Digital Omnibus

Call for Evidence

bitkom

At a glance

Toward a Coherent EU Tech Framework

Initial position

The last mandate has transformed the legal landscape of Europe's digital economy, marked by a broad set of new regulations and directives from the European Commission. From cybersecurity and artificial intelligence to data economy, few areas of the digital economy have remained unaffected. As these new laws enter the critical phase of implementation, inconsistencies and overlaps, particularly in definitions and obligations, are becoming increasingly apparent. Instead of delivering the promised legal clarity to support innovation made in Europe, businesses are grappling with a jungle of regulatory complexity.

Bitkom highly welcomes the Commission's plan for a digital omnibus package which is offering a vital opportunity to streamline the current digital framework. The Commission must deliver on the targets it set and cannot afford to fall short of its own stated ambitions.

Focus areas for action

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

- **Streamline Cybersecurity Reporting Obligations**
  Overlapping requirements across recent cyber laws have fragmented the regulatory landscape. Companies face parallel reporting duties, inconsistent national implementations, and regulatory duplication. In this context, the Cybersecurity Act (CSA) must evolve beyond certification to serve as a central coordinating tool for coherence and simplification. Streamlining incident reporting, currently duplicated across Network and Information Security Directive (NIS2) and Cyber Resilience Act (CRA), must be a priority – guided by the principle of «one incident, one report, one mechanism» supported by clearer roles, consistent definitions, and a stronger mandate for ENISA.

- **Provide Targeted Adjustments to the AI Act**
  To support a competitive AI economy in Europe while effectively addressing AI-related risks, targeted adjustments in the AI Act are needed. In particular, the application of high-risk requirements should be postponed by at least 24 months, as key standards are unlikely to be finalised before December 2026 due to the complexity of the consensus-building process. Furthermore, all high-risk requirements listed in Annex I A should be integrated into relevant sectoral legislation (following the existing logic of Annex I B). The AI Act should serve as projects due to privacy-related concerns. The digital omnibus must address these

maximum harmonisation instrument, ensuring that efforts to align sector-specific regulations do not exceed their requirements.

- **Create a Functioning Framework for the Data Economy**
  While the recent acquis of rules on access, localisation, intermediation, and transfer of (non-)personal data has avoided the fragmentation of the single market for data during its very onset, it has not been possible to create a fully coherent framework yet. In particular, there is a need to address different material scopes, timely applicability, as well as certain interactions between laws. In addition, their implementation merits more attention to be as consistent and fast as needed. We also highly encourage the Commission to consider the Data Act (DA) in the Digital Omnibus to turn it into an ambitious initiative in line with the ongoing political discourse.

- **Ensure High Privacy Standards that Enable Innovation**
  Data is essential for driving innovation and maintaining global competitiveness, especially in areas like AI model training. However, unresolved conflicts between the General Data Protection Regulation (GDPR) and other digital regulations – such as the AI Act and the DA – create legal uncertainty, particularly around the processing of personal data. That's why we call on the Commission to address the GDPR in the Digital Omnibus through targeted amendments. The reform of the outdated ePrivacy Directive should take a holistic approach, addressing the entire directive – not just the cookie rule – as its isolated, sector-specific design no longer fits within today's broader data protection and digital legal framework.

- **Maintain eIDAS as the Single Reference for Digital Identity**
  The updated eIDAS Regulation and its Implementing Acts already provide a comprehensive framework for electronic identification, authentication, and credential validation. Further simplification should preserve eIDAS as the central reference point to guarantee European interoperability. Clearer and more consistent rules are needed to prevent overlap, ensure coherence, and create a stable and predictable compliance environment.

- **Ensure Coherent Enforcement Among Member States**
  Enforcement structures across Member States differ significantly in terms of focus, capacity, expertise, and resources, resulting in inconsistent implementation. The effects of this imbalance were evident with the GDPR and now pose similar risks for the NIS2 Directive. Stronger coordination at the European level, supported by efficient structures and regular dialogue, is essential to promote collaboration among national authorities and achieve consistent enforcement across member states. In addition, greater attention should be given to addressing gold-plating practices.

Content

1 Cybersecurity

Over the past twelve months, cyberattacks have caused damages amounting to 289 billion euros for German companies.[1] This figure underscores the urgent need for a robust and effective approach to cybersecurity. Against the backdrop of an increasingly hostile threat landscape, German industry strongly supports a holistic European strategy to strengthen resilience against cyber risks.

Since 2016, the European Union has laid the foundation for such a strategy through a comprehensive cybersecurity regulatory framework addressing both organisations and digital products. The Network and Information Security Directive (NIS-1 Directive) and its recent update, NIS-2, have been central to harmonising cybersecurity requirements across Europe. With NIS-2, the EU has significantly raised the bar by requiring companies to implement risk management measures and to report cybersecurity incidents.

These efforts have been complemented by the CSA and the CRA, which focusses on product resilience. Together, these instruments represent an ambitious framework. Yet the steady rise in regulatory obligations has created a paradox: measures intended to enhance security often divert resources away from practical risk mitigation.

The forthcoming Digital Omnibus offers the European Commission a key opportunity to recalibrate the regulatory environment. To strengthen resilience and foster innovation, it is essential to streamline cybersecurity regulation and avoid overlapping or conflicting provisions. The complexity of requirements, certification schemes and harmonized European standards should be limited to what is strictly necessary. A lean and coherent approach not only reduces unnecessary burdens but also ensures legal clarity across the European digital and industrial landscape. Most importantly, regulation must empower companies to act decisively in times of crisis – focusing on defence, containment and recovery – rather than tying resources to excessive compliance tasks. Only in this way can Europe safeguard technological leadership and enable effective implementation across Member States.

