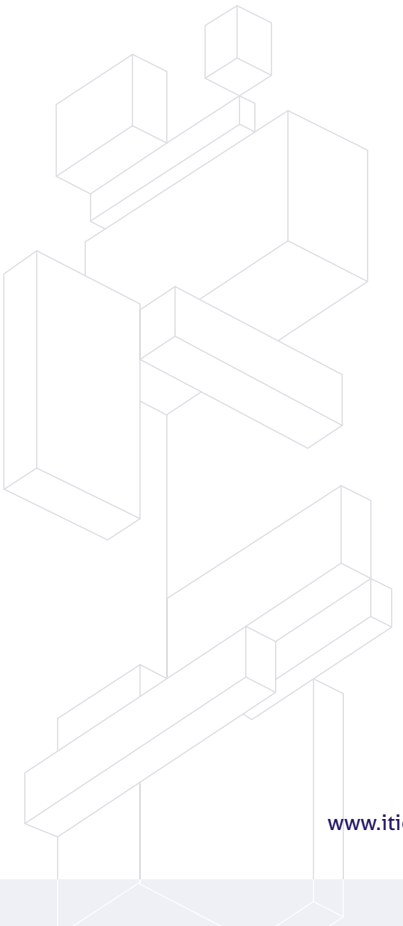
2 Clarifying inter-framework exemptions. To streamline incident reporting, the omnibus simplification package for cybersecurity should clarify that an entity's CRA cyber incident or vulnerability reporting obligations are fulfilled when the entity has already reported the incident or vulnerability under NIS2. Specifically, when a vulnerability exploitation under Article 14(1) CRA or a cyber incident under Article 14(2) CRA qualifies as an incident under Article 23 NIS2, fulfilling the NIS2 reporting obligation should be sufficient for compliance with the CRA.

3 Enhance coordination and establish a common taxonomy and reporting templates. ENISA, CSIRTs, and competent authorities are well-positioned to establish and manage communication and information-sharing procedures among themselves. Strategic coordination among CSIRTS, ENISA and competent authorities is essential, leveraging ENISA's single reporting platform and standardizing requirements across CSIRTs and other bodies to streamline efforts and avoid redundancies in cybersecurity incident reporting. In particular, we recommend the development of a common incident taxonomy and standardized reporting templates to ensure consistency and reduce administrative burden. In the context of the upcoming Cybersecurity Act (CSA) review, we also suggest considering a formalized support role for ENISA, where requested by Member States, to facilitate greater alignment of reporting practices and taxonomy.

4 Include liability clauses in the reporting framework. Liability protections should be incorporated into the reporting framework to provide legal clarity and reassurance for companies. Enhanced legal certainty will encourage more timely and complete reporting, improving situational awareness and response across the EU.

5 Prioritize streamlining establishment rules across different regulatory frameworks. Ensure that the oversight of all data-related and cybersecurity rules is harmonized in the providers' member state of establishment.

6 Extend the country of origin principle. The CSA review should prioritize extending the country of origin principle - including across all services in scope of the CRA, NIS2 and DORA - where it does not currently apply, in place of country of consumption control which introduces unnecessary operational and legal complexity and cost.



Align Definitions Across Frameworks and Foster Harmonization: Definition of "Main Establishment" (CRA and NIS2) and Other Key Concepts

Challenge

EU cybersecurity regulations use different terminology to define similar concepts, leading to confusion and implementation challenges for companies operating across multiple frameworks.

A key example is the divergent definition of "main establishment". Article 11(7) of the CRA provides a different definition of **"main establishment"** than Article 26(2) of the NIS2. This can lead to unclarity for companies that must determine reporting points under both legal frameworks. Moreover, some Member States appear to have adopted an interpretation of "main establishment" that goes beyond NIS2 whereas others have excluded the concept altogether. This divergence raises concerns, as NIS2's goal was to reduce fragmentation, yet conflicting interpretations of "main establishment" creates additional complexity for companies operating cross-border, undermining the one-stop-shop mechanism.

In addition, the NIS2 Directive refers to **"significant incidents"**, while the CRA introduces the term **"severe incident"**, each with differing scopes and thresholds.

Although these definitions apply to distinct environments - service provision under NIS2 and product security under the CRA - such inconsistencies create uncertainty in assessing reporting obligations, especially when incidents may fall under more than one framework.

Moreover, EU cybersecurity frameworks lack a harmonized understanding of what constitutes the moment an entity **"becomes aware"** of a cybersecurity incident or vulnerability, which is critical for the calculation of statutory reporting deadlines.

Finally, another area of divergence concerns the geographic scope of reporting obligations. The CRA does not currently include geographic limits, potentially creating uncertainty for manufacturers regarding the jurisdictional impact of an incident. In contrast, NIS2 limits reporting to incidents that impact the EU, which helps provide clarity.

→ Recommendations

To improve legal certainty and support coordinated implementation:

1 **Align the definition of "main establishment".** The CSA review should align the definition of "main establishment" across multiple frameworks including the CRA, NIS2, and DORA so that entities falling under the scope of more than one act can rely on a legally consistent definition and interpretation of main establishment.

2 **Issue guidance on the legislative intent of "main establishment".** The European Commission should issue guidance clarifying the legislative intent behind the concept of "main establishment" under NIS2, to promote uniform interpretation and application across all 27 Member States and safeguard the functioning of the One-Stop-Shop mechanism.

3 **Align incident severity definitions.** The European Commission should align definitions of incident severity used across the CRA, NIS2, and DORA to reduce ambiguity.

4 **Align the concept of "becoming aware" of an incident.** All cybersecurity-related regulations should adopt a consistent definition for when an entity is considered to have become aware of an incident or vulnerability. We recommend all cybersecurity regulations be aligned with the European Data Protection Board's (EDPB) guidelines on personal data breach notification and NIS2 Implementing Regulation 2024/269 - which state that entities are considered to be aware of a breach or incident when they have a reasonable degree of certainty that a security incident has occurred.

5 **Introduce geographic impact limits in the CRA.** We recommend that the CRA set clear geographic limits that focus on incidents with an impact within the EU, in line with the approach under NIS2.

Harmonize Security Requirements and Compliance Processes

Challenge

NIS2, DORA, GDPR, the CRA, and other EU regulations and mechanisms (e.g. Network Code on CyberSecurity (NCCS) or the 5G Cybersecurity Toolbox) each establish security requirements and compliance processes for organizations and products sold in the EU. While multiple regulations often apply to a single entity, the overlapping requirements differ across regulations and each regulation has a separate process to demonstrate compliance.

The resulting complexity creates challenges in tracking each regulation, integrating the disparate requirements into an organization-wide security program, and working with customers and regulators to document compliance. Even when a company's compliance strategy is simply to adhere to the strictest security requirements among the overlapping regulations, the company still faces multiple processes and audits to demonstrate compliance with each regulation. This diverts company resources to inefficient compliance processes rather than truly impactful security activities and innovation.

Recommendations

The EU should strengthen security outcomes and reduce unnecessary regulatory burdens by harmonizing security requirements and compliance processes across regulations, as well as providing clear reciprocity where compliance with one regulation qualifies as compliance with other regulations. To the extent feasible, this should include:

1. **Harmonizing definitions.** Ensure terms that are used in multiple regulations are defined consistently.

2. **Reciprocity of audits.** Clarify that security and compliance audits performed under one EU regulation qualifies towards fulfilling audit requirements under other regulations for both entities that are required to perform audits and also supervisory authorities when conducting audits. Moreover, it should be clarified that certifications and attestations such as applicable ISO certifications and SOC 2 reports may be used to fulfill audit requirements (see also subpoint 6 below).

3. **Reciprocity of testing.** Clarify that security testing performed under one EU regulation, such as vulnerability scans and penetration tests performed under DORA, qualifies towards fulfilling testing requirements under other EU regulations.

4 **Streamlining documentation and reporting processes.** The EU should establish a single streamlined process for entities to document and report compliance with multiple overlapping regulations.

5 **Harmonizing subcontractor risk management.** Regulations requiring supplier and sub-contractor to adhere to security standards should have consistent requirements, and compliance with one regulation should qualify towards compliance with others.

6 **Reciprocity for standards compliance.** The EU should clarify that it provides reciprocity for compliance with internationally recognized standards and certifications such as, but not limited to, ISO 27001 and SOC2.

7 **Avoid duplication in product certification requirements under CRA and NIS2.** Article 24(2) of the NIS2 Directive allows for the introduction of delegated acts requiring the mandatory use of certified ICT products. This could directly overlap with the CRA, which already establishes conformity assessment and CE marking requirements for ICT products. To avoid duplicative certification obligations and increased administrative burden for manufacturers, we recommend that CE marking under the CRA be deemed sufficient for compliance with any NIS2 delegated act on ICT product certification.

Scope of "Remote Data Processing Services" (CRA and NIS2)

→ Challenge

The CRA includes "remote data processing services" in its scope (Article 2), which may conflict with NIS2's coverage of digital infrastructure and digital service providers, potentially creating ambiguities for entities required to comply with both legal frameworks. The scope of "remote data processing services" is particularly unclear, as the intention was to limit the CRA's scope to avoid overlap with NIS2 measures applicable to cloud services.

However, Article 3 of the CRA provides a broad definition which can encompass a wide range of cloud services, including Platform-as-a-Service (PaaS). Efforts to refine the scope of remote data processing are critical to clarify the CRA's scope of application. Providing clarity will also enable manufacturers to allocate resources effectively to ensure compliance for the products that fall within scope.

→ Recommendations

In the context of the implementation of the CRA, the clarification of the term "remote data processing services" should be prioritized. Alternatively, providers of cloud solutions that are in scope of NIS2 should be explicitly and fully excluded from the CRA, to avoid duplicative requirements.

Data Disclosures under the Data Act

→ Challenge

The Data Act obliges the disclosure of data, potentially even in security-critical contexts – which could conflict with the NIS2 Directive requirements on confidentiality and encryption. While Article 4(2) of the Data Act positively introduces limitations to data sharing where there can be safety and security risks, more clarity would be needed on the application of this 'handbrake.'

