AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Digital Omnibus

Priorities for simplifying the EU's digital rules

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €4 trillion in 2023, directly supports more than 4.6 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 56, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Table of Contents

Executive summary

Regulatory burdens are a top concern for businesses in Europe, with 84% of American Chamber of Commerce to the EU (AmCham EU) members citing them as a primary barrier. Without bold action, the EU risks losing business confidence and much-needed investment, jeopardising its economic and sustainability goals.

This paper outlines AmCham EU's principles and priorities for simplifying the EU digital rulebook to foster growth and a robust Digital Single Market, ahead of the European Commission's publication of a digital simplification package in late 2025.

A Digital Simplification package must help to build a Digital Single Market, ensure greater harmonisation among EU Member States' laws, remove unnecessary hurdles for businesses and eliminate inefficiencies that hinder their competitiveness. Equally, the package must embrace commercial and technological openness and reject protectionism, ensure a level playing field and find a better balance between horizontal and sectoral regulation when developing digital rules.

This paper proposes recommendations in the following four areas for action:

Cybersecurity: The proliferation of EU cyber regulations has led to significant complexity and overlapping requirements, often diverting resources from actual security enhancement to compliance. To improve EU cyber resilience, it is essential to increase the use of the main establishment principle, to streamline reporting through a single, harmonised regime, align taxonomy and ensure confidentiality. The Simplification Package must also simplify the Cyber Resilience Act, drive consistency of the NIS2 Directive across Member States and improve the Cybersecurity Act's certification framework to be more transparent, reliant on international standards and technical in nature.

Data/privacy: A Data Union Strategy is essential to streamline existing data rules, creating a simplified framework for data sharing. This involves clarifying the Data Act (international transfers, trade secrets) and the Data Governance Act (international transfers), optimising the GDPR (international data transfers, pseudonymisation, GDPR/AI Act interplay) and modernising the ePrivacy Directive by deleting obsolete provisions and moving remaining obligations to other frameworks.

Connectivity: The EU's telecom regulatory framework (EECC) requires enhanced legal coherence and certainty. The EECC must streamline requirements by tailoring them for consumer protection concerns, simplifying notifications and avoiding duplicative regulation. The 'Country of Origin' principle in the Commission's White Paper on how to master Europe's digital infrastructure needs would go against the goal of simplification and should be rejected.

Artificial Intelligence: The EU AI Office's central role in guiding AI Act implementation must be affirmed to ensure the secondary legislation is coherent, cohesive and in line with the text of the Act. Timely consultations with sufficient stakeholder response time are crucial. Formally confirming the retraction of the AI Liability Directive proposal is also vital to simplify compliance. The applicability of high-risk requirements under the AI Act should be delayed until 12 months after relevant harmonised standards are published, to ensure legal certainty, consistent enforcement and sufficient time for companies to adapt.

By adopting these recommendations, the EU can significantly reduce administrative burdens, foster a more predictable and practical regulatory environment and unlock Europe's full potential for investment, innovation and competitiveness in the digital economy.

Overview of digital simplification recommendations by policy area and legislation

Cybersecurity

Subtopic	Key simplification suggestions
Cybersecurity reporting	Replace fragmented reporting (GDPR, NIS2, DORA, CRA, etc.) with a single regime, reporting to one EU entity; avoid weekend reporting and overreporting of minor incidents.
Main establishment	Expand the use of the 'main establishment' principle for streamlined compliance across cybersecurity laws.
Reporting templates	Create one harmonised EU-wide incident notification template; avoid low-impact incident reporting and reduce unnecessary triaging.
Conformity assessments	Introduce a centralised conformity assessment framework to avoid inconsistent requirements under NIS2, DORA, CRA.
Single national entry point	Designate computer security incident response teams (CSIRTs) as the single entry point under NIS2 and CRA for harmonised, secure and efficient reporting.
Taxonomy alignment	Align terms like 'significant' and 'severe' incident; harmonise definitions for when an organisation is 'aware' of an incident.
Confidentiality	Strengthen technical standards to protect sensitive information in notifications under NIS2, CRA, GDPR and DORA.
Cyber Resilience Act (CRA)	Exclude sectors like finance already covered by DORA; define terms like 'remote data processing' clearly; simplify and delay vulnerability reporting; avoid rushed or unclear implementation.
NIS2 Directive	Harmonise transposition timelines, audit requirements, thresholds and reporting deadlines; address jurisdictional conflicts and overlaps with DORA.
Cybersecurity Act review	Empower ENISA with additional resources; ensure ENISA aligns with international standards, consults stakeholders transparently and avoids sovereignty-based criteria in certification schemes.

Data/privacy

Subtopic	Key simplification suggestions
Data Act	Remove overlapping international transfer rules; narrow definition of 'connected product'; eliminate forced trade secret sharing; clarify data portability vs. GDPR/DMA; streamline B2G access under 'exceptional need'.
Data Governance Act	Replace Chapter VII with the GDPR's international transfers regime to ensure alignment and ensure free data flows.
GDPR	Embed proportionality more clearly in Article 24; simplify documentation under accountability; streamline international data transfer regime; support use of pseudonymised data; clarify overlap with AI Act.
ePrivacy Directive	Delete outdated rules (eg on billing, caller ID); migrate remaining parts into GDPR or future legislation; reform cookie consent rules to reduce banner fatigue and allow low-risk exemptions.
Data Union Strategy	Align all data laws (Data Act, GDPR, ePrivacy, DGA) into a clear, predictable and interoperable regime to foster secure and scalable data sharing across the EU.

Connectivity

Subtopic	Key simplification suggestions
European Electronic Communications Code (EECC)	Tailor consumer protection rules for business contracts; simplify and harmonise notification and reporting procedures; avoid duplicative regulations with GDPR, e-privacy and cybersecurity obligations; reject the 'Country of Origin' principle as it fragments the market.

Artificial Intelligence

Subtopic	Key simplification suggestions
AI Act	Empower the AI Office to lead coherent implementation; delay sector-specific rules until AI Act is fully operational; ensure clear guidance for sectors like healthcare; create R&D exemptions; clarify 'putting into use' definition; delay the applicability of high-risk requirements under the AI Act until 12 months after relevant harmonised standards are published,

Subtopic	Key simplification suggestions
	to ensure legal certainty, consistent enforcement and sufficient time for companies to adapt.
AI Liability Directive	Officially retract the proposal to avoid overlapping and confusing obligations on AI developers and users.

1. Introduction

Regulatory simplification is critical for enhancing Europe's competitiveness for business. President von der Leyen stated her own commitment to regulatory simplification and reducing administrative burdens as part of the Commission's broader competitiveness agenda. This focus was sorely needed since the suite of legislation that the first von der Leyen Commission delivered across multiple policy areas was excessive in breadth and depth. As an illustration, the Commission must process over 900 implementation acts in the coming legislative period.[1] These pieces of legislation placed multiple overlapping new burdens on businesses, resulting in uncertainty about their implementation and business compliance.

Excessive regulatory burdens have become a major deterrent to business confidence and attracting investment in Europe: 84% of AmCham EU member companies rank reducing regulatory burdens as a top priority for policymakers to support business operations in Europe. Simplification must mean streamlining, and in many cases reducing, the scale of the burden on businesses to put Europe back on a course to growth and to improve its competitiveness.

Importantly, simplification in digital policy should ensure the EU's digital goals are met in a manner that is predictable and practical for companies.

Although the Commission is not expected to issue the Digital Package or the results of the Fitness Check on the digital acquis before late 2025, it is widely understood that the package will focus on:

- The simplification of cybersecurity legislation, including the review of the Cybersecurity Act;
- A Data Union strategy to ensure organisations can share data seamlessly and at scale;
- Targeted simplification of the broader digital acquis to reflect businesses' needs and constraints.