59%

of German companies consider cyberattacks to be a threat to their existence.
(↗ Bitkom, 2025)

Common registration, reporting and uniform application

One of the most pressing challenges in the current cybersecurity landscape lies in fragmented reporting obligations. The CRA, NIS-2, the Digital Operational Resilience Act (DORA), the AI Act (cf. Art. 73) and the GDPR each impose specific procedures for incident notification, with differing authorities, reporting channels and requirements. Groups of undertakings need to conduct a complex scope investigation merely for the purpose of registering their legal entities separately instead of simply registering the entire enterprise centrally. For multi-domain companies operating across borders, this patchwork results in significant complexity and overlap.

[1] ↗ Bitkom Study »Wirtschaftsschutz 2025«.

Under NIS-2, essential and important entities must notify significant incidents to the national competent authority or the national CSIRT in every Member State where they operate. The CRA requires manufacturers to report actively exploited vulnerabilities in digital products both to national CSIRTs and to ENISA. Providers of high-risk AI shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred. GDPR adds its own breach notification rules, while DORA establishes obligations for the financial sector.

A particular burden stems from the stringent timelines. Both NIS2 and CRA stipulate initial reporting within 24 hours of becoming aware of an incident. While justified in critical cases, such short deadlines are often impractical when information is still incomplete, leading to multiple preliminary reports that divert resources away from actual incident response. When incidents cut across multiple domains – such as data protection, financial systems and product security – companies face overlapping processes to multiple authorities, creating duplication and compliance risks without corresponding security benefits.

In particular, for companies operating across multiple Member States, divergent interpretations and enforcement practices create uncertainty and risk of inconsistent compliance, making it difficult to implement a unified security strategy. To resolve this, reporting processes across regulatory instruments must be standardised. Harmonisation should cover definitions, thresholds, timelines, reportable items, formats and competent authorities. An overarching EU digital regulation definition source for all regulations could provide a centralized overview for regulated companies and institutions. A one-stop-shop reporting mechanism should be established, enabling companies to meet all obligations through a single submission. ENISA's CRA single reporting platform could serve as such a platform for incident notifications under both the CRA and NIS2 frameworks, allowing organizations to submit one report that is automatically forwarded to the relevant national authorities and CSIRTs. Member States would retain full authority over incident response and enforcement, while ENISA's platform would operate solely as a technical intermediary. To further enhance efficiency and consistency, a secure and efficient centralized communication mechanism should be developed within this platform for follow-up inquiries, enabling competent authorities to share information, reduce redundant requests, and ensure consistency in messaging. As an interim step, Member States should introduce national one-stop-shops to reduce immediate burdens and designate a single notification endpoint for both CRA and NIS2 to further streamline the process for companies operating across borders.

The European Digital Identity Wallet (EUDI Wallet) could provide secure authentication on such a platform, further simplifying processes. Safeguards must also ensure that a single report suffices for cross-border incidents, avoiding duplicate sanctions for the same event.

Cybersecurity Act

The CSA adopted in 2019, was designed as a central instrument to strengthen the security of information and communication technologies. At the time, no other EU-wide product-related cybersecurity requirements existed. Since then, however, the regulatory environment has grown more complex. With NIS-2, DORA, the CRA, the

delegated Radio Equipment Directive (RED), and the AI Act multiple overlapping regulations have emerged. National regulations, schemes and goldplating create further complexity. Instead of providing clarity, the CSA risks becoming another element of fragmentation. To remain effective, the CSA must evolve into an umbrella regulation that brings coherence to this patchwork. It should provide a framework for enforcement and certification, aligning sectoral and horizontal initiatives. Existing risk management systems like ISO/IEC 31000 should be considered as a general base and for the integration of several risk management systems. ENISA, as the EU's cybersecurity agency, should be given a stronger mandate to promote coherence and support implementation through practical tools.

Bitkom recommends that ENISA conduct a comprehensive mapping of overlaps and inconsistencies across EU cybersecurity regulations. This analysis should rely on internationally recognised standards and propose concrete measures for simplification. Mapping EU requirements against established standards would help both authorities and businesses, following a risk-based approach, highlighting gaps and clarifying the relationship between EU rules and international frameworks. Well-established standards such as ISO/IEC 27001 should serve as the foundation for demonstrating compliance wherever possible.

In addition, ENISA should lead the development of a harmonised cross-sectoral reporting framework under the CSA. Today, reporting obligations are dispersed across NIS2, CRA, DORA, GDPR, DA, and AI Act each with its own thresholds, timelines and channels. A centralised reporting portal, grounded in harmonised standards and coordinated by ENISA, would substantially enhance legal clarity and strengthen Europe's collective ability to respond to threats. To succeed, such a framework must ensure interoperability, aligned definitions and standardised procedures, while avoiding redundant obligations and duplicate sanctions. For instance, there is considerable potential for harmonization when it comes to CE marking requirements. These should be aligned across regulatory frameworks, with a single technical file format recognized across frameworks and clear Commission guidance to ensure uniformity across Member States. By assuming a coordinating role, ENISA can ensure that the CSA becomes the foundation for coherence and effectiveness rather than an additional layer of complexity.

Network and Information Security Directive 2

The transposition and application of NIS-2 across EU member states lacks uniformity in timelines, scope and requirements, creating legal uncertainty and additional burdens for companies. Thirteen member states have not yet implemented the regulation. Inconsistent approaches are evident in several areas:

- Some member states, such as Hungary, have applied NIS-2 early, while many others have delayed or not yet transposed it.
- The treatment of minor activities, such as small-scale solar energy production, employee charging points or non-hazardous chemicals, varies significantly.
- Authorities like NUKIB in the Czech Republic consider recitals non-binding if not explicitly included, disregarding Recital 114 and thereby risking double registration for groups of undertakings.

- NIS-2 does not clarify which evidence or certification must be provided by Important and Essential Entities, while some member states introduce additional schemes, such as Germany's C5, complicating EU-wide compliance.

As Member States may also add further national requirements, companies operating cross-border face substantial monitoring and compliance overheads. This situation can only be addressed through full harmonization and uniform application of scope, timelines, obligations and requirements across the EU.