→ Recommendation

More clarity should be provided by specifying that in the event of a conflict, the national implementation of the NIS2 Directive is to be applied as a matter of priority.

Repealing the RED Delegated Act

→ Challenge

Implementing the RED Delegated Act cybersecurity requirements is a resource-intensive process, requiring the assessment of the products falling in scope against standards that may not even be ready timely. Manufacturers who fall in scope of the two legislations will face significant challenges in transitioning from the regime stood up under the RED Delegated Act to the CRA, as the two regimes require conflicting types of compliance approaches.

This will require that manufacturers subject to both regimes effectively stand up one compliance regime that will not necessarily translate well to the other, inefficiently allocating cybersecurity resources. Although the RED Delegated Act will apply from 2 August 2025, harmonized standards were only cited in February 2025. This leaves little time for stakeholders to prepare comprehensive self-assessments, which may lead to bottlenecks at notified bodies and a sharp increase in the cost and timing of compliance. Such an outcome should not be repeated during CRA implementation.

→ Recommendations

The omnibus simplification package should address the transition from the RED Delegated Act to the CRA, particularly for manufacturers subject to both frameworks by:

1. Repealing the RED Delegated act.
2. Outlining practical steps for manufacturers to transition their processes and products to CRA requirements.
3. Facilitate the transition from RED Delegated Act conformity to CRA conformity by recognizing the conformity modules and standards of the RED Delegated Act as a means to demonstrate compliance to the corresponding requirements of the CRA.

Expanding CRA Compliance Timelines

Challenge

The effective implementation of CRA depends on the timely availability of harmonized standards. To support effective CRA implementation, the omnibus simplification package should address the need to align compliance timelines with the availability of CRA harmonized standards.

Industry requires at least 8–12 months to integrate standards into product development cycles—often longer for products like microprocessors. Standards must therefore be available well before compliance deadlines, ideally before conformity assessments can even begin. Given that sufficient time should be ensured for the development and integration of harmonized standards and that delays in the standardization process may occur, the package should allow for a possible extension of the CRA's applicability timeline. As with the RED framework, postponing applicability is more practical than imposing unrealistic development timelines.

Recommendation

The omnibus simplification package should allow for a possible extension of the CRA's applicability timeline, acknowledging that delays in the standardization process may occur and that industry requires adequate time to integrate standards into product development cycles.

Harmonizing Public Procurement Requirements

Challenge

As highlighted in the Draghi report on competitiveness, public procurement practices are not harmonized across the EU, reducing economies of scale, impeding Member States' access to innovation, and limiting industry opportunities. In cybersecurity, these impediments are even more significant, with some Member States requiring national accreditations, certifications, and requirements that are not aligned with European or international standards or the EU Cybersecurity Certification Scheme on Common Criteria (EUCC).

Recommendations

The European Commission should pursue harmonization of cybersecurity-related procurement requirements. ENISA and the ECCC could also play a role in raising awareness and promoting harmonization, helping ensure greater market openness and access to cutting edge cybersecurity solutions. Consequently, we welcome the ongoing evaluation of the Public Procurement Directives as a timely opportunity to support harmonization and reduce market fragmentation.

Cybersecurity Act Review

Challenge

The upcoming review of the CSA, which will include the announced omnibus simplification package for cybersecurity rules, provides a critical opportunity to streamline the EU's cybersecurity certification landscape.

Draft certification schemes under the CSA have often lacked reference to existing and internationally recognized cybersecurity standards, such as those developed by ISO/IEC JTC1 SC27 (e.g., the ISO/IEC 27000 series). This has led to ambiguous terminology and requirements that are not always grounded in industry best practices. As mentioned above, the absence of mutual recognition of CABs that deliver equivalent certifications and audit results from third countries creates unnecessary compliance burdens and limits global interoperability.

Moreover, some proposals have included non-technical, sovereignty-based requirements such as data localization, ownership and immunity from non-EU laws. These criteria would reduce competition in the EU cloud and cybersecurity market, and limit access to cutting-edge technologies for both businesses and public authorities.

Data localization requirements would also be detrimental, as they would complicate the exchange of global threat intelligence, increase costs for maintaining state-of-the-art solutions, and limit opportunities for alternative storage in cases of data loss or network outage.

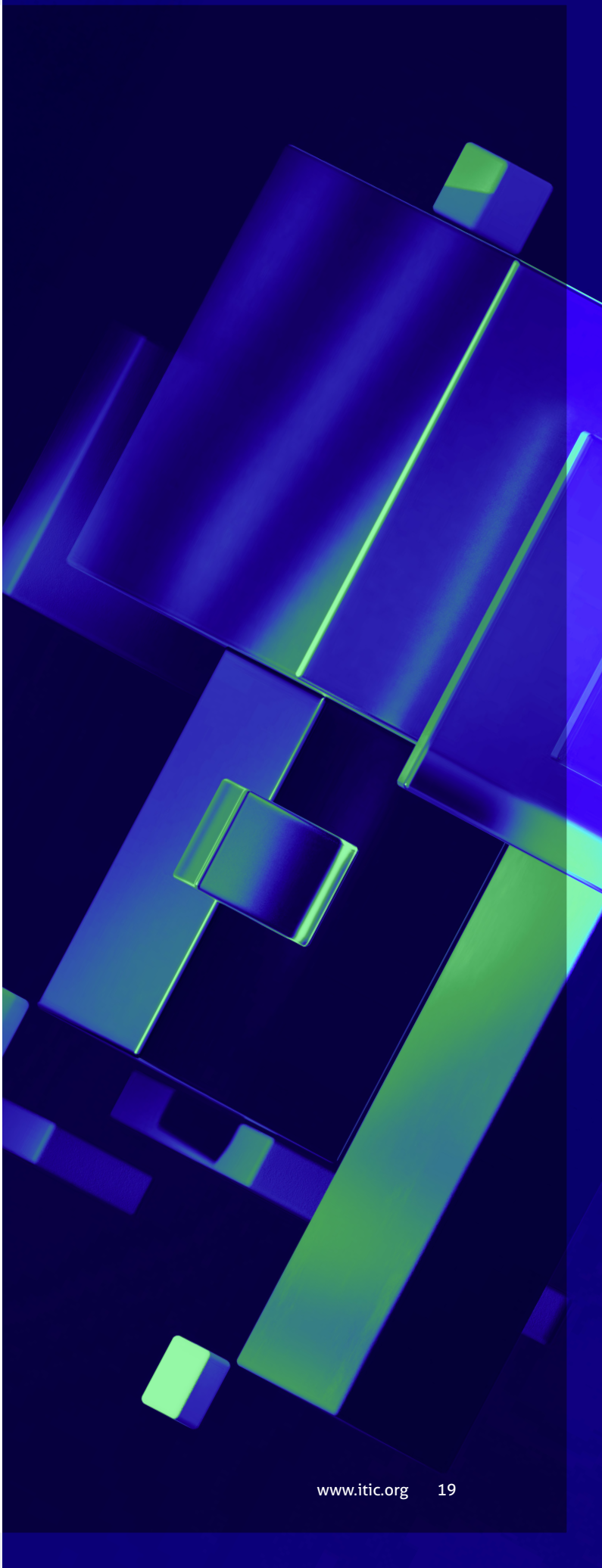
Such approaches risk undermining, rather than strengthening, the EU's cybersecurity posture. Restricting access to innovative, highly secure global solutions and cybersecurity services could inadvertently create gaps and vulnerabilities in Europe's cyber defenses and by that weaken the EU's resilience. Before implementing such disruptive policies, it is crucial to first assess Europe's cybersecurity capabilities and needs in depth. In this exercise, it is crucial to recognize that the current cyber threat landscape is global. Threats do not stop at the EU's borders. Therefore, tackling these challenges effectively requires access to global cybersecurity tools that enable real-time intelligence sharing and robust threat mitigation strategies.

→ Recommendations

1 The EU needs cybersecurity certification schemes that leverage existing and internationally recognized cybersecurity standards to foster global interoperability and to reduce unnecessary compliance burdens for businesses. Schemes should clearly reference standards developed by internationally recognized bodies such as ISO/IEC, CEN-CENELEC and ETSI.

2 The EU should support the mutual recognition of CABs from trusted third countries, allowing cybersecurity certifications and audit results issued by these bodies to be accepted without duplicative assessments.

3 Any review of the Certification Framework must focus on objective criteria for assessing supplier risk profiles, ensuring access to services from trusted and high-performing technology providers. This includes assessing supplier risk profiles through clear risk evaluations, and establishing criteria for establishing "trusted technology provider" based on governance, risk management and transparency considerations rather than sovereignty criteria. Such approach ensures collaboration with providers that deliver highly secure solutions and implement robust technological and organizational safeguards. This is preferable to unclear and broad sovereignty requirements, which will raise costs, limit choice for European users, and hinder European competitiveness.



Artificial Intelligence Rules

The recently published AI Continent Action plan lays out a vision to support AI development and deployment in Europe. The plan rightly recognizes the central role of regulatory simplification in support of the competitiveness of the EU's AI ecosystem. **For the plan to be successful, the EU must be more ambitious with its regulatory simplification agenda on AI** and robustly engage with industry to understand businesses' needs.

Regulatory complexity and unpredictability are cited by businesses of all sizes as an obstacle to investments in AI adoption and to rolling out new AI products in the EU.[4] The AI Act will not be the only regulation applying to AI: it will coexist with other horizontal rules such as the GDPR, cyber-security regulations, the DSA, the GPSR, the new Product Liability Directive, the Copyright Directive as well as sectoral rules, e.g. on Medical Devices and Machinery. AI model and system developers, and also in some cases business deploying AI systems, will have to implement all those requirements in parallel. For the EU to successfully become an AI Continent, it is therefore essential to ensure a coherent and streamlined implementation of existing laws.