During this critical simplification process, it is vital that the EU includes US business voices in these discussions. US investment in Europe exceeded €4 trillion in 2023 and directly supports over 4.6 million jobs across the EU. US companies are often found to have the highest quality, most technologically advanced and most innovative solutions. The companies producing these solutions have operated in Europe for decades and employ European workforces to build European products and innovations that are vital for Europe's critical infrastructure and supply chains. If the EU wants to unlock the potential of its industry and workers, while supporting its strategic objectives in the digital space, it should ensure that the digital acquis supports European workers and researchers to continue their innovation regardless of the parentage of their employer.

[1] Hoppe T., 'Green Deal: 900 implementation acts pending – industry warns of "tsunami"', Table. Briefings. 6 December 2024, https://table.media/en/europe/feature/green-deal-900-implementation-acts-pending-industry-warns-of-tsunami/.

Case in point:

AmCham EU member companies across different sectors and market segments all face significant compliance burdens stemming from the EU digital acquis related to both the cost of compliance and scale and feasibility of compliance.

For one AmCham EU member company, the implementation of the Digital Operational Resilience Act (DORA) represented a multi-year compliance effort, involving over 60 internal stakeholders across more than 20 cross-functional teams. Up to 10 dedicated meetings per week were needed to coordinate workstreams. The regulation triggered deep operational changes, including the creation of a new threat-led penetration testing team and a central audit programme.

Identifying in-scope services and critical suppliers proved especially complex, requiring company-wide input and extensive supplier engagement. Flowing down new terms to suppliers and collecting supplier information to support client compliance obligations involved intense legal and procurement coordination. Notably, DORA requires supplier information far beyond current industry norms – including data such as supplier business continuity plans.

The EU Data Act is creating similarly high compliance demands, requiring massive cross-functional efforts across legal, product, compliance, cybersecurity, development and government affairs teams.

Companies are also facing escalating compliance costs due to overlapping NIS2 and ESG regulations. These include substantial legal advisory and policy monitoring costs, along with the need for extensive compliance documentation and audits. Businesses are also investing in technology upgrades and security systems to meet NIS2 requirements, while simultaneously addressing the growing demands of ESG reporting. This often requires hiring additional compliance teams and implementing training programmes for staff. Moreover, companies must manage data mapping, data protection and incident response processes to comply with both frameworks. The burden extends to conducting risk assessments, Data Protection Impact Assessments (DPIAs) and producing detailed reports.

For one AmCham EU member company, managing NIS2 compliance involves an internal working group of multiple teams, which has already spent several months mapping internal security policies against the directive. Audit costs for NIS2 alone could exceed €9 million across all 27 EU Member States, with ISO27001 certification fees potentially reaching €1.6 million.

These compliance demands divert substantial resources away from core business priorities, compelling companies to allocate significant budgets to audits and risk management – ultimately limiting their ability to invest in innovation, R&D and future competitiveness.

With these stakes in mind, this paper provides recommendations that, if adopted, would ensure that the scope of the Digital Omnibus package delivers on improving Europe's competitiveness and meeting its strategic objectives.

Simplification principles in digital policy

- **Reinforce the Digital Single Market**: The Single Market for digital services and technologies is still far from being a reality and the EU is behind schedule in meeting its 2030 Digital Decade targets. To this end, the EU must create a Digital Single Market where people can benefit from the free movement of online services, goods and data and foster the uptake and scale-up of new technologies through investment, innovation and entrepreneurship.
- **Legislative harmonisation**: The EU must ensure greater harmonisation among EU Member States' laws. This could mean favouring Regulations over Directives, introducing broadly-scoped main establishment laws in Directives, increasing the use of sectoral *lex specialis* provisions in cross-sector legislation, prohibiting gold-plating and overlap of parallel legislation or ensuring one-stop-shop or mutual recognition of auditing, conformity, registration, reporting and other enforcement processes. The Commission should also consider enhancing its Technical Regulation Information System (TRIS) to better identify and correct barriers to the single market.
- **Streamline digital regulation**: The EU must streamline its regulatory environment for digital industries, removing unnecessary hurdles for businesses and eliminating inefficiencies that hinder their competitiveness and which create an uneven playing field. Legislative withdrawals such as the AI Liability Directive are positive steps forward, but the EU needs to do more to ensure businesses can focus their investments on innovation and growth – not compliance.
- **Prioritise implementation and enforcement**: Before introducing any new directives or regulations that are similar or parallel to existing regulatory frameworks, the Commission should take stock of whether existing frameworks are being properly enforced and implemented, with all necessary guidelines in place.
- **Embrace openness and stakeholder consultation**: The EU must build and maintain international partnerships and reject protectionism, as openness and market access drive prosperity and allow European citizens' access to best-in-class technologies already available in other markets around the world. EU policymakers must also enhance the way in which they interact with stakeholders when developing and implementing policy, boosting transparency and collaboration with all interested parties, including European businesses with US parentage.
- **Find a better balance between horizontal and sectoral regulation in the development of digital rules**: The EU has a committed policymaking tradition of recognising sectoral regulators to develop sector-specific rules. This has been demonstrated across several sectors including medicine and financial services. However, the EU also adopts several horizontal regulatory frameworks, such as NIS, AI Act, GDPR or more recently the Cyber Resilience Act, whereby all sectors are in-scope of the requirements, despite existing sector rules applying to the end-to-end digital infrastructure of businesses. This has resulted in an inconsistent patchwork of horizontal rules on the one hand (NIS2, CRA) and sector-specific for heavily regulated sectors on the other hand (DORA, EU network code on cybersecurity in the electricity sector, EECC/5G cyber toolbox), which causes substantial implementation and interpretation challenges for

businesses and discourages further investment in the EU. The EU should remove sectors from the scope of the horizontal rules if they face duplicative sectoral regulation.

- **Remove provisions at national level:** When provisions or whole laws are removed 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 by the Court of Justice of the EU. Therefore, proactive clauses should be included that require Member States to remove equivalent provisions in national law and not reintroduce comparable provisions.

2. Specific areas of action

2.1. Cybersecurity

Key points:

- Establish a single, harmonised reporting regime across GDPR, NIS2, DORA, CRA and other regulations as a matter of urgency.
- Expand the main establishment principle to streamline jurisdiction and reduce duplicative compliance.
- Introduce a single EU-wide reporting template and align thresholds to avoid overreporting.
- Clarify and simplify the Cyber Resilience Act implementation, scope and vulnerability disclosure process.
- Harmonise audit requirements and security standards under NIS2; encourage mutual recognition across Member States.
- Empower ENISA with additional resources and ensure certification frameworks reference international standards.

2.1.1. Cybersecurity reporting

The Commission has indicated its objective to use the digital simplification package to address complexity in cybersecurity reporting, as part of its goal of reducing reporting requirements by at least 25% (35% for SMEs). The proliferation of inconsistent cybersecurity reporting requirements in recent years – creating unnecessary and duplicative burdens for businesses – has made this a necessary step. The General Data Protection Regulation (GDPR), Network and Information Systems Directive 2 (NIS2), NIS2 Implementing Regulation, Cyber Resilience Act (CRA), ePrivacy Directive (ePD) and Digital Operational Resilience Act (DORA) all contain different thresholds, timelines and content for incident reports. Businesses are equally in-scope across a variety of different Acts, resulting in numerous similar reports for the same incident. The content and number of data fields in EU reporting is more complicated than any other equivalent jurisdiction.