NIS-2 also tightens requirements for incident reporting. Article 23 obliges all essential and important entities to notify incidents with significant implications for their services. The intent is clear: to provide national authorities with the data needed to build a comprehensive and timely cybersecurity situation picture. Yet this only works if the reported information is analysed, shared and systematically integrated by authorities.

At present, NIS-2 imposes a five-step reporting regime. Companies must submit an initial notification within 24 hours, followed by a second report within 72 hours. Upon request, interim updates may be required during incident handling. A final report is due one month after the first notification. If the incident remains unresolved, a progress report must be filed, with a final report submitted one month after resolution. This system creates heavy administrative burdens. Meeting the 24-hour deadline is difficult when reliable information is scarce. Divergences between Member States exacerbate the challenge, with some requiring broader reporting than others or applying varying cross-border criteria. Companies must therefore implement country-specific procedures, increasing compliance risks and pulling resources away from incident management.

A streamlined approach is needed. Instead of five steps, reporting should be limited to three. First, companies should issue an early warning within 48 hours of detecting a significant incident, limited to basic information such as company name and visible effects. Second, upon request, an intermediary report may be provided. Third, a final report should be delivered no later than one month after resolution.

This simplified model would maintain timely situational awareness for authorities while reducing burdens on companies, ensuring resources remain focused on mitigation and recovery rather than excessive reporting.

Cyber Resilience Act

Although the CRA may not be a central focus of the Commission's omnibus package, it cannot be treated as secondary. Its provisions are closely linked to CSA, NIS-2, GDPR, the AI Act and DORA, and its full enforcement in December 2027 will significantly reshape compliance requirements across Europe. While the CRA has the potential to strengthen cybersecurity in digital products, it also creates uncertainty and imposes considerable administrative burdens on manufacturers.

With horizontal regulations such as CSA, CRA and NIS-2, the cybersecurity regulatory landscape has expanded considerably. In addition, vertical, sector-specific regulations – such as RED (EU) 2014/53, (EU) 2018/1139 and (EU) 2019/2144 – already regulate cybersecurity and certification of specific systems and components. To avoid

unnecessary duplication, the complexity of cybersecurity-related regulation and certification should be kept to a minimum. Where suppliers can demonstrate compliance with applicable vertical requirements, including technical specifications, cybersecurity measures and relevant standards, their products should not be subject to overlapping horizontal regulations.

The downstream measures required to operationalise the CRA remain delayed, leaving manufacturers with insufficient time for preparation. The Commission should therefore define realistic and technically feasible timelines for developing and delivering harmonised standards. Current schedules are highly problematic: the type B standards for handling vulnerabilities are expected to be available to manufacturers by 30 August 2026, only days before the reporting obligations for actively exploited vulnerabilities and severe incidents take effect on 11 September 2026. Combined with obligations for legacy products dating back to the earliest digital elements, this creates disproportionate burdens for manufacturers. A pragmatic solution would be to align the start of reporting obligations with the general applicability date of the CRA on 11 December 2027. Other standards are also to be published close to the corresponding deadlines. Many other product-specific standards on 30 October 2026. This would leave approximately one year to implement the product-specific standards, which is very tight. Further horizontal standards of type B have been announced for 30 October 2027, around 1.5 months before the CRA comes into general effect. This leaves manufacturers with little to no time to adapt their processes to the harmonised standards, which puts them at risk of high penalties.

Article 14 of the CRA requires manufacturers to report actively exploited vulnerabilities through a designated platform in three stages: an early warning within 24 hours to both the CSIRT and ENISA, a detailed notification within 72 hours, and a final report within 14 days after corrective measures. This system duplicates existing frameworks and diverts resources from actual remediation. To improve efficiency, the reporting procedure should be streamlined to two steps: an initial notification within 72 hours with essential information and a comprehensive report within 14 days of corrective action. All notifications should be submitted only once, ideally through ENISA's platform, to eliminate parallel processes.

Further complexity arises from overlapping provisions in existing legislation. In particular, the RED Delegated Regulation (EU) 2022/30 introduces parallel cybersecurity requirements that duplicate the CRA. As the CRA provides a more comprehensive and neutral horizontal framework, the RED Delegated Act should be repealed once the CRA becomes applicable, especially for products covered by both instruments. To ensure continuity, the harmonised standards EN 18031-1/2/3 should be supported in such a way that existing product development processes, risk assessments and technical documentation can be fully leveraged for CRA compliance.

Another critical challenge for manufacturers is the CRA's treatment of «substantial modification.» Originating from the EU's New Legislative Framework, this concept is difficult to apply to digital products, since it is often unclear when software changes trigger reassessment. The Commission should therefore provide clear and practical guidance, including thresholds and examples, to ensure legal certainty in determining substantial modifications.

Manufacturers also face a fragmented supervisory environment with uncoordinated requests from multiple Market Surveillance Authorities (MSAs). To streamline oversight, a lead MSA should be designated based on the location of a manufacturer's main EU establishment, or another suitable basis if required, to act as a single point of coordination for regulatory inquiries.

The CRA also introduces indefinite obligations for monitoring products and reporting vulnerabilities and incidents. Unlike vulnerability management obligations, which end at the close of the support period, monitoring and reporting requirements currently apply without limitation. Such perpetual obligations are disproportionate. Instead, monitoring and reporting should be limited to a defined period, for example three to five years after the end of the support period.

To further reduce complexity, it is necessary to align conformity assessments under the CRA and AI Act. Joint procedures and mutual recognition of assessments would help avoid duplication and foster consistency in implementation. This could be achieved by establishing a Joint Conformity Assessment Framework that integrates the requirements of CRA Modules B, C, and H (as outlined in Decision 768/2008/EC) with the AI Act's internal (Annex VI) and third-party assessments (Annex VII). Additionally, Conformity Assessment Bodies (CABs) with cross-competence should be authorized to assess compliance under both Acts, and mutual recognition agreements should codify that compliance with one framework (such as AI Act Annex VII) satisfies equivalent CRA obligations.