ITI has identified below the most critical challenges that exacerbate regulatory complexity in AI:

AI Act: Proportional and Pro-Innovation Implementation

→ Challenge

A pro-innovation implementation of the AI Act will be fundamental to deliver on its original objective: to create an ecosystem of excellence and trust in Europe. To achieve that, competent authorities should be equipped with the necessary tools to maintain a delicate balance between different policy objectives such as fundamental rights, competition, innovation, privacy, and security.

→ Recommendations

1 **The EU should consider postponing the application of certain requirements of the AI Act,** especially where harmonized standards are not available yet or delayed, for example by implementing a stop-the-clock mechanism similar to the one in the first omnibus package.

2 **It will be important to explicitly mandate regulators to support and safeguard innovation as part of their responsibilities outlined in the Act,** to foster an environment where technological advancements can flourish while ensuring the protection of all individual rights. This will help achieve the AI Act objectives as well as the EU's ambition in the AI Continent Action Plan.

3 **Enhance regulators' skills** by ensuring regulators have the expertise needed to oversee AI regulation and continue to invest in training for their staff – including via robust engagement with industry.

4 **Remove the possibility of disproportionate enforcement actions in the AI Act,** which disincentivize and jeopardize innovation. Especially, Article 74 (13) of the AI Act – which empowers market surveillance authorities to access source code - remains extremely concerning as it would put at risk companies' sensitive IP and undermine their investments. Access to source code contravenes widely accepted best international practices for digital trade and should therefore never be requested by market surveillance authorities.

5 **Ensure upcoming AI Act secondary legislation, guidance and other compliance tools like the Codes of Practice are targeted, proportionate, workable and in line with the EU's simplification objectives.** Robust engagement and consultation with industry must be prioritized to adequately reflect technical developments and feasibility.

AI Act: Diffusion of Enforcement Responsibilities Across Authorities

Challenge

The AI Act's enforcement structure creates significant complexity for businesses providing or deploying high-risk AI systems across multiple EU markets. While GDPR allows companies to primarily work with a single national authority where they have their main establishment, the AI Act creates a more complex structure. Companies must engage with multiple national Market Surveillance Authorities for general compliance across and within different Member States, and additionally may face oversight from the European Commission's new AI Office for matters relating to general-purpose AI models. This complex structure poses challenges for companies of all sizes who must navigate multiple regulatory interfaces.

The financial burden of this fragmented enforcement approach is substantial. Some estimates indicate that compliance costs could reach €400,000 for a single high-risk AI system, and the cost of obtaining an external conformity assessment can be up to €1 million.[5]

For innovative companies developing AI solutions across multiple EU markets, managing relationships with multiple national supervisory authorities could create significant administrative and financial barriers to innovation.

The AI Act describes several coordination mechanisms for high-risk AI systems which seem to build on product safety regulation mechanisms, such as mutual exchange of information and possible alignment of decisions. While these are positive, there is still a substantial risk of fragmentation of competencies within the same jurisdiction which creates complexity and harms legal certainty for businesses operating across jurisdictions.

Recommendation

The European Commission should implement a streamlined enforcement mechanisms whereby companies primarily interface with one single national authority while maintaining high standards of safety and fundamental rights protection.

AI and Privacy: Potential Enforcement Conflicts

→ Challenge

The AI Act and the GDPR both regulate a number of foundational elements of AI governance, including the use of data for AI training, bias monitoring, accuracy and representativity. Oversight around the application of these requirements will be shared between different national and European authorities – with diverse mandates and expertise – while some developers and deployers of AI will have to apply these requirements concurrently.

This complexity makes enforcement activities less predictable, increases risk of fragmentation and diverging interpretation among competent authorities, ultimately undermining legal certainty. In turn, it increases the difficulty of companies' compliance efforts, especially in a quickly evolving area like AI governance, and could deter investments in AI technologies in Europe. Greater certainty for downstream entities - AI users and providers - is also needed in order to meet the EU's goal of driving wider adoption of AI across the economy.

→ Recommendations

In order to mitigate risks of inconsistent enforcement of the AI Act and GDPR, we make the following recommendations for EU policymakers:

1 **Conduct a comprehensive mapping of regulatory complexities and overlaps.**

2 **Establish formal cross-regulatory coordination mechanisms, e.g., an adhoc forum of EU-level enforcement bodies and authorities.**

3 **Provide joint guidance on areas of inter-section between the AI Act and the GDPR.** For example, clarifications are required on issues related to data minimization, bias mitigation, sensitive data and accuracy (see examples below).

4 **Explore working with industry and trade associations to provide joint training programs for regulators from both the data protection and AI domains.** This will foster a shared understanding of the technical and legal complexities of AI and promote smoother collaboration.

5 **Ensure proportionality in compliance obligations** and avoid ambiguity or disproportionate/unworkable obligations, revisiting guidance where needed.

- For example, the December 2024 EDPB opinion on AI models sets complex obligations for downstream entities using AI models trained by another party to assess lawfulness of upstream processing – which could be unfeasible and serve as a barrier to adoption by EU businesses.

AI and Privacy: Data Governance Challenge Bias Mitigation and Monitoring

Challenge

The AI Act includes requirements to assess and mitigate potential biases in training, testing and validation datasets of high-risk AI systems (Article 10). Similarly, requirements for General purpose AI models with systemic risk (Article 55) require providers to assess and mitigate 'systemic risks,' which could potentially include biases. To comply with these requirements, developers will need to process data about different topics – including sensitive topics – which may be restricted under the GDPR.

Special categories of data may also be required, and Article 10(5) AI Act allows for the processing of special categories of data (as defined in the GDPR) by providers of high-risk AI systems when it is "strictly necessary for the purposes of ensuring bias monitoring, detection and correction". Article 10(5) AI Act says this processing is "subject to appropriate safeguards for the fundamental freedoms of natural persons." However, this allowance is limited to high-risk systems, creating a gap for other AI systems and, crucially, General Purpose AI (GPAI) models. In addition, the conditions for the processing of special categories of data set in Article 10(5) of the AI Act are not fully aligned with article 9 of the GDPR.

The GDPR contains restrictions and prohibitions on the processing of special category data (race, ethnicity, health data, etc.). This could create obstacles for developers' compliance with the AI Act bias mitigation requirements, since AI models need to reflect wider cultural and social contexts, including sensitive topics, to be effective, accurate, and unbiased. In addition, Article 10(5)(e) of the AI Act requires deletion of certain personal data "once the bias has been corrected," which could complicate dynamic bias detection and correction across the lifecycle of the AI system. These complexities could also hamper the development of beneficial AI use cases, especially in vital sectors like healthcare – which require processing sensitive data. The European Parliament, in a recent study, echoes these concerns, noting that "the GDPR, which imposes limits on the processing of special categories of personal data, might prove restrictive in a context dominated by the use of AI in many sectors of the economy, and faced with the mass processing of personal and non-personal data."

→ Recommendations

1 **Guidance.** Generally, it will be important to provide further guidance on the balance between bias monitoring on the one hand and use of (sensitive) personal data on the other – as well as ensuring coherent interpretations from authorities enforcing the GDPR and the AIA. Specifically, more guidance on the fulfilment of the Article 10(5) safeguards for processing special categories of data would be helpful. We would recommend simplifying Article 10(5) of the EU AI Act by aligning its conditions for the processing of sensitive data with what is required in the GDPR.

2 **Ensure access to diverse datasets for bias testing.** The AI Act's Article 10(5) allowance for special categories of personal data processing for bias mitigation should be extended to the training of all AI systems and GPAI models, not just those classified as "high-risk." Limiting this crucial provision to high-risk systems creates a counterproductive restriction. Bias detection and correction, and the development of representative, culturally relevant AI, are essential for all AI systems, regardless of their risk classification.

3 **Advocate for a pragmatic interpretation of GDPR.** A pragmatic interpretation of Article 9 of the GDPR is crucial to provide a more comprehensive framework for lawful processing of special categories of personal data in AI contexts, and ensure the development of AI models adapted to the European continent. This could be done by broadening the scope of applicable legal bases under GDPR Article 9(2), for instance exploring the relevance of "scientific research" (Article 9(2)(j)) or "substantial public interest" (Article 9(2)(g)) for AI development.

4 **Encourage the use of Privacy-Enhancing Technologies.** The EU should strongly encourage and incentivize the use of Privacy-Enhancing Technologies (PETs) to minimize privacy risks when processing special categories of personal data for AI.

AI and Privacy: Representativeness, Accuracy, and Data Minimization

Challenge

The AI Act requires developers to ensure representativeness and completeness of training, validation and testing data sets (Article 10), as well as accuracy and robustness (Article 15). To comply with these requirements, companies need to access and use large amounts of data, including data that may be considered personal. On the other hand, the principle of data minimization in Article 5 GDPR aims at limiting the processing of personal data to the minimum amount necessary. Conflicting interpretations between Data Protection Authorities and national AI Act authorities could complicate developers' compliance with the two regulations - and companies currently face uncertainty on how to reconcile these different objectives, especially in absence of further guidance.

Modern AI, especially General Purpose AI (GPAI) and Large Language Models (LLMs) require large datasets for effective training, accuracy, and to mitigate biases. With the rapid progress of AI, it is crucial to avoid making assumptions about what data is needed to train a model, how long data needs to be retained, and the impact of deleting, pseudonymizing, or anonymizing training data. At the training stage, developers can implement data minimization safeguards such as developing a responsible data collection framework and using technologies like data scrubbing and synthetic data, to the extent it is feasible. However, data minimization does not necessarily mean using small data volumes for AI training, rather proportionality is key when applying data minimization to AI.

Recommendations

1 **Authorities should take a balanced, proportionate and coordinated approach to interpreting data minimization.** As the AI Act and the GDPR are applied in parallel, authorities should ensure that developers can legally process large amounts of data at the scale needed for training modern AI models – including for the purpose of complying with the accuracy/representativeness requirements of the AI Act – without triggering unnecessary regulatory restrictions.