This complexity has important implications for business investment and, ultimately, the EU's cyber resilience. Multiple reports, across differing receiving bodies, serve limited productive value to businesses and does not improve risk management practices or the ability to remediate incidents. In fact, these reporting demands can ultimately cause businesses to move resources away from mitigation, response and recovery from the incident itself to compliance. This redirection of cybersecurity expertise, which is nonetheless required for incident reporting compliance, weakens the EU's cyber resilience. Larger organisations, such as those within the technology and financial sectors, will be able to resource teams, but this will reduce the availability of skilled cybersecurity professionals for less resourced organisations and sectors.

To make cybersecurity reporting simpler, businesses should be subject to a single reporting regime whereby they report incidents under one format, to one EU entity, which can cascade information to adjacent regulators as necessary. Additionally, primary supervisors or authorities, such as financial regulators for financial institutions or market surveillance authorities for technology providers, should take precedence and reflect the only regime a business should be expected to comply with.

Main establishment

Increasing the use of and consistent criteria for the main establishment principle for EU cybersecurity regulations would streamline reporting by allowing companies to submit reports done under the GDPR, NIS2, DORA, CRA and other rules to the EU Member State of their main establishment.

This is already the case for certain services under the NIS2 Directive, but this must be expanded to cover more sectors – such as public electronic communications services – which are often offered by vendors on a cross-border basis within the EU. It must be acknowledged, though, that some sectors, such as financial services, are unlikely to be able to adopt such an approach.

Reporting templates

Together with a more consistent use of the main establishment principle, the Commission should adopt one harmonised template for cybersecurity and data breach notifications across the EU, replacing the various templates that exist today. This process should involve various authorities, including the European Union Agency for Cybersecurity (ENISA), national cybersecurity agencies, European supervisory authorities under DORA and data protection authorities under the GDPR.

Reporting templates should enable businesses to remediate incidents. Reporting thresholds should be sufficiently high to ensure that only incidents that could have an impact on the wider economy or disrupt the operations of the business are reported. Detailed templates covering low-level incidents require businesses to triage all incidents according to the EU's criteria, with certain businesses triaging approximately 20-100 incidents for every single reportable event. Triaging serves no risk management function, creates cybersecurity skills shortages, removes investment from productive activity and increases the cost of doing business in the EU.

The current EU approach is burdensome and often results in overreporting in comparison to other jurisdictions. There are several common classification criteria proposed by the EU that drive overreporting of less impactful incidents that do not require authority intervention. The following classification criteria, for example, could be removed across NIS2, GDPR, ePD, DORA and CRA reporting:

- **Recurring incidents**: An incident is considered recurring when the same root cause leads to two repeated incidents across a six-month period and, together, they breach reporting

thresholds. The root cause criteria within all EU incident reporting rules are high-level and often do not correlate (eg a change management related incident could be the result of human error, infrastructure implementation or a supplier issue, despite being all in scope for a recurring incident). There is a high degree of administrative burden comparing non-significant incidents within firms and the policy objective is unclear.

- **Geographic spread**: Incident reporting regimes require firms to determine if an incident has occurred across two Member States, which is a criterion under DORA. This occurs with a high degree of frequency due to transactions occurring across jurisdictions and the locations of branches and IT infrastructure being spread across Member States. The spread has little to no correlation to the significance of the IT incident and drives high reporting numbers.
- **Weekend reporting**: EU incident regimes require firms to report over the weekend or within a certain timeframe on the Monday morning. This has limited logic, with authorities regularly not working over the weekend period, portals not being open to input and no new information being produced in relation to the incident (eg market impact for trading does not occur outside trading hours). This causes an unnecessary burden on firms with limited policy upside. Highly significant incidents will be remediated and face authority intervention even without a weekend reporting requirement.
- **Costs:** Incident reporting often requires businesses to subjectively quantify costs of an individual cybersecurity or operational incident to a highly prescriptive degree. DORA, for instance, requires a business to quantify the staff salary cost for reporting teams, which are 24/7 and undertake triage activities for all reporting requirements (eg a financial institution can be in scope of 100+ reporting rules globally). Attributing costs to staff salaries for incident response is complex and subjective, often bearing little relevance to the incident's severity or providing tangible information for regulators. Economic costs are also required early in reporting phases and are beyond the capabilities to analyse in a short period. Cost requirements should be simplified and allow businesses to concentrate on remediation.

Conformity assessments

A major challenge in the EU cybersecurity landscape is the lack of harmonisation in conformity assessment processes and procedures across different cybersecurity legislations, such as NIS2, DORA and the CRA. This fragmentation creates administrative burdens for businesses, especially when they operate across multiple EU Member States. To address this, the EU should establish a centralised conformity assessment framework, ensuring that all cybersecurity legislation follows uniform assessment methodologies and mutual recognition of certifications across Member States.

Single national entry point for reporting

The national notification entry points under the NIS2 Directive should serve as key points of contact under other legislation that also requires notifications. To ensure harmonisation with the CRA, the NIS2 Directive should prioritise reporting to national Computer Security Incident Response Teams (CSIRTs) over the competent authorities, potentially through a single, secure, EU-wide intake portal. The financial sector, in addition, should report based on DORA and should not be expected to widen reporting requirements to CSIRTs. This approach would improve trust and streamline the overall information-sharing framework.

Taxonomy alignment

NIS2's use of 'significant incidents' differs from the CRA's definition of 'severe incident', creating inconsistencies. While they cover incidents in different domains (provision of the services versus build environment of the manufacturer), the CRA should also set geographical limits that focus on impact within the EU, as found under NIS2.

Additionally, all cybersecurity regulations must be aligned on what it means to 'become aware' of the incident or vulnerability. All cybersecurity regulations should be aligned with the EDPB's guidelines on personal data breach notifications and the 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.

Firms subject to reporting requirements have experienced inconsistencies across Member States regarding their interpretation of incident reporting requirements. Certain Member States have yet to implement reporting structures that allow for firms to comply effectively with the reporting rules that are in effect. The EU should not introduce reporting rules for firms when Member States have yet to ensure they are harmonised in interpretation or have not implemented appropriate portals and security practices to allow reporting to take place. Businesses have experienced Member States enforcing reporting requirements that are no longer applicable, refusals to recognise reports being submitted outside of EU Member States (businesses have 24/7 reporting teams that operate globally and therefore may submit outside of the EU) and requirements to re-submit each reporting stage across every submission. All cause substantial administrative burden.

Confidentiality

Confidentiality of the sensitive information shared in notifications under the NIS2 Directive, CRA, GDPR, ePD and DORA is essential. Member States should work on technical requirements for the reporting channels and ensure a common high level of security in the government entities that are assigned as reporting entry points.

2.1.2. Cyber Resilience Act

Throughout the Cyber Resilience Act's development, the business community expressed concern over the Act's increasing level of complexity and burden on businesses, and the final text has proven itself to be unclear and unnecessarily complex in several areas.

A significant proportion of the Cyber Resilience Act will be predicated on further requirements being developed during the implementation phase. This includes detailed guidance on the role of separate sectoral regulation, the interpretation of remote data processing, substantial reconfiguration of products and guidance on its Essential Cybersecurity Requirements. All respective future guidance materially impacts the compliance programme of all businesses and serves to create highly uncertain implementation challenges and timelines. The EU should consider speeding up the production of guidance or forbearance for businesses following the implementation timeline. In general, the EU should reconsider digital regulation where extensive levels of guidance are produced during the implementation period. This runs counter to effective policymaking and creates unnecessary implementation challenges for businesses operating in the EU.

Scope

One of the CRA's primary areas of confusion and complexity is the definition of remote data processing and accompanying recitals related to providers of cloud solutions. Such providers appear to be excluded from the CRA but are then brought back into the regulation if they offer applications, which in today's mobile-first world, is often a requirement. This overlap duplicates requirements for cloud solutions providers, making compliance with both the NIS2 and CRA requirements complex and costly. This is particularly challenging for emerging European cloud providers with fewer resources. Accordingly, providers of cloud solutions that are in scope of NIS2 should be explicitly and fully excluded from the CRA.