Finally, the scope of the CRA also extends to trivial products such as A/D converters or devices whose only «digital interface» is a USB charging port, for example electric toothbrushes. Although these products present virtually no cybersecurity risk, they are nevertheless subject to the full New Legislative Framework conformity assessment. As established in the Machinery Directive («trivial machines») and the EMC Directive («inherently benign products»), a specific exemption for «inherently benign products» should be introduced in the CRA. This category would apply to products with digital elements that, due to their technical simplicity, cannot pose cybersecurity risks.

2 AI Act

Significant implementation challenges and unclear requirements threaten the AI Act's goal of mitigating AI-related risks while fostering AI innovation in Europe. This is clearly reflected in the fact that 93% of German companies affected by the AI Act report that the effort required for its implementation is considered either rather high or very high.[2]

To realign the Act with its original intent, the EU Commission has announced an AI Act simplification as part of its competitiveness agenda. We aim to support the EU Commission's competitiveness agenda by offering key recommendations for a feasibility-focused AI Act simplification package that safeguards innovation.

Postpone the entry into application of high-risk requirements by at least 24 months

The AI Act's entry into application for high-risk AI requirements is scheduled for August 2026. However, the development of harmonised standards, which are crucial for establishing and demonstrating compliance, is facing significant delays. Officially, the revised standardisation request indicates that standards should be available by August 2025. In practice, however, internal estimates from CEN-CENELEC's JTC21 – the group responsible for drafting these standards – suggest that the first standards may not be ready before mid-2026, and full availability may not be achieved before end of 2026. This timeline raises concerns about the practical feasibility of meeting the AI Act's requirements. Even once standards are published, companies will need adequate time to assess and integrate them into their development and governance processes. Implementing new standards requires adaptation of existing systems, training, and alignment with other internal compliance frameworks.

To enable the development of high-quality standards and allow sufficient time for their implementation, the AI Act simplification package should extend the implementation timeline for the high-risk requirements under Annexes I and III by at least 24 months and correspondingly delay the applicability of fines for non-compliance by 24 months in this regard.

This extension is justified, as current planning horizons – already considered optimistic given the complex and protracted consensus-building process – indicate that the relevant standards will not be fully finalised before the end of 2026. Organisations with experience in implementing digital regulations note that compliance with a single standard often requires more than 12 months.[3] Given that the implementation of the AI Act's high-risk requirements is expected to involve up to 35 (partially referenced) standards in total[4], a significantly longer timeframe will be necessary to ensure effective and compliant adoption. Given implementation uncertainties, guidance should ensure parties have appropriate time to cure good faith noncompliance before penalties apply.

[2] ↗ Bitkom Study »KI in der deutschen Wirtschaft«, 2025.
[3] ↗ Dr. Kilian et al., European AI Standards, p.26.
[4] ↗ Dr. Kilian et al., European AI Standards, p.26.

Integrate high-risk requirements related to Annex I A into sectoral legislation

Early implementation challenges are exposing the limits of applying horizontal AI rules to established sectoral frameworks, especially for those under Annex I section A. The development of harmonised standards for AI is proving slower and more complex than anticipated. Manufacturers are left uncertain as to how new AI-specific standards will align – or conflict – with existing ones that already govern their products. This uncertainty is bound to create bottlenecks and undermine long-standing compliance pathways.

The problem is particularly acute in the area of conformity assessment. The AI Act introduces obligations that current conformity assessment bodies are neither clearly authorised nor equipped to manage under existing sectoral regimes. In highly regulated sectors such as automotive or medical devices, where notified bodies are already under strain, adding AI-related requirements without a clear integration pathway poses a risk for compounding delays and market disruption.

This regulatory burden will weigh the heaviest on manufacturers in sectors where Europe holds longstanding competitive advantages, such as automotive, machinery or medical equipment.

For these reasons, Annex I should be streamlined by merging its two sections and extending the more flexible Section B approach to the entire annex. This would ensure that AI requirements can be progressively incorporated into sectoral frameworks in a more stable and controlled manner, rather than applying immediately and in parallel with sectoral legislation. Crucially, this would allow harmonised standards for AI to be translated and embedded into sector-specific contexts without undermining existing conformity procedures.

Integration of AI requirements into sectoral frameworks should follow a sequenced process grounded in existing legislation. The goal is not to reopen well-functioning regulatory systems, but to align them with the AI Act in a way that respects their structure and avoids legal uncertainty. For this approach to succeed, the AI Act simplification package must clarify the AI Act's status as a maximum harmonisation instrument. Sector-specific measures through delegated acts, implementing acts or technical specifications must not impose requirements beyond the AI Act. This is essential to prevent inconsistent or excessive obligations, and would strengthen the replicability of AI harmonised standards, maintaining a unified definition of 'state of the art' across sectors.

Risk of absence of grandfathering provisions for legacy products

The absence of grandfathering provisions in the EU AI Act poses a significant risk to the continued availability of well-established NFL-products on the EU market. These legacy products, developed in full compliance with existing CE marking regulation prior to the entry into force of the AI Act on 1 August 2024, face disproportionate regulatory burdens that may render their continued placement on the market economically unviable.

- **Critical Deadline:** Without grandfathering, many products may be withdrawn from the EU market by 2 August 2027, due to the high cost of compliance with the AI Act – costs that are not justifiable for many manufacturers.
- **Impact:** This risk is particularly acute for providers that rely on long-standing, proven technologies, e. g. healthcare providers relying on clinically proven technologies
- **Legal Interpretation:** Article 111 of the EU AI Act applies to the individual product (identified by serial number), not merely to the model or product type. This means that even previously marketed units may be subject to new conformity assessments.

For AI systems whose development demonstrably began before 1 August 2024, the development-related requirements of the EU AI Act should be waived during conformity assessment procedures.