2 **Further joint guidance from authorities that addresses these points is needed.**

Documentation Requirements in the AI Act and GDPR

Challenge

The GDPR sets out when detailed accountability documentation is required for AI systems and models, including data protection impact assessments (DPIAs), and legitimate interest assessments. Similarly, the AI Act and its associated Code of Practice set out rules for when technical documentation, implementation of Safety and Security Frameworks, and/or continuous risk assessments are required. To minimize burdens on AI developers and ensure efficient regulatory oversight, the EU should actively seek opportunities to leverage existing GDPR compliance mechanisms to fulfill AI Act obligations, in particular relating to data – while pursuing the objectives of both regulations.

Missing this opportunity to streamline documentation obligations will create more red tape, as companies subject to both frameworks, including smaller firms, may struggle to manage multiple, overlapping documentation requirements, diverting resources from core development activities. AI Act competent authorities and DPAs may interpret similar requirements differently, leading to uncertainty and compliance challenges.

Recommendation

Documentation of personal data processing activities, risk assessments, and mitigation measures should not be unnecessarily replicated in the technical documentation of General Purpose AI (GPAI) models. The aim should be to create a streamlined and integrated approach to documentation that promotes compliance with both the AI Act and GDPR requirements without imposing unnecessary administrative costs or regulatory duplication.

Overlapping Reporting Obligations in the AI Act and GDPR

Challenge

Article 33 GDPR requires notification of data breaches to the supervisory authority within 72 hours, and, where the breach is likely to result in high risks to fundamental rights, also to the data subject (Article 34 GDPR). At the same time, Article 73 AI Act requires providers of high-risk AI systems to set up a system for continuous monitoring of their systems and to report serious incidents that may affect safety or health.

If an incident in an AI system simultan-eously results in a data breach (e.g., unauthorized access or loss of personal data), both the reporting obligations under Articles 33, 34 GDPR and incident reporting under Article 73 AI Act would apply. This could cause complex and duplicative reporting requirements.

Recommendation

These reporting requirements should be streamlined.

AI Data Processing

Challenge

The EU has identified AI as crucial to its future competitiveness. In order to enable a thriving AI ecosystem in Europe, it is important that GDPR is implemented appropriately for this purpose. A key concern in the current regime is the legal grounds for repurposing personal data for further use. When such further use is envisaged, data controllers are required to either justify it via a compatibility assessment, or revert to obtaining consent.

Recommendation

To ensure that the GDPR enables responsible AI development while maintaining high data protection standards, the full range of legal grounds under Article 6 GDPR should be available for further processing of personal data, including for AI development and innovation.

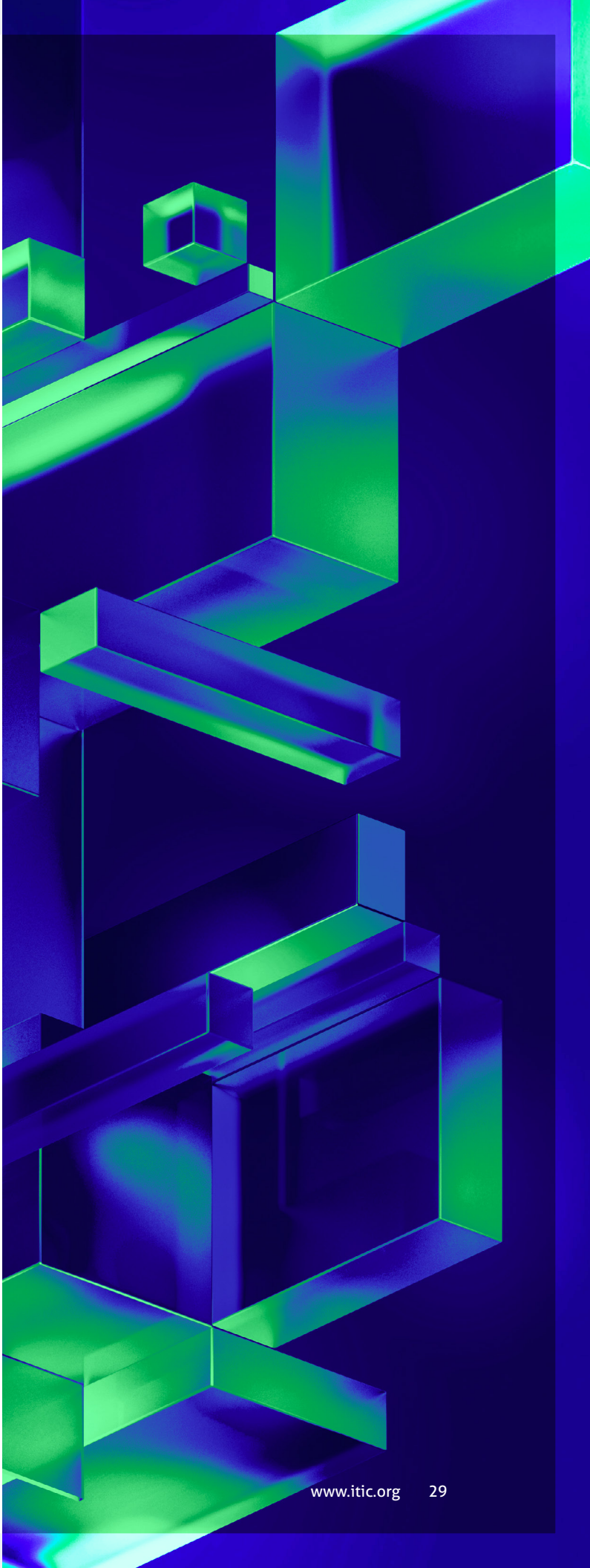
Purpose Specification

Challenge

The GDPR's purpose limitation principle (Article 5(1)(b)) mandates that personal data be collected for "specified, explicit and legitimate purposes." This principle should be interpreted in a pragmatic manner, considering that General-Purpose AI models (GPAI) are designed for a wide and evolving range of applications, many of which are unforeseen at the training stage, but are determined by the users of these systems in the deployment phase. A narrow interpretation of "specified purpose" could act as a significant barrier to GPAI development, preventing the emergence in Europe of novel and beneficial AI applications that cannot be anticipated exante.

Recommendations

A pragmatic interpretation of the GDPR is needed to consider training AI models a legitimate purpose under the GDPR, and thus provide GPAI model developers with legal certainty around the use of personal data for training AI models.



AI Act and Sectoral Regulation

Challenge

The EU AI Act will regulate a number of high-risk AI systems that are already covered by Union harmonization legislation, as listed in Annex I of the Act. The EU laws listed in Annex I cover a number of products and industrial goods, including machinery, medical devices and radio equipment, and sectoral regulations are enforced by different market surveillance authorities at national level.

Products covered by these laws will fall in the scope of the AI Act as a high-risk AI system if two conditions apply – as defined in Article 6(1) of the AI Act: 1) an AI system is a "safety component" of the product or is the product itself; and 2) the product is required to undergo third party conformity assessment under the relevant Union harmonization legislation.

Under Article 96 of the AI Act, the Commission is empowered to issue guidelines to help clarify the relation between Annex I laws and the EU AI Act, as well as to facilitate streamlined enforcement. These efforts are also being pursued under the newly established EU AI Board.

The interplay between the AI Act and these Union harmonization legislations can create significant issues for providers of AI systems, such as clarity and alignment over key definitions, role and cooperation of different enforcement authorities, availability of standards, as well as issues related to conformity assessment and certification.

Recommendations

1 **Targeted definition of safety component:** Recital 55 of the AI Act clarifies that components used solely for cybersecurity purposes should not be considered safety component, in the specific case of management and operation of critical infrastructure (as per Annex III point 2 of the AI Act).

- However, draft Commission guidelines on the interpretation of the notion of safety component for the Radio Equipment Directive (RED) noted that cybersecurity components mentioned in Articles 3(3)(d-f) of the RED could be considered safety components under the AI Act. This would potentially bring into the scope of the AI Act a large number of products, beyond the initial targeted approach of the Act.
- In order to provide clarity to operators in the market, **the Commission should clearly state that components used solely for cybersecurity purposes should not qualify as safety components under the EU AI Act.** This would be more in line with the targeted risk-based logic underpinning the AI Act.

→ Recommendations

2 Clear criteria on third party conformity assessment: As mentioned, the second condition for AI systems mentioned in Annex I to fall under the scope of the AI Act is the obligation to undergo third party conformity assessment under relevant Union harmonization legislation. In the case of the RED, the regulation does not foresee the mandatory involvement of a Notified Body for the conformity assessment of the product. Article 17 of the RED is clear about the fact that a third-party conformity assessment is mandatory only in the very limited cases where relevant harmonized standards do not exist or if the manufacturer does not use relevant harmonized standards (if they exist). Further, Article 17 lists self-assessment as the first method to demonstrate compliance with the RED.

- However, the draft Commission guidelines noted that self-assessment for certain components – including cybersecurity components- is an "opt-out" of procedural nature that does not affect the qualification of a radio equipment device as high-risk AI system. We believe this guidance is inaccurate, as it does not reflect the fact that the RED does not foresee the mandatory involvement of a Notified Body.
- If the interpretation of the Commission was confirmed and used by the Member States market surveillance authorities, it would mean that any radio equipment embedding AI cybersecurity components would be classified as a high-risk AI system. This would be not only contrary to the spirit of the legislation (risk-based approach, only a limited number of AI systems should be high risk) but also pose very serious practical problems in terms of bottleneck and market access. It would delay the placing on the EU market of new radio equipment devices significantly, to the detriment of EU consumers and businesses.

3 Alignment between AI Act and Medical Devices Regulation requirements: Medical technology companies are concerned that the AI Act's requirements may conflict and cause unclear interplay with existing regulations, particularly the **Medical Devices Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR)**, potentially causing confusion, inconsistency, and delays in innovation and bringing safe medical AI systems to patients.

- There is a need for better alignment between horizontal AI Act rules and vertical medical device regulation and standards, with clear guidance from the European Commission and consultation with industry stakeholders to ensure clear and efficient implementation.
- There should also be continued discussion on how any future MDR/IVDR revisions can be leveraged to simplify this overlapping regulatory framework for AI medical devices.
- For instance, the definition of 'substantial modification' in the AI Act needs to clearly align with existing definitions and guidance for medical device regulations to avoid conflicting requirements for AI-based medical technologies.