The CRA is the first product legislation to be applied across other regulated sectors and intangible services that, historically, have been removed from scope. The Act has provided no guidance to sectors that are supervised separately from market surveillance authorities and do not recognise the terminology, enforcement or basis for the Act. The financial sector, for instance, is already subject to extensive cybersecurity and ICT risk management regulation and supervision. These rules have been comprehensively updated through DORA, which entered into force in January 2025. Without substantial guidance or a sectoral exemption, it is unclear how the Act will apply to intangible services. Equally, the Act has introduced significant uncertainty regarding enforcement, with market surveillance authorities able to remove all banking applications or debit/credit cards from the market of a Member State without any interaction with financial authorities. Adding a new regulator for financial services is an unclear objective of the Act and serves to create a complicated and overly burdensome regulatory environment for financial services. Financial services should be removed from scope via Article 2(5), confirming that DORA constitutes a higher level of protection than the CRA.

Timing of implementing guidance

The CRA contains a complex set of product safety and resilience requirements that hardware and software vendors will need to implement into their product development lifecycles once the requirements are final. These lifecycles often take multiple years from the time a product is designed until it is fully developed for release on the market. Time is therefore truly of the essence for vendors to receive definitive guidance on topics that are key to interpreting CRA requirements.

While the final overall implementation deadline for performing conformity assessments is 11 December 2027, many of the most crucial requirements are not yet fully defined, pending further interpretative guidance from the Commission. The timing of release of key implementing guidance – urgently needed by industry – remains within the EU Commission's control. This includes the guidance referenced in Article 26 of the CRA concerning (i) the overall scope of CRA, (ii) the application of support periods to various categories of products with digital elements and (iii) the concept of substantial modification. The Commission must publish drafts of the guidance for industry consultation and finalise such guidance as soon as possible. Only then will vendors have sufficient time to incorporate the guidance, given the long lead times needed to incorporate requirements into the development of their products.

Vulnerability reporting

Article 14 and related recitals must be amended to prevent premature disclosure of previously unknown vulnerabilities that are not already patched or otherwise addressed (ie a 'zero-day vulnerability'). Instead, reporting should take place only after mitigating or corrective actions have occurred.

In the case of a zero-day vulnerability for which the vendor is working to develop and release a software security update or guidance to address the vulnerability, software vendors should be allowed reasonable time (before being forced to disclose the vulnerabilities to third parties) to develop and release the update or guidance to customers on how to better protect themselves until the update is released. If not, vendors who value transparency will often feel forced to rush out untested updates or guidance simply to provide public disclosure before being forced to selectively disclose the vulnerability to a subset of governments with mandatory disclosure laws – a result that would concern many of the vendors' customers. The net result would likely involve vendors rushing to provide security updates that either do not fully address the underlying issue or, given the rush to market, contain further bugs that can be exploited or result in widespread availability 'outages' of software. This would be a worse software security outcome for users within the EU.

Requiring software vendors to disclose 'zero-day vulnerabilities' to EU authorities before having sufficient time to address them can have global implications. Such a policy may prompt other countries – including countries that do not share EU values and may use the information to conduct cyber-attacks – to adopt similar laws. The result would be global fragmentation of such requirements that would further contribute to a worse outcome for the security of customers.

Establishing a central repository of vulnerabilities and security guidance that customers and governments – as the CRA intends – can easily refer to, offers clear value. Indeed, other governments maintain such lists (such as the U.S. government's National Vulnerability Database) which have been of great value to the security community. However, we are concerned that collecting information on zero-day vulnerabilities into any one database will result in a treasure trove for malicious actors. Such a database will almost certainly be a target for hackers looking to exploit those yet-unpatched vulnerabilities across critical infrastructure systems. Instead, the Commission, via ENISA, should chart known exploited vulnerabilities that companies should prioritise patching to protect their infrastructure and data, analogous to the U.S. Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (KEV) Catalog.

Trademark and branding and substantial modification

According to Article 21, the Obligations of Manufacturers would apply to businesses if the placing of the product with digital elements includes their trademarks or name. Applying higher requirements based on whether a 'product with digital elements' includes a company's name introduces significant uncertainty for businesses. For instance, the 'critical' products annex includes payment cards, which include the trademark of the financial institution and the payment scheme. It is unclear where accountability lies and how the Act can be applied.

A proportionate and risk-based approach to guidance on product modification is much needed. White-labelling is a critical avenue by which market participants in the EU can embed digitisation in their offerings and participate in the wider economy. This is critical to non-technology providers where participants will make significant, but predominantly cosmetic, changes to a product, even though this will not negate the safeguards of the original manufacturer. A substantial modification should only come into effect if the modification constitutes a material change in the risk of the product that was not considered or foreseen in the initial risk assessment of the product by the distributor or manufacturer. A disproportionate approach would upend how white-labelling occurs in the EU, resulting in a highly complex implementation with confusing outcomes for consumers.

2.1.3. NIS2 Directive

The NIS2 Directive represents a crucial step towards enhanced cybersecurity within the EU. However, in recent months, we have seen EU Member States transpose the Directive in different ways, resulting in a fragmented regulatory landscape and operational and compliance challenges for pan-European service providers. Specific areas of concern include discrepancies in reporting obligations, definitions of scope and security audit requirements and the interplay with sector-specific regulations[2].

The Commission must act to harmonise the Directive's implementation, leverage international standards and foster mutual recognition of audits to reduce duplication and complexity.

Scope

Early transposition efforts have included different definitions for which sectors and entities would fall within the scope of the Directive. The Hungarian transposition, for instance, adds some (sub)sectors to the original NIS2 sectors, while the Czech Republic transposition demonstrates divergence in its definition of 'important' and 'essential' entities, potentially leading to discrepancies in which organisations fall under the scope of the regulation. The Commission should therefore provide guidance to Member States on the scope of the NIS2 Directive to streamline its transposition, including through a more harmonised timeline.

Compliance phase-in periods

Different Member States have differing phase-in periods for when the requirements of their NIS2 transposition laws become effective. Some Member States are phasing the requirements' deadlines. An example of this is the Italian law transposing the NIS2 Directive, which allows for 18 months and nine months respectively for obligations to comply with cybersecurity risk management measures and incident reporting obligations. On the other hand, Belgian law transposing the NIS2 Directive effectively gives covered entities 30 months from 18 October 2024 (ie until 18 April 2027) to implement the cybersecurity risk management measures, though does not contain a phase-in period for incident reporting. Other EU member countries do not have explicit phase-in periods for either meeting cybersecurity risk management measures or incident reporting obligations. The Commission should provide guidance to Member States urging them to introduce phase-in periods of NIS2 requirements in general, especially given the diverging approaches Member States are taking to implement these requirements. Regulated entities should be given reasonable time to understand and prepare for these diverging requirements before complying with them.

Reporting deadlines and thresholds

The NIS2 legislation has an explicit requirement to notify the CSIRT or the competent authority within 24 hours of becoming aware of a 'significant incident' or to report the 'significant incident' to the CSIRT or competent authority within 72 hours of becoming aware of it. Nevertheless, some Member States have not fully reflected this requirement in their national transpositions. In Hungary and Croatia, for example, cybersecurity incidents must be reported 'without delay'. This divergence risks undermining the harmonised approach intended by the NIS2.