This approach would prevent undue disadvantage to EU-based manufacturers with legacy products and reinforce trust in the stability and predictability of the EU regulatory environment. We therefore propose amending Article 111(2) as outlined in the table in the Annex (see p. 29)

Allow sandboxes to grant presumption of conformity

Regulatory sandboxes are designed to support testing and compliance efforts by allowing companies to experiment with AI systems in a controlled environment. Established jointly or individually by Member States, these sandboxes will provide a practical space to assess how AI systems meet regulatory requirements.

Currently, Art. 57(7) states that the competent authority will issue written proof of successful sandbox activities. Providers can use this documentation to demonstrate compliance, but it only serves as evidence that may be 'taken positively into account.' This limited recognition fails to reflect the substantial effort involved in successful sandbox participation and does not adequately support companies in demonstrating compliance after exiting the sandbox.

The AI Act simplification package should specify that, upon successful exit from a sandbox, participating companies receive presumption of conformity for the tested AI system or model. This would not only enhance the attractiveness of sandboxes but also provide clear benefits to companies willing to actively engage with authorities in the sandbox environment.

Personal data to improve AI reliability and safety

To ensure that AI is reliable and safe, providers often need to process personal data throughout the AI system's development and operational lifecycle. This data is crucial not only during the early stages of development, but also for ongoing monitoring to detect and mitigate issues such as bias and performance degradation. However, the AI Act's current provisions on data processing create unnecessary limitations that may reduce the effectiveness of bias mitigation.

Art. 10(5) of the AI Act establishes an exception to Art. 9 GDPR, allowing the processing of special categories of personal data to detect and correct bias. However, the wording

is more restrictive than the GDPR itself, as it requires demonstrating that the processing is 'strictly necessary' rather than simply 'necessary.' This creates a higher burden of proof, potentially discouraging AI providers from engaging in essential data processing that could enhance system reliability and safety. Additionally, Art. 10(5)(e) mandates that special categories of personal data must be deleted once bias has been corrected. This fails to account for the need for continuous bias monitoring throughout the AI system's lifecycle, as bias can emerge dynamically when the system is in use.

Furthermore, the AI Act restricts the re-use of personal data in regulatory sandboxes. Under Art. 59, personal data lawfully collected for other purposes can only be used if the AI system serves a substantial public interest. This narrow criterion excludes companies developing AI systems for other beneficial purposes not explicitly listed, such as cybersecurity, defence, economic resilience, education, food safety and agriculture. This limitation could hinder innovation in fields where AI can deliver significant societal and economic benefits.

To address these issues, the AI Act simplification package should:

- Harmonise the standard of necessity between the AI Act and GDPR by replacing 'strictly necessary' with 'necessary' in Art. 10(5);
- Clarify that bias monitoring should continue throughout the AI system's lifecycle and that personal data used for this purpose should not be automatically deleted once initial bias correction has been achieved; and
- Amend Art. 59 to allow companies to re-use personal data they already hold for the testing and improvement of AI systems, under strong privacy safeguards, even if they do not directly serve a substantial public interest. This would ensure that useful and beneficial AI applications are not arbitrarily excluded from sandbox environments.

Replace Fundamental Rights Impact Assessment with enhanced Data Protection Impact Assessments

Art. 27 requires providers of high-risk AI systems to conduct fundamental rights impact assessments (FRIAs). These assessments evaluate how the AI system itself may impact individuals' fundamental rights, including human dignity, non-discrimination, and freedoms protected under the EU Charter. At the same time, Art. 35 GDPR requires data protection impact assessments (DPIAs) to assess how the processing of personal data may affect individuals' rights and freedoms.

Whilst the two assessments differ in focus – FRIAs assess the AI system, whilst DPIAs assess personal data processing – in practice they cover overlapping concerns. Conducting both assessments would lead to redundancy and obviously increase the compliance burden for public authorities and companies in scope.[5]

Instead of introducing a new assessment, the AI Act simplification package should clarify that the relevant deployers and providers should conduct a DPIA. Art. 27(4)

[5] Companies may be in scope through public procurement, as private entities providing public services, or as deployers AI systems for selected uses cases covered in Annex III.

already allows for this possibility, but it needs to be clarified unconditionally to ensure consistency. AI providers should be able to determine whether a DPIA is sufficient for FRIA requirements, reducing duplicate work while upholding comprehensive risk evaluation.

Additionally, the obligation to notify authorities (Art. 27(3)) should be deleted, as DPIAs under the GDPR do not have such a mandatory notification requirement. Similarly, the possibility in Art. 27(5) for the AI Office to develop a separate questionnaire should also be deleted, as it would force companies to align their DPIA practices with an additional template.

Risk of double regulation in the automotive sector

Apart from the issues outlined above regarding the sectoral regulations in Annex I, Section A, the automotive sector – covered by Section B – faces a particularly pressing risk of double regulation. Due to the extensive approval requirements set out in Regulation (EU) 2018/858, combined with the diverse technical regulations of the UNECE, all relevant aspects of AI in high-risk applications are already covered in the automotive sector – particularly in the area of autonomous driving and driver assistance systems.

An additional adoption of AI Act provisions into the vehicle type-approval regulation would lead to unnecessarily complex and duplicative documentation obligations, audits, and risk management systems – without providing any meaningful increase in safety for end users beyond what is already ensured by the existing regulations.

Moreover, such a divergence between EU type-approval regulations and those of the UNECE framework would result in significant additional economic and time burdens for the automotive industry, thereby undermining its competitiveness through new trade barriers.

In light of the issues, we recommend exempting all AI systems covered by the automotive regulations in Annex I, Section B, from the high-risk requirements of the AI Act. Accordingly, the automotive regulations should be removed from Annex I, Section B.

Remove unnecessary provisions

The AI Act introduces a range of provisions that, whilst aiming to enhance safety and transparency, may instead create unnecessary burdens or legal uncertainties without clear added value. Removing these provisions would maintain the AI Act's core protective goals without imposing impractical obligations.