Data Governance and Data Privacy Rules

Data is the lifeblood of the digital economy. As the EU pursues its competitiveness objectives – and in view of the upcoming Data Union Strategy, it will be crucial to shape a clear and agile regulatory framework that incentivizes the use of data and allows companies to innovate with confidence. The current legal framework on data governance is spelled out in several pieces of legislation, including the Data Act, Data Governance Act, AI Act, DMA, ePD, GDPR and sectoral legislations. Many of these frameworks are new and overlapping, and companies are facing increasing complexity and uncertainty in applying these new rules in parallel.

The Data Act in particular creates several challenges due to unclear definitions – including for the products, services and data in scope – complex requirements, overlaps, and uncertainty over expected deliverables in support of its application (such as guidance, standards and model contracts). On top of that, its complex requirements are creating significant implementation costs and compliance burden for companies. This uncertain landscape will disincentivize investments in data innovation.

1 **An ambitious clarification and simplification of the Data Act will thus be essential** to support the emergence of an innovative data economy in Europe.

2 **In the meantime, we also recommend considering adapting the timelines for the implementation of the Data Act,** to ensure transition periods are sufficient and relevant guidelines and legal clarity are in place for businesses.

3 **The implementation timelines should also take into account the readiness of EU Member States to designate competent authorities** and adopt the rules required under Article 40 of the Data Act. These rules, relating to penalties and enforcement, are essential to legal certainty, yet they have not been published to date. Without clarity on which authorities will oversee compliance, especially in non-personal data contexts, businesses face additional uncertainty. Revised transition periods are therefore necessary not only to allow companies to operationalize their obligations, but also to give Member States the time to establish oversight structures and issue guidance to support consistent application across the EU.

We outline below several concrete areas where targeted guidance and alignment are urgently needed to reduce fragmentation, foster simplification and support effective data-driven innovation:

Clarify Definition of Data (Data Act)

Challenge

The definition of data in scope in the EU Data Act is general and unclear and companies are facing difficulties in interpreting it. In addition, companies face uncertainty over how to distinguish between different types of data falling under various legal frameworks (e.g., personal vs non-personal, product data vs related service data). This creates an overlap with existing obligations under the GDPR, the Trade Secrets Directive, and sector-specific rules, increasing the risk of inconsistent interpretations and compliance gaps. It is also unclear how derived or inferred data (e.g., such as data generated through software processing or analytics) should be treated under the scope of the Data Act. This is especially relevant for determining which data must be shared and under what conditions.

Recommendation

General and sector-specific guidance should be released, while consulting with market stakeholders. Additional guidance would also be needed on how companies should interpret key concepts such as "readily available data" or the notion of "*where relevant and technically feasible*" for the sharing of readily available data.

We further recommend that this guidance explicitly address how companies should classify different categories of data (e.g., raw, inferred) considering other applicable EU legislation, and clarify the treatment of different categories of data in the context of access and sharing obligations.

Clarify and Narrow Down the Definition of "Related Service" (Data Act)

Challenge

The Data Act's definition of **"related service"** is currently very broad. Article 2(6) of the Data Act defines a related service as essentially any digital service (other than a connectivity service) connected to a product such that without it the product would lose some function, or any service added later to enhance the product's functions. In practice, this sweeping scope could create significant **practical and legal problems** for companies. The ambiguity around what counts as a product "function" means businesses may struggle to determine which of their software offerings fall under this definition. Even EU guidance notes that identifying a product's functions is "ongoing and evolving," likely requiring further interpretation by courts. This undermines **legal certainty** by making compliance obligations unclear and unpredictable. Firms might have to invest in compliance for a wide array of services, unsure which are in scope, thereby raising compliance costs and complexity.

An overly inclusive interpretation of "related service" risks **discouraging innovation in software markets**. If virtually any software feature or application that interacts with a connected device could be deemed a "related service," companies may hesitate to develop new functionalities or third-party services for devices. They would fear triggering data-sharing obligations or other burdensome requirements in unpredictable ways, potentially chilling incentives to innovate, **which would run counter to the Data Act's aim of preserving incentives for data-driven innovation**. The broad definition could also lead to **enforcement overreach**: regulators might apply the Data Act's obligations (such as data access rights) to software features that are only tangentially related to the device's operations. This would sweep in services that are not genuinely integral to a product's use, going beyond what's necessary or proportionate. Notably, Recital 17 of the Data Act already recognizes some limits by excluding generic connectivity, power supply, and other after-market services from the "related service" category. However, beyond those obvious exclusions, the boundary remains unclear – a situation that could undermine the Data Act's objectives of **legal certainty and proportionality**.

→ Recommendations

1 **To address these concerns, ITI recommends narrowing the definition of "related service," either via harmonized implementation guidelines or via the upcoming simplification packages.** In our view, only digital services that provide essential functionalities indispensable for the device's intended use and that are directly involved in the collection or generation of data through the device's embedded components should qualify as "related services."

- This refined definition would exclude ancillary or peripheral software functionalities that do not fulfill an integral role in the device's operation. By clearly delineating truly indispensable services, policymakers would enhance legal certainty for businesses (companies can confidently identify which services are in scope) and uphold the principle of proportionality (regulatory obligations would apply only where justified by a tight link to the product's core functions and data).

2 **We also recommend that the Commission provide more illustrative examples of what qualifies as a related service and related service data.** Given the broad and evolving nature of the definition, concrete examples would help businesses better understand which services fall under scope and ensure consistency in application across industries. These examples should help distinguish between essential services and peripheral functionalities that are not integral to the device's operation, in line with the suggested refined scope (e.g., whether payment functionalities embedded within IoT devices or remote diagnostics services should be considered related services).

Guidance on Information Disclosure for Connected Products (Data Act)

Challenge

The Data Act contains obligations for the disclosure of information regarding the collection and processing of data before concluding contracts for connected products or related services (Article 3.2). Companies are obliged to provide the information to the user in a clear and comprehensible manner. The user has rights to be informed of the type, format and estimated volume of the data that the connected product is capable of generating, whether the connected product is capable of generating data continuously and in real-time, along with the data storing techniques and the intended duration of retention. The user also has rights to be informed of how they can access, retrieve or erase the data, including the technical measures, terms of use and quality of service. For related services, the obligations for disclosing information are more extensive. It is currently unclear what specific type of information needs to be provided. Due to lack of a clear picture on the minimum required information, such as "the type, format and estimated volume of product data", there is a concern that the volume and granularity of disclosed information will vary significantly between companies.

Recommendation

We recommend that the Commission issue workable and proportionate guidelines to help clarify the minimum required information to be disclosed, including sample acceptable information disclosure examples for typical types of connected products or related services.

Trade Secrets (Data Act)

Challenge

The Data Act introduces provisions on compulsory sharing of trade secrets (Article 4) if all necessary technical or organizational measures have been taken prior to the disclosure to preserve their confidentiality. This eviscerates the value of trade secrets by requiring to demonstrate the high likelihood of serious economic damages before trade secrets owners are allowed to exercise all of their protective rights. No other IP right places such a minimum bar to enforcement. It is imperative in a trade secret regime that trade secret owners have the final say as to whether or not to share information because sharing always bears a risk, and the trade secret owner is never made completely whole when a trade secret is misappropriated.

Recommendation

ITI believes that more control should be given to trade secrets holder over the sharing of trade secrets. The Commission should consider removing the compulsory sharing of trade secrets from the Data Act.

Data Portability (Data Act, DMA and GDPR)

Data Act – DMA

Challenge: Both the DMA and the Data Act aim to empower users with new data portability rights; but Article 5 of the Data Act prohibits companies designated as gatekeepers under the DMA from becoming a data recipient under the Data Act. As a result, a gatekeeper company may interpret the Data Act as requiring it to decline user requests to export data to services (including core platform services) operated by another gatekeeper company. In doing so, the exporting gatekeeper would risk non-compliance with Article 6(9) of the DMA.

Data Act – GDPR

Challenge: Article 5 of the Data Act prohibits undertakings providing core platform services designated as gatekeepers under the Digital Markets Act regulation from becoming data recipients under the Data Act. It's unclear how this ban would interact with the portability regime of the GDPR (Article 20), that does not provide for such ban, and which can thus create conflicting requirements.

Recommendation

The EU should provide clear guidance to resolve potential conflicts between the Data Act, the DMA, and the GDPR regarding data portability. Specifically, it should clarify how Article 5 of the Data Act interacts with users' rights under Article 20 of the GDPR and with obligations under Article 6(9) of the DMA, to ensure that companies can comply with all applicable frameworks without undermining users' data portability rights.

Data Act Access Rights Versus GDPR Data Subjects Rights

Challenge

Companies need to balance the access rights enshrined in the Data Act (Article 3-5 DA) with the rights of data subjects under the GDPR, such as the right to rectification, erasure and restriction of the processing of personal data (Article 16 et seq. GDPR). While the Data Act applies without prejudice to GDPR, practical challenges may arise when fulfilling access requests under the Data Act, particularly where such data includes personal data. In these cases, access must be provided in a manner that complies with the GDPR. Ensuring alignment between the two regimes can be complex, especially where there is a risk that disclosing data under the Data Act could inadvertently challenge compliance with data protection obligations.

Recommendations

Proportionate and workable guidance would be needed on this topic. Guidance should recognize the value of privacy-preserving technologies such as pseudonymization and anonymization to ensure compliance with both regulations.

Data Sharing Versus Data Minimization (Data Act, GDPR)

Challenge

There is tension between the principle of data minimization in Article 5(1)(c) GDPR, (i.e., the obligation to collect and store as little personal data as possible) and with the obligation to make data available under Article 3 of the Data Act. It is unclear in certain instances if the Data Act imposes on manufacturers the obligation to collect data where they are currently not collecting it (or identifying data as being associated with a particular individual or data subject).

For example: A company collects certain data related to the use of their connected products only for the users who volunteered to create a personal cloud account associated with the product. A minority of users use this option. To be able to link usage data with each user and comply with the Data Act, would the data holder have to make the creation of a personal account mandatory in this case? And how to reconcile this obligation with GDPR data minimization principle?