As stated previously, national notification entry points under the NIS2 Directive should serve as key points of contact under other legislation that requires notifications. To ensure harmonisation with the

[2] https://www.amchameu.eu/system/files/position_papers/amchameu_fragmented_implementation_nis2_transposition_final_0.pdf

CRA, the NIS2 Directive should prioritise reporting to national CSIRTs over the competent authorities. This approach would also improve trust and streamline the overall information-sharing framework and ensure consistency across EU Member States.

In addition, different Member States are proposing different reporting thresholds in their transposing legislation. For example, Article 23(1) of EU NIS2 requires service providers to report significant incidents to customers: 'Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are **likely to** adversely affect the provision of those services'. However, the draft Dutch implementation of the law contains very similar language but replaces 'likely to' with 'may' as follows: 'Where appropriate, the essential entity or important entity shall without undue delay notify recipients of its services of significant incidents that **may** adversely affect the provision of those services'. The use of 'may' broadens the scope of reportable incidents, adds uncertainty in how to make such a determination and creates divergence of requirements for companies that offer services across multiple EU jurisdictions, such as providers of cross-border public electronic communications services.

To prevent unnecessary added compliance costs with no commensurate benefit to EU security, these incident reporting requirements must be harmonised to the extent they impact providers of cross-border services across multiple EU jurisdictions.

Security measures

Member States are adopting diverging security control frameworks to prove compliance. These approaches include referencing standards in supplementary materials, developing national frameworks that blend elements from multiple standards and, in certain instances, considering compliance with specific standards (eg ISO 27001).

The Commission and ENISA should work with Member States to develop a harmonised security control framework, which would also apply to the services in scope of the NIS2 Implementing Regulation. Ideally, a globally recognised framework should be adopted. If this is not feasible, the framework should, at a minimum, draw upon existing globally recognised frameworks.

Security requirements and audits

Particularly concerning are the divergent security audits that entities need to follow in each jurisdiction, as these are the most time-consuming and costly, with no obvious cybersecurity benefit. Even with the main establishment principle, the NIS2 Directive illustrates how inconsistencies among Member States balloon to potentially prohibitive costs.

For example, companies offering public electronic communications services (PECS) throughout the EU are subject to 27 separate laws purportedly covering the same topic, but with inconsistent results.

In many cases, while each country requests its own audit, this audit would take place against the same set of central processes within a company, as systems are centralised for the EU (meaning the same processes are audited 27 different times). Member States should consider mutual recognition of audits to avoid undue bureaucracy, multiplication of efforts and high fees.

In Hungary, for example, companies will have to carry out periodic audits by one of four third-party auditors approved by the Hungarian government to Hungarian standards, which will be shared with the Hungarian government. In Belgium, companies will have to carry out a different audit to Belgian government-approved standards (either Belgium's CyFun standard or ISO 27001) on a periodic basis.

The Commission and ENISA should work with Member States to develop a mutual recognition policy. Such a policy would accept audits that are conducted in other Member States in accordance with that country's EU NIS2 transposition law. It would also accept a pan-European audit and certification as a presumption of conformity at national level and recognise audits from third countries, provided mutual recognition of conformity assessment is in place.

In addition, Article 32(2) of NIS2 directs Member States to ensure that competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to a variety of inspections and audits, including targeted security audits carried out by an independent body or competent authority. Principles of mutual recognition and acceptance of audits should also apply to these targeted audits to avoid having duplicative audits of the same service provided across borders.

Overlap with DORA

ICT service providers for financial entities could face additional or conflicting cybersecurity requirements because of overlapping regulations from the NIS2 Directive and the Digital Operational Resilience Act (DORA). This is a particular concern when an entity is designated as both a critical ICT third-party service provider under DORA and an essential or important entity under NIS2, leading to oversight from multiple authorities, including a 'lead overseer' under DORA. The Commission should strive to harmonise these regulations, ensuring that compliance with NIS2 automatically equates to compliance with DORA.

Jurisdiction

The concept of main establishment allows entities operating across multiple Member States to streamline their reporting and compliance. At the same time, it helps avoid reporting and supervision overlaps, thus leveraging government resources more effectively.

However, during the transposition of NIS2 nationally, some Member States chose to challenge the principle of main establishment. This is, for example, the case with the Italian National Cybersecurity Agency's interpretation of the law and the Slovak NIS2 transposition law. Requesting entities to register and report to Member States outside of their main establishment is against the principles of the NIS2 Directive and will result in further fragmentation.

As noted, the concept of main establishment should be extended to entities in other sectors if they have operations in more than two Member States. Entities should also be allowed to leverage their main establishment under NIS2 as their jurisdiction for other cybersecurity legislative pieces, like the Cyber Resilience Act.

2.1.4. Cybersecurity Act Review

Role of ENISA

ENISA has undergone a massive transformation from a small agency to being recognised in the EU and globally as the EU's agency for cybersecurity. However, it has not yet maximised its potential. ENISA should take a more proactive role that scrutinises EU policy to ensure the EU promotes cybersecurity more broadly.

ENISA has the legal mandate to cooperate with the private sector and therefore receives support from the Advisory Group and from the Stakeholder Cybersecurity Certification Group (SCCG). However, ENISA can do more to enhance its stakeholder engagement, allowing the SCCG to directly assist its work programme or the Rolling Work Programme for Cybersecurity. Stakeholders must also be able to provide direct input to existing networks like the CSIRTs Network or the NIS Cooperation Group. This will ensure that ENISA and national cyber authorities have input from industry before decisions are made. ENISA should devote additional resources – for example, a full unit – to public-private cooperation.

Cybersecurity Certification Framework

The Cybersecurity Act review must also improve the Cybersecurity Certification Framework, in particular by addressing the issues which emerged during the work on the draft Cloud Certification Scheme.

Development of schemes

The Commission, in several instances, did not follow the process described in the Certification Framework to request ENISA to work on a given scheme. Instead, it has circumvented this process and tasked ENISA with developing a scheme without consulting the European Cybersecurity Certification Group (ECCG) or Stakeholder Cybersecurity Certification Group (SCCG) due to the Union Rolling Work Programme for European cybersecurity certification. The European Commission must adhere to established processes in the Certification Framework or propose amendments to them.

Transparency and stakeholder consultation on draft schemes

Several versions of the draft EUCS scheme, including drafts that added sovereignty requirements, were not formally consulted with the SCCG or externally with stakeholders. ENISA may not be able to consult every time that a new draft is issued. However, it must consult them when important changes are proposed, such as the mentioned sovereignty requirements. The Cybersecurity Act review must increase transparency and stakeholder consultation on draft schemes.

Reference to international standards

The EU needs a cybersecurity certification scheme that leverages existing and internationally recognised cybersecurity standards to foster global interoperability and to reduce unnecessary compliance burdens for businesses. Draft schemes often lacked reference to international standards, such as those developed by International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) JTC1 SC27 (ISO/IEC 27000 series), leading to ambiguous terminology and requirements not grounded in industry best practices and standards. Any updates to the Certification Framework must ensure that it fully leverages existing international standards.

Technical-based schemes

A Certification Framework that produces technical, standards-based schemes achieved through open consultations and excluding non-technical criteria would serve the interest of businesses, citizens and the European economy as a whole and speed up the approval process. Any review of the Certification Framework must refrain from including non-technical measures, such as discriminatory sovereignty requirements, which will only raise costs, limit choice for European users and damage the EU's competitiveness.

2.2. Data

Key points:

- Align the Data Act with GDPR to eliminate overlaps on international transfers and trade secret disclosures.
- Withdraw Chapter VII of the Data Governance Act to reduce barriers to international data flows.
- Clarify and reinforce GDPR's proportionality and accountability principles to ease operational burdens.
- Remove obsolete parts of the ePrivacy Directive and consolidate rules into GDPR or new frameworks.
- Implement a Data Union Strategy to unify the fragmented EU data landscape and promote scalable data sharing.