Art. 72(3), for example, requires providers to follow a specific post-market monitoring plan, the framework of which will be designed by the Commission through an implementing act. This approach limits providers' flexibility in developing monitoring plans that are tailored to their specific AI systems and risk contexts. Additionally, the process for drafting implementing acts allows very limited opportunities for industry consultation and co-design. As a result, companies are unlikely to meaningfully contribute to shaping the framework, raising concerns about its practical feasibility. To address this, Art. 72(3) should be deleted. Instead, providers should have the freedom

to develop post-market monitoring plans that are adaptable to specific operational needs.

Furthermore, Art. 82 allows national authorities to require AI providers to take additional measures beyond those specified in the AI Act, 'without undue delay,' if a compliant AI system is deemed to still present a risk. Whilst the intention is to address emerging safety concerns, allowing individual Member States to impose extra measures creates inconsistent obligations across the EU. If some countries choose to enforce stricter requirements whilst others do not, the single market will suffer; on the other hand, if Member States decide to follow one another's lead, there is a risk of an unchecked expansion of the AI Act's scope. The Commission's proposed oversight is vague and limited, offering little assurance of maintaining consistency across the EU. Art. 82 should be deleted. Compliance with the AI Act should be sufficient for AI systems to be marketed throughout the EU, without the risk of additional national measures that undermine harmonisation and legal certainty.

3 Data Acquis

The recent data law acquis has brought new opportunities by increasing trust in data sharing, reducing data localisation measures, and clarifying data access rights and obligations. Nevertheless, this complex regulatory framework also impacts businesses' ability to compete internationally and comes with significant and costly implementation efforts for businesses. For the growth of the EU Data Economy – and thus the competitiveness of European companies – legally reliable access to relevant data is essential. In detail, while DA, DGA, ODD, FFNPDR, GDPR, ePrivacy Directive all have their merits, their parallel application and overlaps render them difficult to understand and implement. If laws counteract each other, legislative intention can remain unfulfilled while implementation causes high effort. Thus, we welcome the Digital Omnibus' effort to simplify digital regulation and reduce bureaucratic burdens. However, the Commission seems to exclude Data Act (DA) and GDPR (see Chapter 4) from the Digital Omnibus.

Include the Data Act in the Digital Omnibus

We highly encourage the Commission to consider the DA in the Digital Omnibus to turn it into an ambitious initiative in line with the ongoing political discourse. Including the DA is crucial to obtain a holistic picture of the data acquis and reduce the administrative burden on companies.

Concrete areas for harmonisation between horizontal digital laws, including but not limited to the reporting obligations in the DA in particular, can be found in the table in the Annex. Furthermore, we are open and committed to certain harmonisations and clarifications, including but not limited to the definitions, to the substance of the DA, already this year.

Create clarity for international data transfers

Guidance on non-personal data in international contexts under Art. 32 DA should ensure that reliance on valid GDPR mechanisms like SCCs and TOMs measures are clearly deemed as sufficient under the DA. When it comes to cybersecurity data flows, as suggested in our EDUS submission, the most effective cyber defence relies on world-wide data sources and globally distributed infrastructures and is hindered by data localization measures.[6]

Increase transparency for Cloud Standards

To ensure effective implementation of Art. 35 DA, the development of standards for technical portability and interoperability must be transparent, inclusive, and based on continuous stakeholder input. The ongoing development of the methodological framework for the standards repository should be subject to public consultation and

[6] In terms of cybersecurity data flows and international data flows more generally, see Bitkom, ↗ Feedback on the public consultation on an EU Data Union Strategy, 2025.

include continuous mechanisms for feedback and participation to reflect the complexity and broad relevance of data processing services.[7]

Reform EU Data Governance Bodies

While the EU has implemented far-reaching rules for the data economy in particular with DA and DGA, their success largely depends on fair enforcement and feasible compliance. Therefore, the EU should review enforcement mechanisms in the wider field of data policy, including at the intersection of horizontal and vertical rules. In terms of governance, there is room for improvement regarding the EDIB. Its capacity should be heightened by allocating more staff and increasing the frequency of meetings. Ideally, it should be institutionalised and brought on par with the EDPB. There is a need to increase the transparency of its nomination procedure and its work results. Decisions by EDIB (and EDPS) should be made reviewable by EGC/ECJ.

[7] See Bitkom, Feedback on the public consultation on an EU Cloud AI Development Act, 2025, ↗ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14628-AI-Continent-new-cloud-and-AI-development-act/F3571510_en.

4 Data Protection and ePrivacy Directive

The EU's data protection regulatory framework is a prime candidate for targeted simplification. We are concerned, however, that the European Commission appears to be excluding the GDPR from the scope of the Digital Omnibus. Given the considerable overlap and independence between the GDPR and new digital laws as well as the direct reliance of the ePrivacy Directive on GDPR concepts, it is essential that the GDPR is addressed within the Omnibus through targeted amendments. Adressing ePrivacy in isolation, risks perpetuating legal uncertainty, duplicative obligations, and a lack of coherence and proportionality across the digital regulatory framework. The Omnibus reform must aim to make data protection not only robust but also innovation-enabling

This interdependency will only increase if, as part of the reform, Art. 5(3) of the ePrivacy Directive is withdrawn or if all legal bases under Art. 6 GDPR are made available for the purposes of Art. 5(3). In such scenarios, the interpretation and application of the GDPR – including the scope and conditions of all legal bases for processing – will directly determine the permissibility of a wide range of activities governed by ePrivacy. This would make consistency, coherence, and proportionality between the two frameworks not just desirable, but absolutely essential.

Nonetheless, Bitkom welcomes the inclusion of the ePrivacy directive in the European Commission's call for evidence on the Digital Omnibus. The ePrivacy Directive is a striking example of an outdated rule that conflicts with and doubles on more modern GDPR consent requirements. The result – the well-known syndrome of cookie fatigue – has been counterproductive for consumers and onerous for businesses.

In our view, the reform should address the ePrivacy Directive as a whole – not just the cookie rule. The directive is no longer fit-for-purpose with the existing data protection and digital legal framework due to its isolated, sector-specific approach, and the European Commission should take a holistic approach to its reform.