Recommendations

General guidance on this topic is needed. Specifically, we recommend that the Commission provide clarity on how to navigate this tension, offering practical advice on scenarios where the two regulations conflict. Clear frameworks should be provided to help companies understand when they can continue to apply data minimization principles (e.g., by anonymizing data where possible) and when they must collect or share data for compliance with the Data Act, without compromising the user's privacy rights. Guidance should also clarify how these obligations apply in cases where only limited personal data is involved or where technical data must be shared for operational purposes.

Making Data Available to Public Sector Bodies
(Data Act – Chapter V)

→ Challenge

Chapter V of the Data Act requires companies to make some of their data available to public sector bodies in certain circumstances. This possibility creates potential challenges, including the adequate protection of data confidentiality, as well as the intersection with companies' data protection obligations.

→ Recommendations

1 Joint guidance between Data Act authorities (for example under the European Data Innovation Board) and privacy authorities (such as within the EDPB) would be needed to clarify that compliance by a data holder with the requirements of Chapter V of the Data Act will be deemed lawful for the purposes of Article 6 of the GDPR.

2 To the extent that public disclosure of shared data is required, public sector bodies should be required to maintain a high standard of confidentiality, integrity and security of the data. While the Data Act contains some obligations in this regard, it should be made clearer that public sector bodies should:

- Not make any public disclosure about the data, or the data holder
- Provide reasonable undertakings required by the data sharer to maintain the security and integrity of shared data
- Implement technical and organizational measures at least equivalent to the data holder, and treat the data in the same manner as the data holder (i.e. in terms of criticality, confidentiality, privacy etc.)

3 We also recommend additional clarity over whether any public safety exception exists for controllers and/or data processors of public safety data, specifically as relates to data access requests.

Switching and interoperability between Data Processing Services (Data Act – Chapter VI)

→ Challenge

Chapter VI of the Data Act contains complex obligations for providers of data processing services (such as cloud) to facilitate and enable customers' switching to other services. Many of the obligations would require additional clarifications and simplification.

→ Recommendations

1 The Commission should provide more targeted and workable guidance on the definition of data processing services with examples for categorizing data services.

2 The notion of "same service type" (recital 81) should be further clarified. The Commission should issue workable guidance with examples of where two data processing services will be treated as being of 'the same service type'.

3 The Commission should provide a template for information sharing for data processing services in scope of Article 28.

4 Clarify Article 29(2) - Provide clarity on what is meant by charging "reduced switching charges" from 11 January 2024 to January 2027.

5 The possibility for the Commission to impose harmonized standards or common specifications under Articles 33 and 35 should be removed. Instead, consistent with current Article 33(11), the Commission should issue non-binding guidelines where necessary that focus on duly identified interoperability obstacles, allowing standards and other industry initiatives to evolve alongside technologies and market demand.

6 Streamline contractual requirements where a data processing service provider is already obliged to make public disclosures of information (i.e., Article 25 of the Data Act on contractual terms vs Article 26 disclosure.).

Data Transfers Rules
(Data Act, Data Governance Act, GDPR)

Challenge

The GDPR contains rules for international transfers of personal data (Chapter 5). On the other hand, Article 32 of the Data Act mandates providers of cloud services to take measures to prevent international transfer or governmental access to non-personal data when this would create a conflict with EU or national law. Under the Data Act, companies would need to put in place technical, legal, and organizational measures for international transfers of non-personal data. Similar requirements also apply for certain data in the scope of the Data Governance Act (DGA).

Most businesses process mixed data sets including personal and non-personal data, and currently apply the safeguards of the GDPR to all transfers. It is currently not clear how the enforcement of the Data Act will interact with the GDPR and whether additional compliance measures for transfers of non-personal data will be required.

Recommendations

The Data Act must be updated to reflect that where a provider's systems store personal data, any valid transfer mechanism under GDPR should suffice for compliance, without the duplication of obligations under the Data Act.

As such, **we propose to remove Articles 32 and 28(1) of the Data Act to avoid these overlaps and unnecessary complexity**. In the same vein, **Chapter VII of the Data Governance Act on International Access and Transfer should be withdrawn** in favor of the international data transfer regime under GDPR.

International Data Transfers (GDPR)

Challenge

International data transfers are critical to economic growth and innovation. To support trusted and secure global data flows, there is a need for more flexible approaches to Chapter V GDPR transfer mechanisms that maintain high standards of protection while recognizing diverse and legitimate legal and cultural approaches to privacy. The essential equivalence standard by which third country data protection laws and practices are assessed in order to establish adequacy of protection of transferred personal data presents challenges. In practice, only a handful of countries have been able to qualify for an "adequacy decision" that requires an almost identical legal regime to be established in the third country. Outside these limited decisions, companies are not able to rely on their own guarantees for protecting data but must assess and be accountable for the commercial, national security and law enforcement regimes in the third country, over which they have no agency. Beyond the EU legal framework, this is also creating issues in third countries which use GDPR as a blueprint and adopt similar transfer regimes without the equivalent privacy culture or institutions to enable and enforce it. At the same time, these efforts often place a significant burden on organizations without a clear or proportionate contribution to overall data protection outcomes. In addition, the requirement for each controller/provider to basically do an adequacy assessment of each jurisdiction by itself places a disproportionate burden on all companies (including SME's) and could be replaced by an industry-wide mechanism.

Recommendations

The EU needs to lead the way in promoting flexible and interoperable rules to ensure that companies have access to different avenues and mechanisms to move data between jurisdictions securely, providing value for consumers and certainty for business. We recommend fostering a multilateral approach to personal data transfers mechanisms by referencing international, principle-based standards, such as the OECD Privacy Guidelines and Global Cross Border Privacy Rules.

This would ensure a strong baseline of protection, while introducing a degree of flexibility that allows for mutual recognition of data privacy regimes around the world, as opposed to unilateral, rigid and prescriptive assessments that require each jurisdiction in turn to match every provision of the GDPR. In addition, the GDPR regime could favor some practical adjustments e.g. on the adequacy assessments to help both SME and larger companies being compliant.

Personal Data and Pseudonymization

Challenge

While GDPR is intended to be a risk-based framework, in practice, the treatment of data by companies is largely determined by what the data is, rather than the purpose for which it is processed. This is particularly evident in the broad and expanding concept of "personal data," which captures a wide range of information regardless of the likelihood of harm or identifiability in context. This creates significant legal uncertainty and can discourage the use of technical measures that could meaningfully enhance privacy and data security. Pseudonymized data is a key example. While it significantly limits the ability to link data to individuals, it is afforded little regulatory flexibility compared to anonymized data. As a result, the framework does not provide sufficient incentives for companies to use privacy-enhancing techniques, even where they meaningfully reduce risks to individuals.

Recommendations

To better align the GDPR with its risk-based objectives and support privacy-preserving innovation, the regulation should provide more flexibility in the treatment of pseudonymous data. Specifically:

- Companies that implement strong technical and organizational safeguards should be afforded greater flexibility to process pseudonymized data closer to the approach taken with anonymous data.
- A more realistic standard of the likelihood of deidentification should be introduced.

ePrivacy Directive

Challenge

The current ePrivacy Directive is an outdated law. First adopted in 2002 and updated last in 2009, many of the provisions are obsolete, such as billing, caller ID, call forwarding and subscriber directory. More fundamentally, the Directive is no longer fit for purpose and creates an unlevel playing field without adding any clear added value. It was adopted prior to the GDPR, which already governs the processing of personal data processed in this sector. As such, it includes provisions on security and confidentiality that are already arguably established in the more recent law. In addition, it creates a convoluted and restricted set of grounds for processing communications, traffic and location data, and accessing terminal equipment, that would be better served by the general grounds for processing data in Article 6 of GDPR. Finally, the protracted and unsuccessful legislative process and withdrawal of the ePrivacy Regulation proposal demonstrates that applying a sector specific data privacy regime to the electronic communications is not straightforward.

Recommendation

The European Commission should remove the ePrivacy Directive from the EU acquis and national transpositions should be repealed. Specifically, the GDPR should serve as the horizontal legal framework governing the processing of personal data in the electronic communications sector, including for cookies, as well as traffic and location data.

Sustainability Rules

In the current EU mandate, it is crucial for policymakers to ensure that sustainability legislation does not hinder the uptake of digital technologies, just as digital legislation should not create barriers or being a disincentive for companies to deploy technological solutions that support decarbonization and climate objectives. Companies are navigating overlapping EU-level tech and sustainability regulations, national frameworks, and inconsistencies from the divergent implementation across Member States. These challenges might be compounded by varying timelines for international treaties and EU legislative measures, which can lead to confusion and hinder smooth cross-border operations.

Digitizing Consumer and Regulatory Information

Challenge

EU regulations require companies to provide physical regulatory information on waste sorting, safety, and environmental considerations in multiple locations, often leading to redundancy, overlaps, and inefficiencies. This includes placing information on the product itself, in printed documentation within the product's packaging and on the product packaging, all in the national language of the respective market.

While these requirements aim to ensure consumer awareness and compliance, they result in ex-cessive paper use, logistical complexity, and higher compliance costs. Moreover, requirements are spread over numerous legislations under the New Legislative Framework (NLF), including on market surveillance, ecodesign and energy labelling, and established through consumers' rights and waste requirements, making it difficult for businesses to navigate the regulatory environment efficiently.

Recommendations

To address this challenge, we encourage the Commission to take concrete steps to accelerate the digitization of regulatory information. This can be achieved by allowing digital formats as a legally recognized alternative to physical formats. Providing consumer and regulatory information digitally would not only reduce paper waste, transport weight, and ink usage but also increase accessibility for consumers by enabling real-time updates and improved usability of information. The Commission should also undertake targeted measures, including:

1 **Clarifying the interrelation between the Digital Product Passport (DPP) and existing databases such as the European Product Registry for Energy Labels (EPREL).** While the DPP is expected to become a standard requirement, exceptions are mentioned for cases where existing digital systems meet the necessary criteria. However, the relationship between EPREL and ESPR remains unclear. It is uncertain whether the reliance on EPREL constitutes a deviation from ESPR of EPREL will be adapted to align with ESPR principles. ITI members face significantly different operational and setup requirements when preparing for the DPP compared to uploading information into EPREL. Further clarity is needed on how these systems will interact and what specific obligations will apply to industry.