2.2.1. Data Union Strategy

The EU has more opportunity to grow its data economy. The costs and complexity businesses face, stemming from new layers of data regulation, hinder growth. The objective of the Data Union Strategy would help the EU unlock its potential as a data economy by addressing existing data rules to ensure a simplified, clear and coherent legal framework for businesses to share data seamlessly and at scale, while respecting high privacy and security standards.

The Commission must utilise the Data Union Strategy as a simplification tool to streamline existing rules on data.

2.2.2. Data Act

EU policymakers' priority should be to achieve clarity in the Data Act and address ambiguities raised by stakeholders across all sectors. There are several areas in which the Data Act could be better aligned with other legislation.

International data transfers

The Data Act introduces new requirements for data transfers that go above and beyond GDPR's established framework for personal data transfers. This is particularly challenging for companies handling mixed data sets, as it creates impediments to companies' ability to transfer non-personal data, much like the restriction the GDPR imposes on personal data, and results in administrative burdens that outweigh the actual risks. That is why the Data Act must be updated to reflect the notion that where a provider's systems store personal data, any valid data transfer mechanism under the GDPR should suffice for compliance, without the duplication of obligations under the Data Act. Removing Articles 32 and 28(1) would get rid of these overlaps and reduce unnecessary complexity.

Scope of 'connected product'

The definition of 'connected product' in the Data Act is excessively broad, potentially encompassing a vast range of hardware and associated digital services. This extensive scope risks creating clear compliance burdens, particularly on manufacturers of products where data generation is incidental rather than a primary function, or for products already well-understood by consumers, such as personal computers, tablets and smartphones.

To foster innovation and reduce unnecessary regulatory overhead, the Commission should consider narrowing this definition. A more focused scope, potentially excluding devices whose primary function is not the storing, processing, or transmission of data on behalf of others, or at least clarifying the status of common consumer electronics like smartphones, would significantly simplify compliance and allow businesses to focus resources on core Data Act objectives for relevant industrial data.

Information disclosure for connected product data collection

There is uncertainty and lack of clarity in the Data Act when it comes to the 'type, the format and estimated volume' of product data that needs to be disclosed at minimum. The Commission should issue guidelines on the minimum required information to be disclosed, including examples of typical types of connected products or related services.

Trade secrets

The Data Act introduces provisions on compulsory sharing of trade secrets (Article 4) when all necessary technical or organisational measures have been taken prior to the disclosure to preserve their confidentiality. If the trade secret owner can demonstrate that it will suffer serious economic damage, it can refuse to provide access to the data, but the data user/requestor can challenge the decision.

Compulsory sharing of trade secrets should be removed from the Data Act. It eviscerates the value of trade secrets by placing a minimum bar of damages before trade secrets owners are allowed to exercise all 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 to share information. Sharing always bears a risk, and the trade secret owner is never made completely whole when a trade secret is misappropriated.

If, after the trade secret owner and the requestor have negotiated protections for the subject trade secret, the trade secret owner can still demonstrate that it will suffer serious economic damage from the disclosure, then trade secrets should be excluded from data sharing. Perhaps an additional obligation can be imposed on the trade secret holder to give notice that information is withheld. There could be a mechanism to object, but any costs associated with an objection should be borne by the data requestor or by the 'loser' in an administrative proceeding concerning the information. However, ultimately, the best scenario is for trade secrets not to be shared at all and for this provision to be removed from the Data Act.

Data portability complexity

The interaction between the Data Act, GDPR and Digital Markets Act (DMA) creates complexity around data portability. For example, if a European company collects Internet of Things (IoT) data, they must follow the GDPR's data minimisation and portability obligations. However, the Data Act introduces

certain restrictions and obligations to make data available – for example, for portability towards DMA gatekeepers. Companies require further guidance to balance this complexity.

Further, for data generated using connected products or related services by consumers, Chapter II of the Data Act imposes obligations that largely duplicate GDPR rights (eg access under Article 15 GDPR, portability under Article 20 GDPR) and transparency requirements (Article 13/14 GDPR). This overlap is burdensome for businesses and confusing for consumers. Consideration should be given to explicitly carving out such consumer-generated data from the scope of Chapter II of the Data Act. This would recognise that the GDPR already provides a robust and familiar framework for consumer data portability and access, thereby streamlining compliance for businesses.

In addition, the Data Act, GDPR and DMA are enforced by different authorities, both at the EU and Member State levels. This could lead to diverging interpretations and legal uncertainty for companies. The Commission should address the interplay between these regulations and align Article 37 (10-13) with the GDPR to reduce administrative overlap and ease compliance burdens for companies.

Interoperability of data processing services

Under Article 35 of the Data Act on the interoperability of data processing services, the EC may adopt standards and/or specifications through a delegated act. The European Commission is planning to adopt a first set of standards/common specifications already by September 2025. However, it is pertinent that this initiative is preceded by thorough stakeholder consultation and not as a goal in itself. The EC should only impose mandatory requirements based on identified specific cases of genuine interoperability obstacles that cannot be solved by industry. This will ensure mandatory standards deliver real value rather than create unnecessary complexity, including through hampering innovation, creating security concerns and adding administrative compliance burdens, in particular for start-ups and SMEs. Absent such evidence, the EC should refrain from acting or limiting such actions to recommended standards/specifications only.

B2G Data Sharing Obligations

Chapter V of the Data Act introduces novel and broadly defined obligations for data holders to make data available to public sector bodies in cases of 'exceptional need.' This lack of definition of this new concept creates legal uncertainty and potential operational burdens. To enhance clarity and manageability, the obligation to share data under Article 14 should be strictly confined to 'product data' and 'related service data' as defined within the Act itself. This would provide a clear boundary for requests and align the obligation with the core subject matter of the Data Act, reducing the burden of identifying and providing broader categories of data.

Additionally, to prevent an unmanageable influx of requests from a multitude of public bodies, the Commission and Member States should be required to establish and maintain prescribed, publicly accessible lists of EU bodies and national public sector bodies that are explicitly empowered to make such data requests under Chapter V. This would provide essential clarity for data holders and ensure requests originate from legitimately authorised entities.

2.2.3. Data Governance Act

International data transfers

Like the above comments on international data transfers in the context of the Data Act, the Data Governance Act must also enable the free flow of data and remove any unnecessary impediments to the transfer of data. For this reason, Chapter VII of the Data Governance Act on International Access and Transfer should be withdrawn in favour of the international data transfer regime under the GDPR.

2.2.4. GDPR

Proportionality principle

While the GDPR aims for a risk-based approach, its practical application often leads to compliance efforts that are disproportionate to the actual risks involved, the nature of the processing, or the costs of implementation. To ensure the GDPR supports innovation and manageable compliance, the principle of proportionality should be more explicitly recognised within the Regulation itself. For instance, the Commission could clarify in Article 24 that obligations on controllers should be interpreted and measures implemented in a manner that is proportionate to the nature, scope, context, purposes of processing and the reasonably assessed risks to individuals, as well as implementation costs. This would provide a clearer mandate for both businesses and Data Protection Authorities to adopt more balanced and pragmatic approaches.

Accountability principle

The principle of accountability (Article 5(2) GDPR), while crucial, often translates into voluminous and duplicative documentation. Article 5(2) should be clarified to explicitly permit controllers to rely on a single set of assessments and documentation for multiple processing operations that are similar in terms of their nature, scope, context and purpose, thereby reducing redundant administrative efforts.

International data transfers

The essential equivalence standard by which third country data protection laws and practices are assessed to establish adequacy of protection of transferred personal data is a very cumbersome operational burden for companies that creates legal uncertainty, while failing to significantly contribute to the data protection posture. In practice, only a handful of countries have been able to qualify for an adequacy decision. 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.