70%

of German companies warn that current data protection rule hinder digital innovation (Bitkom, 2024).

Integration instead of parallel regulation

The comprehensive, technology-neutral approach of the GDPR already covers the cases of personal data processing regulated by the ePrivacy Directive. Remaining core provisions on the protection of the confidentiality of electronic communications should be transferred to a uniform European legal framework. Parallel sector-specific regulation is neither necessary nor effective.

Simplification and risk-based approach

The future legal framework should be based on a clear, risk-based approach that creates legal and planning certainty while promoting innovation and economic development in Europe. Documentation and verification requirements must be

proportionate, empowering organisations of all sizes to focus resources on high-risk scenarios.

Today, 94 % of German companies describe their data protection compliance burden as high, and in 63 % the workload has further increased over the past year. Simplification and a risk-based approach are therefore essential to ensure that resources can be focused on high-risk processing instead of excessive formalities.[8]

Modern cookie rules

In order to overcome widespread ‘consent fatigue’, the ePrivacy cookie rule requires urgent modernisation. Deleting Art. 5(3) from the ePrivacy Directive and introducing a modern, risk-based provision into the GDPR would be the most effective simplification. This would allow essential, low-risk activities to proceed on a more appropriate legal basis like legitimate interests, subject to the GDPR's robust balancing test and safeguards.

Currently, 76 % of users are annoyed by cookie banners, and 68 % say they do not want to deal with them at all. Although one third (34 %) consider cookie and tracking settings important, almost the same share (31 %) admit they do not understand them. This illustrates how the current ePrivacy consent regime has failed both in usability and effectiveness, fostering ‘consent fatigue’ instead of meaningful transparency.[9]

Harmonisation and central enforcement

It is crucial to create clear, EU-wide harmonised guidelines that replace divergent national interpretations. The different interpretations of the consent requirement (or rather the exceptions to it) by national regulatory authorities, e. g., for non-invasive analytics, lead to significant distortion of competition, massive uncertainty on the part of companies, and high legal costs.

An effective ePrivacy reform must overcome the fragmented supervisory structure. We therefore advocate the establishment of a uniform European mechanism for interpretation and enforcement. The role of the European Commission should be strengthened or, alternatively, a central body should be created to ensure consistent, innovation-friendly and legally secure guidelines.

[8] ↗ Bitkom Press Information «Datenschutz: Aufwand für Unternehmen nimmt zu«, 2024.
[9] ↗ Bitkom Press Information »Drei Viertel sind von Cookie-Bannern genervt«, 2024.

5 European Digital Identity Framework

The revised eIDAS Regulation and its Implementing Acts already establish a detailed framework for electronic identification, authentication and validation of credentials. Without careful coordination with existing and future legislation such as the upcoming EU Business Wallet (EUBW) or NIS 2, stakeholders may face duplicate or ambiguous obligations across instruments, increasing costs instead of reducing them.

Simplification should ensure that existing eIDAS provisions remain the single point of reference to ensure European interoperability. Clarifications are needed so that rules are coherent and do not overlap, providing legal certainty and a predictable compliance environment. Instead of creating new tools, existing Trust Services covered by eIDAS should be used to support new digital services and Wallet functionalities. Transparent and efficient certification and conformity assessment process must also be ensured.

A harmonised LPID for legal persons

The Legal Person Identification Data (LPID) remains insufficiently defined in practice. In countries without unified registers, organisations such as universities, churches or public authorities often lack a clear legal identity basis. At the same time, representation rights are managed inconsistently, relying on fragmented mandate registers or unstructured documentation. These gaps slow down digital processes and hinder cross-border trust.

A harmonised EU-wide LPID schema should be introduced as a foundation for the EUBW, covering entities not present in national registers and establishing common minimum criteria. This forms the basis for digitally verifying representations, ensuring legal certainty and reducing manual administrative effort.

6 Annex

1 General Information

Legal Act	Problem	Possible Solution
Cross-regulatory	**Symptom-based approach instead of addressing root causes:** General problem of inconsistent definitions and differing interpretations of legal terms. For example, »dark patterns«: the prohibition of dark patterns appears in the Data Act (Recital 38), the DSA (Art. 25), and the DMA (Art. 6(3), Recitals 50ff.). Nevertheless, the term is being used again in the preparation of the Digital Fairness Act, although it is still unclear what exactly is meant by it or there is no clear consensus on its definition.	Orientation based on the definition in Article 25 DSA, including the illustrative examples and guidelines pursuant to Article 25(3) DSA
Cross-regulatory	**Ineffectiveness of non-affectation clauses:** So called non-prejudice or non-affectation clauses do not help resolve conflicts of objectives among the various digital EU legal acts. For example, Article 2(7) AI Act, Article 2(4)(g) DSA, and Recital 7 Data Act state that the GDPR remains unaffected. Nevertheless, the EU legal acts influence and overlap with each other in many areas of practical implementation.	Specific rules on precedence Harmonized definitions (consistent terminology) Joint practical guidance and handbooks, for example issued by the Commission, which specifically describe typical conflict scenarios in practical implementation and provide solutions