2 **Ensuring the Commission's support for an actionable use of the Digital Product Passport across sustainability-related legislation.** Old and new legislations requiring additional product information for end-users, consumers, or market surveillance authorities should leverage the DPP as a unified digital tool. For example, in the Green Claims Directive, a single data carrier such as the DPP should be the mechanism for providing transparent and easily accessible information to consumers. In this regard, we welcome amendment 81 by the Parliament in its first reading position (Article 5.6.1), as well as the Council's amended Article 5.8, which explicitly references the DPP in the legal text.

3 **However, while we support the broader use of the DPP for the above-mentioned reasons, we encourage the Commission to remain attentive to potential implementation challenges.** First, any additional requirements on material content needs to be carefully assessed for products already covered by product-specific regulations. In particular, requiring material data for modular networking equipment is not feasible as the DPP does not support updates following upgrades, repairs, or refurbishments.

Second, legislation should refrain from prescribing the specific physical placement of the DPP on products or packaging. Mandating its position - for instance, alongside a green claim – could lead to legal confusion and practical barriers, particularly for small-format packaging. Such constraints risk undermining the flexibility needed for effective DPP implementation across diverse product categories and use cases.

Stronger Alignment Between Policies to Favor Simplified Verification Procedures

→ Challenge

The lack of alignment between different legislative instruments often leads to duplication of efforts and legal uncertainty. A key example is the interaction between the Green Claims Directive proposal and the Corporate Sustainability Reporting Directive (CSRD). As it stands, companies are required to disclose sustainability-related information under CSRD, yet these disclosures are not recognized as substantiated claims under the Green Claims Directive. Similarly, the upcoming Code of Conduct for sustainable telecommunications networks risks repeating these inefficiencies if it is not designed in coherence with existing frameworks.

→ Recommendations

1 The information disclosed in CSRD reports should be recognized as substantiated claims under the Green Claims Directive. Such alignment would reduce unnecessary duplication, simplify verification processes, and provide companies with a more predictable regulatory framework.

2 The European Commission should ensure the upcoming Code of Conduct for sustainable telecommunications networks is firmly aligned with existing legislative framework, including the CSRD and the EU Taxonomy. This principle of alignment should be extended to other regulatory frameworks to address similar inefficiencies.

Breaking Silos and Adopting a Coordinated Approach

Challenge

One of the major barriers to regulatory efficiency is the discrepancy between international agreements, such as the Basel Convention, and EU initiatives, such as the Waste Shipment Regulation (WSR). These frameworks often have differing timelines and inconsistent application, leading to uncertainty and market disruption.

This lack of coordination is particularly problematic for sectors like waste and second-use materials, as regulatory misalignment hinders the objectives of a circular economy. Companies engaged in cross-border trade of waste and second-use materials face unnecessary complexity due to inconsistent interpretation and implementation of rules across Member States. While the European Commission has demonstrated some willingness to address such concerns in the context of the mentioned WSR, continued efforts are needed to harmonize rules and ensure a functioning Single Market for waste.

Recommendation

To address these challenges, the Commission should prioritize a synchronized approach across different legislative initiatives. Aligning implementation timelines of international agreements and EU regulations is essential to reducing market fragmentation and providing businesses with a predictable regulatory landscape.

Moreover, regulatory coherence should be a guiding principle within the upcoming Circular Economy Act, and the revision of the Waste of Electric and Electronic Equipment (WEEE) Directive presents an opportunity to reinforce this approach by ensuring consistency with other circular economy-related legislation.

Waste Electrical and Electronic Equipment Directive (WEEE)

Challenges

This revision must be effectively managed to minimize overlaps with other circular economy-related legislation, ensuring clarity, and simplification. In particular:

- Definitions may play a crucial role in simplifying or complicating the legislative framework. For clarity, it is important to maintain consistency with the Basel Convention and uphold the current distinction between e-waste and items shipped for repair or reuse, as outlined in the WEEE Directive Annex VI, Article 2(a). Eliminating this distinction could create unnecessary barriers for companies aiming to achieve circularity, as repairing or reusing products would become more complex.
- The shipment of used electronic products across Member States should be smoother and more efficient. Currently, some Member states require proof that a device shipped for reuse has been tested as functional, leading to inconsistencies in the implementation of Article 2, Annex VI. These variations create hurdles and inefficiencies.
- Addressing regulatory barriers that disincentivize the purchase of refurbished products should be a priority. Under the current system, when a product is first placed on the EU market, producers pay a fee to contribute to e-waste management. However, if that same product is later reintroduced as a refurbished item, even with only cosmetic changes, in another EU country, the producer is required to pay the fee again, as there is no EU-wide system recognizing refurbished products across borders. The absence of a single market for e-waste creates additional costs and discourages investment in refurbishment, ultimately hindering circularity goals.

Recommendations

To optimize the WEEE Directive via the upcoming revision, the following measures should be adopted:

1 Maintain the distinction between e-waste and products shipped for repair and reuse to avoid unnecessary regulatory burdens on circularity efforts.

2 Streamline the shipment of used electronic products by harmonizing functional testing requirements and ensuring consistent implementation of Annex VI across Member States.

3 Establish an EU-wide mechanism to prevent double taxation on refurbished products, facilitating the creation of a single market for refurbished goods and stimulating demand for sustainable consumption.

4 Favor regulations over directives wherever possible to provide greater legal certainty and minimize disparities in national implementation.

Substances of Concern in Products (SCIP) Reporting under the Revised Waste Framework Directive

Challenges

Article 9(1)(i) of the revised Waste Framework Directive (WFD) sets out that any supplier of an Article must provide certain information on substances of concern in that Article to ECHA as of January 5, 2021. While the objective of improving transparency on hazardous substances in the product lifecycle is advised, practical implementation of SCIP reporting has raised several challenges for industry stakeholders, particularly OEMs in the ICT sector.

Under the current requirements, 247 substances must be tracked and reported at the lowest Article level. This granularity significantly increases the complexity and resource intensity of SCIP compliance. OEMs rely heavily on supplier-provided data, but many suppliers lack adequate knowledge of chemical legislations, leading to frequent inefficiencies – such as the over-declaration of SVHCs like - and repeated review cycles that delay compliance efforts.

Many suppliers outsource reporting to third parties with limited expertise. and often serve multiple OEMs with the same components across the ICT industry. Although SCIP reporting is mandatory for all component manufacturers, weak enforcement has pushed much of the burden onto OEMs, which result to be responsible for component and article reporting.

The biannual update of the European Chemical Agency's (ECHA) candidate list further complicates compliance as the absence of a grandfathering mechanism requires companies to retroactively amend SCIP submissions for existing products in the ECHA database. Unlike the automotive industry, where OEMs use the same material compliance tool (MD system), the ICT lacks standardized systems, hindering efficient data sharing and consistency for SCIP filings. Additional challenges include technical limitations of the SCIP portal – such as delayed product listings and limited support – which disrupt workflows and risk customer dissatisfaction.

Despite these significant demands, there is little evidence that SCIP data is meaningfully used by recyclers or consumers, raising concerns about the proportionality and effectiveness of the current reporting framework.

→ Recommendations

To address these challenges and enhance the effectiveness of SCIP reporting while ensuring a more balanced compliance burden across the value chain, we recommend the following:

1 **Simplify reporting requirements** by focusing on simplification, integration, and risk-based reporting. Reduce redundancy by allowing reporting at a higher article level where appropriate.

2 **Adopt the grandfathering mechanism** that exempts products already on the market from retroactive SCIP reporting obligations when new substances are added to the candidate list. This would streamline compliance processes and reduce the burden of rereporting, therefore allowing companies to focus on new products and substances.

3 **Integrate SCIP with Digital Product Passport (DPP)** to streamline regulatory reporting and potentially replace SCIP with a more comprehensive tool.

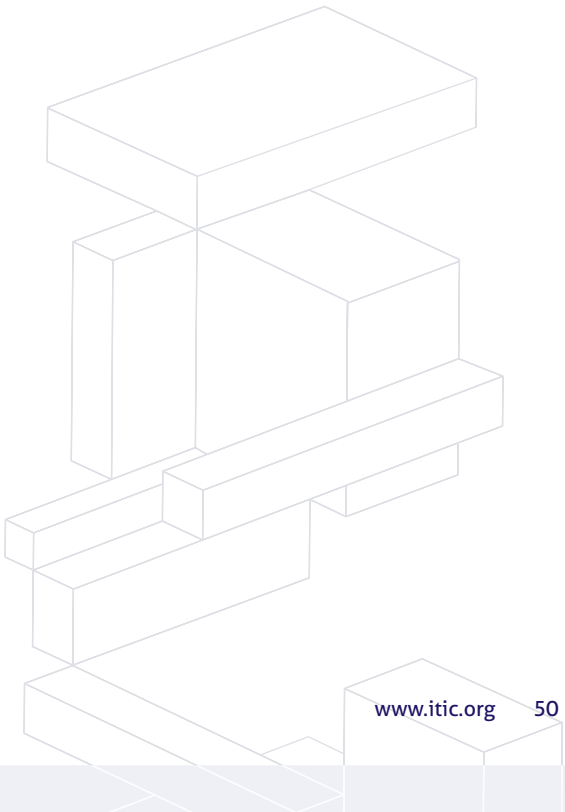
4 **Strengthen monitoring and enforcement** of SCIP reporting requirements by component suppliers. If suppliers were held more accountable for their reporting duties, the burden on OEMs could be significantly reduced and compliance levels across the supply chain would improve.

5 **Enhance supplier training and support** by leveraging the educational role of ECHA which should develop comprehensive training programs, including workshops and webinars, to keep suppliers informed of regulations and best practices.

6 **Establish a centralized compliance platform for ICT** to help standardize the reporting process and reduce duplicated efforts among OEMs.