A multilateral approach should be fostered by recognising personal data transfers by way of reference to an international, principle-based standard, such as the OECD Privacy Guidelines and Global Cross Border Privacy Rules. This would ensure a core baseline of protections, 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 of each jurisdiction in turn, requiring every provision to be matched.

The Commission should also evaluate how to ease the current requirement for each controller/processor to essentially do an adequacy assessment in each jurisdiction.

We believe there is a great need to streamline the GDPR's transfer regime for SMEs and large companies alike. First, by introducing an intra-group data transfer certification mechanism under Article 46. This would allow corporate groups to self-certify adherence to a set of Commission-defined principles and safeguards, thereby being presumed to have provided appropriate safeguards for internal transfers without the need for repetitive, case-by-case Transfer Impact Assessments (TIAs). Further simplification could be achieved by clarifying within Article 46 that a single TIA can be conducted for a set of similar transfers to the same or similar third countries where comparable safeguards are applied, reducing duplicative assessment efforts. Additionally, updating the Standard Contractual Clauses (SCCs) framework to explicitly cover transfers to data importers established in third countries whose processing is already subject to the GDPR by virtue of Article 3(2) would address a current gap and provide legal certainty for such common transfer scenarios.

Personal data and pseudonymisation

While GDPR purports to be risk-based, companies' treatment of data is largely determined by what the data is, rather than the purpose for which it is used. To streamline its impact, attention should be paid to the sprawling concept of personal data. To incentivise the adoption of technical and organisational data protection controls, companies' usage of pseudonymised data should be encouraged (eg by concrete and practical guidance) and a more realistic and future-proof standard of the likelihood of deidentification should be introduced. Specifically, the existing European Data Protection Board guidance should be revisited to recognise newer methodologies such as privacy-enhancing technologies as tools that can help businesses meet GDPR compliance obligations.

AI data processing

The EU has identified AI as crucial to its future competitiveness. GDPR implementation is key to enabling a thriving AI ecosystem in Europe. Indeed, Generative AI systems rely on general-purpose AI models, also called foundation models, that are usually trained on vast amounts of data to achieve a variety of purposes. Both regarding new data collection and repurposing of previously collected data, regulatory guidance should facilitate lawful mechanisms for the use of personal data in model training. Organisations should be able to rely on Article 6(1)(f) 'legitimate interests' legal basis for processing personal data, including publicly available data collected through methods like web scraping, so long as the controller's legitimate interest is not outweighed by the rights of individuals. Mitigation measures should of course be appropriate but should also be sufficiently flexible to account for a variety of models and goals, as well as for evolutions over time. In addition, Article 6(1)(f) could be amended to recognise a 'whitelist' of common, lower-risk processing activities (such as fraud prevention, network security, product improvement and essential research) which are presumptively lawful, affording controllers a 'margin of appreciation' in their balancing tests for such low-risk activities.

To support innovation in AI and other research areas, Article 9(2) GDPR exemptions for processing Special Category Data (SCD) should be expanded and clarified. This could include explicit provisions for processing publicly available SCD where appropriate safeguards are in place and ensuring that scientific research purposes (under Article 89(1)) clearly encompass the development and training of AI models, including general-purpose AI. The definition of SCD itself in Article 9(1) could also benefit from narrowing to focus on data that is explicitly sensitive or processed with the intent to infer sensitive characteristics, reducing the over-broad interpretation that currently poses challenges.

Additionally, we call for further alignment of Article 10(5) of the AI Act with the GDPR for special category data processing for bias testing purposes. While bias in AI algorithms is a critical concern that must be tackled from the initial development phases and continuously managed throughout the system's entire lifecycle, the language of Article 10(5) is more restrictive than the one provided in the GDPR, requiring providers to demonstrate that the processing is '*strictly* necessary' instead of 'necessary' in Article 9(2) of the GDPR. Additionally, the obligation under Article 10(5)(e) to delete special categories of personal data once bias has been corrected overlooks the need for continuous bias monitoring throughout the system's operational lifespan, as new biases can emerge during real-world deployment. We urge the Commission to simplify the AI Act requirement by aligning the conditions for processing special categories of data with the GDPR instead of creating more restrictive conditions. Guidance is needed to clarify the areas of overlap between the AI Act and the GDPR, in particular the apparent tension between the data minimisation principle included in the GDPR and the focus of the AI Act on accuracy, transparency and bias avoidance.

2.2.5. ePrivacy Directive

As the challenging legislative process and withdrawal of the ePrivacy Regulation demonstrates, applying a specific data privacy regime to the electronic communications sector is not straight forward. The withdrawal of the ePrivacy Regulation means that the current ePrivacy Directive continues to be the legal instrument in this field. First adopted in 2002, many of the provisions are obsolete, such as billing, caller ID, call forwarding and subscriber directory.

We believe that there is ample room to simplify the ePrivacy framework, by deleting the obsolete provisions and moving the remaining obligations to other frameworks. For example, the obligations on traffic and location data, as well as on breach notifications could be perfectly absorbed by the GDPR, the obligations on confidentiality of communications – while being in urgent need of modernisation – could go to the DNA, the cookie rule could go either way and the provisions on data retention could be included in a future law enforcement proposal.

Crucially, any reform or relocation of the cookie rule must address its current over-restrictiveness and lack of clarity, which has led to 'consent fatigue' for users. A simplified and future-proofed rule should include clear exemptions from consent requirements for common, low-risk and beneficial processing activities. Specifically, Article 5(3) or its equivalent successor provision should explicitly permit storage or access without consent where it is necessary for security purposes, such as ensuring the security and integrity of networks and services, detecting technical faults or errors and preventing fraudulent use or abuse that could impact the service or other users. Similarly, exemptions should cover analytics purposes for first-party web audience measurement, provided this does not entail the profiling of users across different websites, apps or services, enabling providers to understand service usage and improve user experience. Exemption for contextual advertising should also be considered, to permit the display of advertising based on the immediate context of the user's interaction (eg content being viewed, current search query on a site, or device type during a single session).

Furthermore, to reduce unnecessary 'cookie banner' proliferation, it should be clarified that where such exemptions to consent apply, the display of a banner is not mandatory, provided clear and comprehensive information about these activities is made easily accessible to users (eg within a privacy policy).

Finally, the scope of 'storing of information, or the gaining of access to information already stored' needs clarification to ensure it does not inadvertently capture mere transient or ephemeral storage,

or information exchanged as a part of ordinary internet communication protocols (eg TCP/IP headers) that are not targeted for specific data extraction by the service provider. Such an overly broad interpretation does not serve the privacy aims of the Directive and creates undue compliance friction. These targeted simplifications would make the rules more practical, reduce burdens on businesses (especially SMEs) and improve the online experience for users.

2.3. Connectivity

Key points:

- Streamline the European Electronic Communications Code (EECC) to remove outdated or duplicative obligations.
- Apply lighter regulatory treatment for business users, excluding large enterprises from consumer rules.
- Standardise notification and reporting procedures across Member States; support online submissions and shared templates.
- Reject the proposed Country of Origin principle which risks fragmenting the digital single market.

2.3.1. European Electronic Communications Code

The EU's telecom regulatory framework is currently a complex and fragmented web that hampers the ability of operators to respond swiftly to market trends and adopt new technologies. Enhancing legal coherence and certainty should be a top priority.

The piecemeal implementation of the European Electronic Communications Code (EECC) has been late in several Member States and has led to different interpretations (or additional burdens) at the national level. For example, the EECC expanded the definition of electronic communication services (ECS) to include OTT platforms, which prompted Member States to revise national ECS definitions that extend existing ill-fitting telco-specific requirements to OTT services. This led to inconsistent translations and a lack of harmonised implementation across the EU.