7 **Improve ECHA Portal functionality** such as user interface, performance, and responsiveness of the SCIP database to minimize delays and customer dissatisfaction.

8 **Leverage existing compliance data** from other regulatory frameworks such as REACH to fulfil SCIP requirements.



Data Centers: Bottlenecks for Development and Decarbonization

Challenges

In addition to facing some of the highest energy prices globally and dealing with issues related to energy availability and unstable grids, data centers in the EU are also burdened by lengthy, complex, and often unpredictable permitting procedures. These processes vary significantly across Member States, making the EU a less attractive destination for new data center investments. Furthermore, licensing requirements for implementing decarbonization projects – such as heat recovery initiatives – can be excessively bureaucratic, delaying or even blocking sustainable projects. Several companies have reported being penalized not due to a lack of willingness or technical capacity, but because of structural and regulatory hurdles that prevent them from reusing energy or connecting to local heat networks.

Moreover, the Energy Efficiency Energy Efficiency Directive (EED) Delegated Act and related regulatory frameworks introduce additional challenges, particularly for colocation data center operators. Current requirements oblige operators to report on information - such as IT efficiency metrics and data traffic - that belongs to their customers and is not under their direct control. This creates legal and operational uncertainties and raises issues around data ownership and confidentiality. For example, the obligation to report incoming and outgoing data traffic volumes (T IN and T OUT, Annex II 3.c and 3.d) is particularly problematic in bare metal or colocation environments, where data flows are managed by end customers. In such cases, operators often lack the technical means or legal authority to accurately measure or disclose this information. Furthermore, specific reporting obligations, such as incoming and outgoing data traffic volumes or ICT capacity for servers (CSERV) and storage equipment (CSTOR), are commercially sensitive, extremely difficult to measure, and, in many cases, not directly related to sustainability or energy efficiency objectives.

In particular, the ICT capacity for servers (CSERV), as defined in the Delegated Regulation, lacks a standardized calculation method, which creates confusion and inconsistency in its reporting. The regulation refers to 'performance in the active state' as the required value but does not define how this should be calculated. This ambiguity places a disproportionate burden on data center operators, especially enterprise and colocation facilities, who may not have access to such data, or for whom the underlying data belongs to customers. Additionally, the required metrics may imply a level of insight and control over hosted IT workloads that operators simply do not possess.

Several industry actors, including ITI and The Green Grid (TGG), have acknowledged this gap and proposed the adoption of 'PerfCPU' (maximum CPU performance) as a standardized metric to represent CSERV in a consistent, technically feasible manner. They are also developing a practical reporting tool tailored for enterprise and colocation data centers, intended to simplify compliance and reduce the reporting burden while aligning with the intent of the EED. As a result, the current framework risks creating disproportionate administrative obligations without yielding meaningful sustainability outcomes. Instead, it may undermine the EU's attractiveness for data center development and hamper the very digital and green transitions the EED seeks to support.

→ Recommendations

We invite the Commission to assess the existing EED Delegated Act on data centers and the upcoming rating scheme in light of the objectives set out in the AI Continent Action Plan, the roadmap for digitalization and AI in the energy sector as well as the upcoming Cloud and AI Development Act. Special attention should be given to ensuring that reporting obligations are relevant, technically feasible, and respectful of the division of responsibilities between colocation data center operators and their customers. Specifically, ITI recommends:

1 **Reviewing and adjusting reporting requirements** to ensure that data points such as in-coming and outgoing data traffic, ICT capacity for servers (CSERV), and storage equipment (CSTOR) are either removed or made voluntary where appropriate, as they are not directly tied to energy efficiency outcomes and may require disclosure of customer-owned commercial data.

2 **Clarifying the definition and calculation methodology for CSERV,** including by supporting the proposal put forward by ITI and The Green Grid (TGG) to adopt 'PerfCPU' as a standardized metric. This clarification should be formally reflected in the Delegated Regulation, enabling consistent and reliable reporting across the EU.

3 **Promoting adoption of practical compliance tools,** such as the reporting tool developed by ITI/TGG, which is specifically designed to support enterprise and colocation data centers in meeting CSERV reporting obligations.

4 **Continuing close collaboration with expert groups,** including TGG, to refine and validate energy and performance metrics and ensure future amendments are informed by operational realities and technical feasibility.

5 **Developing a robust and practical rating scheme** that streamlines reporting obligations and focuses on metrics that genuinely reflect a facility's energy performance, while minimizing administrative overhead and protecting customer confidentiality.

On the decarbonization front, we recommend that the Commission facilitate and incentivize waste heat recovery by streamlining permitting processes for connecting data centers to district heating networks. Policies should address both the supply and demand sides, ensuring that off-takers are available and viable, and that data center operators are not penalized when they are unable to distribute heat when external constraints prevent them from distributing recovered heat. Simplifying and harmonizing permitting across Member States will be critical to unlock the full potential of data centers.

References

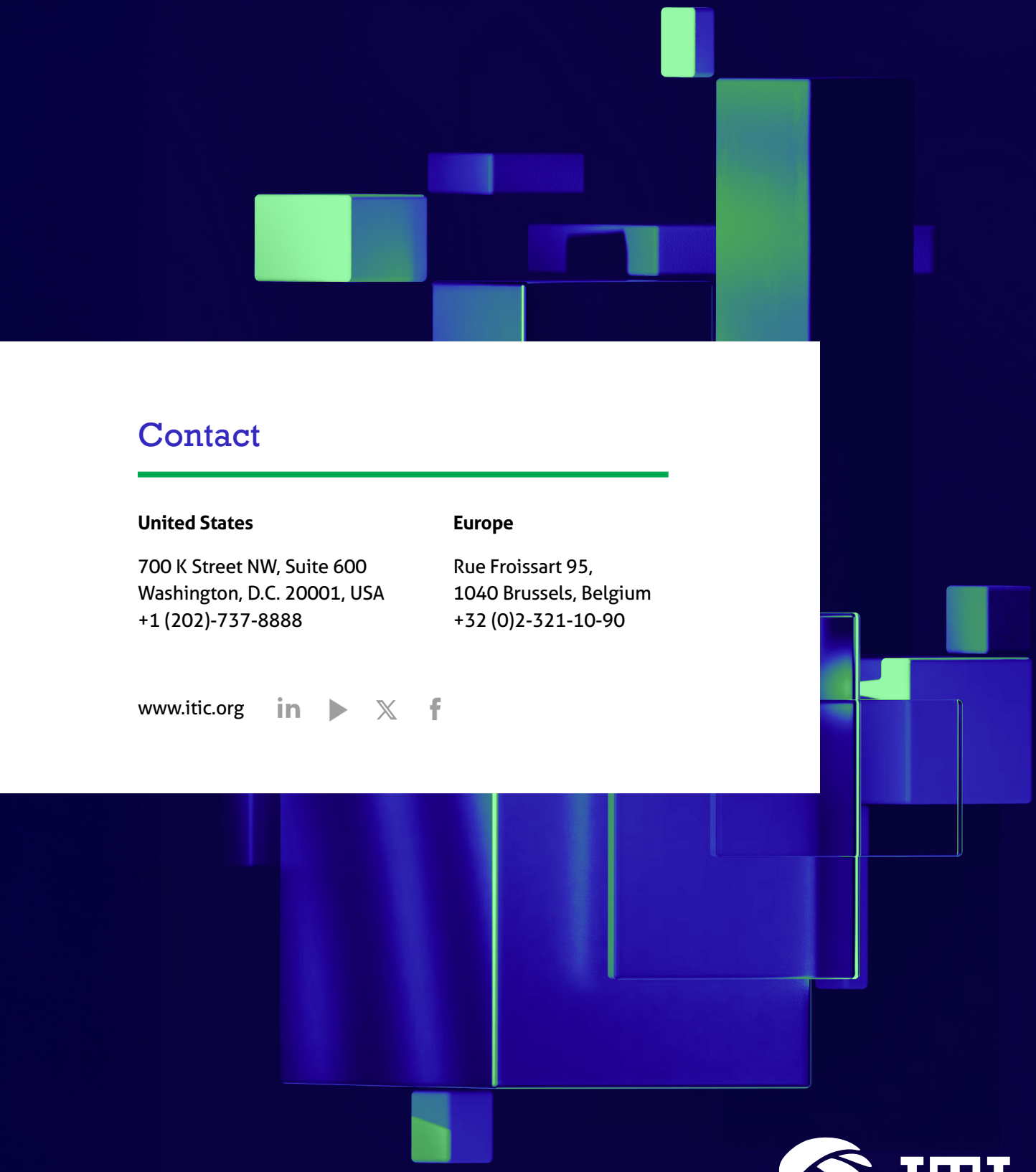
1 Draghi, M. (2024). The Future of European Competitiveness—A Competitiveness Strategy for Europe. https://commission.europa.eu/document/97e481fd-2dc3-412d-be4c-f152a8232961_en

2 A simpler and faster Europe – European Commission Communication. https://commission.europa.eu/document/download/8556fc33-48a3-4a96-94e8-8ecacef1ea18_en?filename=250201_Simplification_Communication_en.pdf

3 For more information: Last year, the tech sector already provided recommendations to pursue better and simplified regulation, increase the EU's attractiveness for investments, and boost Europe's competi-tiveness in the current EU mandate. ITI's recommendations were complemented by targeted proposals on areas like Artificial Intelligence, Cybersecurity and Sustainability.

4 See for example: Strand Partners, Unlocking Europe's AI Potential in the Digital Decade: https://www.unlockingeuropesaipotential.com/_files/ugd/c4ce6f_ecf071799e4c4eba80113648d2b1090b.pdf

5 Mueller, Benjamin. "How Much Will the Artificial Intelligence Act Cost Europe?" Information Technology and Innovation Foundation, July 26, 2021. https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe/.



Contact

United States

700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 (202)-737-8888

Europe

Rue Froissart 95,
1040 Brussels, Belgium
+32 (0)2-321-10-90

www.itic.org

ITI
Promoting Innovation Worldwide