The following measures, applied individually or in combination, would significantly improve the situation without detriment to consumers.

Tailored regulatory requirements for consumer protection concerns

Contracts with non-SME business users should be excluded from the requirements of consumer protection legislation. There is already evidence that at least some Member States could be willing to lighten regulatory burdens on authorised operators based on the nature of their customer base. For example, in December 2023, Italy's AGCOM issued Resolution 307/23/CONS clarifying that its Resolution on end users' protection does not apply to large enterprise customers.

Practical simplification of notification procedures

Notification requirements should be minimised and streamlined wherever possible. Failing this, a common and consistent format should be developed for notifications. All National Regulatory Authorities (NRAs) should accept notifications online. NRAs should be strongly encouraged to publish information about notification regimes and to accept notifications in other EU official languages, primarily English. Common forms and approaches should be developed for the reporting of financial, statistical data, service category and other market information by service providers.

Avoidance of duplicative regulation

While a re-calibration of the relationship between GDPR, e-privacy, EECC and cybersecurity obligations at the EU and the Member State level would undoubtedly raise fundamental questions, it would provide a very material boost to the creation of a Single Market for electronic communications services for business customers. Such a change would drive significant supply-side improvements in terms of compliance and operational costs.

Review of existing regulations

A rigorous review of existing regulations and their relevance to today's technological and business environment is vital, especially before introducing any new regulations. Outdated, duplicative or ill-fitting regulations should be eliminated to help the EU fully benefit from the economic and social advantages of upcoming technological developments.

Pragmatic approach

For example, the proposal for a 'Country of Origin' principle suggested in the European Commission's White Paper on how to master Europe's digital infrastructure needs[3] would be against the goal of simplification. Requiring companies such as telecom operators, equipment vendors and/or their supply chain to consider different rules, build frameworks and infrastructure that meet different standards and report to different regulatory bodies according to the market from which they originate will defeat the purpose of building a Single Market. Companies would not be able to operate on a level-playing field as, by definition, different regulatory bodies will have different response times and a different overall understanding of the applicable rules and regulations.

[3] European Commission, White Paper 'How to master Europe's digital infrastructure needs?', 21 February 2024, https://ec.europa.eu/newsroom/dae/redirection/document/102533.

2.4. Artificial Intelligence

Key points:

- Confirm the central role of the EU AI Office in guiding consistent AI Act implementation.
- Delay sector-specific AI legislation until the AI Act is fully operational and interpreted.
- Introduce a broad R&D exemption for AI development and clarify the scope of 'putting into use'.
- Formally withdraw the AI Liability Directive to simplify compliance for developers and users.
- Delay the applicability of high-risk requirements under the AI Act until 12 months after relevant harmonised standards are published, to ensure legal certainty, consistent enforcement and sufficient time for companies to adapt.

2.4.1. AI Act

As the first comprehensive legislative framework for AI, the Act stands for a complex structure encompassing compliance obligations for all actors along the AI value chain. As the EU AI Office guides its implementation, the role of stakeholders developing and deploying AI should continue to be central. Moreover, the implementation process should focus on the objectives set out in the AI Act while being guided by the priorities laid out in the Draghi Report and the announcements made on AI by President Von der Leyen: supporting investments and simplifying to strengthen European competitiveness.

AI Act Implementation

The EU AI Office's role in implementing the AI Act should be clearly affirmed by the Commission. As the AI Act delegates significant portions of the regulation to secondary legislation, it is of fundamental importance to ensure that these rules are coherent, cohesive and in line with the text of the Act. Businesses would be hit with significant uncertainty should the AI Office not be empowered to centralise this lawmaking process. A specific challenge in this space would be for other DGs to publish rules executing the mandate of the AI Act, without the necessary competences and understanding of the AI Act that the AI Office is instead building.

Additionally, sector-specific legislation on AI should not be considered until the AI Act's implementation is complete. Going forward, the AI Office must ensure future rules provide regulatory clarity, do not layer duplicative requirements onto firms and are developed in partnership with industry. AI regulators can draw lessons from previous regulatory implementation where a lack of clarity withing published guidance, coordinated enforcement and overall engagement with constituents, led to misinterpretations of key issues governed by secondary legislation leading to hesitance on organisations to invest in their respective industries.

A key example of this concerns the need for legal clarity between the EU Medical Device Regulation (MDR) and the AI Act obligations for the healthcare sector. Medical devices and products are planned

and developed years in advance, necessitating clarity around which additional AI Act obligations apply to their products and when. The Commission should clarify through guidance that only those AI Act obligations that are in addition to existing obligations under the MDR/IVDR will apply, with explicit reference to those additional requirements.

Two additional clarifications relevant to the AI Act are necessary. The first pertains to the need for an R&D exemption, beyond purely scientific purposes but to include all commercial purposes. This would strengthen the EU's ability to act as a global hub for research and development. The second clarification concerns the definition of 'putting into use on the market', which causes confusion for companies on whether their AI models are in scope. The EU's guidance on prohibited practices does refer to the EU Blue Guide, which provides clarity that 'putting into use on the market' refers to intended use. However, this interpretation should be more explicit and visible to companies to drive legal clarity and certainty.

Stakeholder involvement

The AI Office should also ensure that future consultations on the implementation of the Act are published in a timely manner and allow for enough time for stakeholders to prepare their responses. For example, the recent consultations on the Definition of AI and Prohibited Uses of AI and on Guidelines for General Purpose AI (GPAI) models had a four-week turnaround for comments, with the former launched during the Christmas holidays. This approach does not provide stakeholders with sufficient time to develop well thought-through inputs to one of the EU's most complex pieces of legislation and is not indicative of a collaborative relationship between the Commission and industry.

Given the clear timeline for the implementation of the Act, future consultations should be launched well in advance of the application dates of specific rules to ensure stakeholder views are represented in final guidance. The Act mandates that the AI Office produces guidance on High-Risk uses 18 months from entry into force. Given how foundational this guidance will be for compliance with the Act, the Commission should launch the consultation process for it before the summer of 2025.

Ensure timely standards for AI

A key concern amongst industry stakeholders is the absence of harmonised European standards that were intended to provide presumptions of conformity for EU AI Act provisions. Without these standards in place, companies are left navigating a fragmented and ambiguous compliance landscape, which undermines legal certainty and risks inconsistent enforcement across Member States. Delays in developing these crucial standards mean that the AI Act's high-risk requirements may apply before companies have the necessary compliance guidance, creating significant uncertainty and a practical impossibility for businesses to adapt existing systems. Any meaningful simplification effort must take this regulatory gap into account and ensure that implementation timelines are aligned with the actual availability of the necessary technical and legal guidance. The simplification package should accordingly propose that high-risk requirements become applicable only 12 months after relevant standards are published. Such an approach would provide greater predictability and adequate time for adaptation, fostering innovation.

2.4.2. AI Liability Directive

The Commission’s announcement to retract the proposal for an AI Liability Directive (AILD) clearly maintains the objective of simplifying the compliance burden on companies by re-evaluating pending legislation. The Commission should confirm this decision by formally retracting the proposal.

3. Conclusion

Europe's digital economy faces challenges from a complex and fragmented regulatory landscape, leading to compliance burdens and hindering innovation. The Commission's commitment to simplification is vital for enhancing competitiveness and unlocking digital potential.

Achieving this requires a strategic approach: building a Digital Single Market through harmonisation, streamlining regulations and fostering stakeholder engagement. Addressing specific challenges in cybersecurity, data policy, connectivity and AI is paramount.

By adopting these recommendations, the EU can create a more predictable, practical and growth-oriented environment. This simplification will strategically position Europe to attract investment, accelerate innovation and secure its digital future.