2 Between GDPR and ...

Legal Act	Problem	Possible Solution
Data Act	**Data access rights under the Data Act vs. data subject rights under the GDPR:** The access rights established in the Data Act (Articles 3 – 5 DA) may potentially conflict with the rights of data subjects under the GDPR, such as the right to rectification, erasure, and restriction of processing of personal data (Articles 16 et seq. GDPR). This may result in situations where the disclosure of data under the Data Act unintentionally infringes upon individual privacy rights.	By employing pseudonymization or anonymization techniques, it can be ensured that no directly identifiable personal information is disclosed when data is shared. However, it should be noted that the use of pseudonymous data does not exempt data from the obligations under the Data Act. Therefore, the proposal is: mixed datasets should not be treated as personal data if the personal data has been pseudonymized according to recognized standards and re-identification by unauthorized third parties can be effectively excluded. Such measures allow access to the data relevant under the Data Act without violating the provisions of the GDPR. In cases where both legal acts apply, it should be assessed whether the more specific provisions of the Data Act take precedence – provided this is compatible with the protection of data subjects' rights.
Data Act	**Legal Basis under the GDPR when user and data subject roles diverge in the Data Act:** Which legal basis under the GDPR is used when the »user« under the Data Act and the »data subject« under the GDPR are not the same person?	See, in principle, recitals 7 and 34 of the Data Act. The solution could be clarification in the text of the regulation itself rather than in the recitals.
Data Act	Does the Data Act allow data processing on behalf of a data recipient, as defined by the GDPR, or must recipients always process the data themselves: Can a data recipient, within the context of a shared data economy and with the user's consent, have data processed by a processor?	The legislator should explicitly determine under which circumstances the GDPR principles are to be applied and how to proceed in cases of divergent definitions. A systematic distinction – such as through specific use cases or data categories – can serve as a guideline here.
Data Act	**Risk potential due to data classification under the Data Act:** The obligation to differentiate between personal and non-personal data and trade secrets poses significant risk potential for data holders. Unclear or incorrect classifications can lead to liability issues, competitive disadvantages, and uncertain legal consequences, for example if personal data is inadvertently disclosed without adequate safeguards.	The introduction of standardized, technical procedures for automated data classification supports data holders in correctly categorizing their data. Certification programs for data management systems can serve as proof of compliance with these standards and strengthen trust in the applied procedures.

Legal Act	Problem	Possible Solution
Data Act	**Circumventing the Data Act through data mixing:** Companies that are not interested in data sharing might attempt to mix generated data with personal data in order to circumvent the scope of the Data Act. This would undermine the intended transparency and access to data, while at the same time ensuring data protection above the requirements of the GDPR.	Option 1: Provide clear, legally binding requirements for pseudonymization and anonymization. Option 2: In case of doubt, give precedence to the right of data access when personal data is pseudonymized in accordance with recognized standards. Recognition of codes of conduct for pseudonymization, a common understanding among supervisory authorities, and Commission guidelines. However, since pseudonymized data is currently still considered personal data, only anonymization is an option.
Data Act	**Distinction between the GDPR right of access and the Data Act right of data access:** The right of access under Article 15 GDPR is primarily intended to allow data subjects to obtain insight into the personal data stored about them. The right of data access under the Data Act, on the other hand, is intended to facilitate standardized and broad access to data-including personal data. This raises the question of what specific benefits this new data access right provides over the existing right of access under the GDPR.	Critically examine the role of the individual user in the context of data disclosure. It may be sufficient for the contractual obligation alone to justify data sharing, without the need for a proactive request for access by the user.
Data Act	**Tension between GDPR data portability and Data Act access rights:** The GDPR (e. g., Articles 5, 6, and 7) imposes strict requirements for the processing of personal data. The Data Act, on the other hand, aims to facilitate access to and sharing of data-including data generated by connected devices. Article 20 GDPR (right to data portability) must be reconsidered in light of the Data Act, which may provide for broader data access rights.	It should be examined to what extent the existing concept of data portability meets the requirements of the Data Act. An adjustment to Article 20 GDPR could involve expanding its scope or integrating differentiated protection mechanisms that solely take into account the extended access rights provided for in the Data Act . A revision and harmonization of the relevant provisions of the GDPR and the Data Act should be carried out to create a consistent legal framework. This includes, in particular, ensuring that the extended data access rights do not undermine the rights of data subjects.
Data Act	**Conflict of objectives between data access and data protection in the Data Act:** The Data Act, with »Access by Design,» calls for the simplest and most standardized access possible to large amounts of data-including personal data-to	Note: Regardless of the Data Act, products and services that process personal data must generally comply with the requirements of Articles 25 and 32 GDPR. It would be paradoxical to dispense with these requirements the more interconnected these products and related services become and thus the higher the

Legal Act	Problem	Possible Solution
	promote innovation and competitiveness. In contrast, the GDPR requires «Privacy by Design,» meaning that the protection of personal data must be integrated into products and processes from the outset. These objectives can come into conflict during product development, as unrestricted data access cannot be realized without risk to user privacy.	risk. Moreover, Privacy by Design and Access by Design do not have to be contradictory if both principles are considered together from the outset.
AI Act	**Overlap between record-keeping obligations and AI Act requirements:** Article 30 GDPR requires companies to maintain a record of processing activities-a requirement that is similar to the risk assessment and post-market monitoring obligations under the AI Act. These overlaps may result in redundant administrative burdens and complicate the consistent application of the regulations, especially for companies that process personal data and use AI systems.	Development of unified guidelines that take both legal frameworks-GDPR and AI Act-into account and establish a common standard for documentation of processing activities, risk assessments, and monitoring processes. Clarification of cases where supplementary evidence (e. g., post-market monitoring for AI systems) is required in addition to the standard requirements of Article 30 GDPR.
AI Act	**Need for integrated risk assessment:** Article 2(7) AI Act states that the GDPR remains unaffected. Nevertheless, the AI Act influences the practical implementation of the GDPR in many areas, especially in balancing interests, risk assessments, and liability issues.	Integrating the risk assessments of the AI Act (e. g., fundamental rights risk analyses) into data protection impact assessments under Article 35 GDPR is considered sensible to avoid duplication (see above).
AI Act	**Conflict between data minimization and anti-bias measures in AI development:** A tension arises from the principle of data minimization and anti-bias measures in generative AI or non-high-risk AI. Article 9 GDPR generally prohibits the processing of sensitive data (e. g., ethnic origin, religion, health) unless an exception applies (e. g., public interest). Article 10(5) AI Act permits the processing of sensitive data in high-risk AI systems to detect and mitigate discrimination. However, this exception does not apply to generative AI or non-high-risk systems, despite the potential for discrimination in these contexts as well. The GDPR requirements often stand in the way of the necessary processing of sensitive data for bias reduction. Developers could face high liability risks if they use data to combat discrimination.	Extension of existing exceptions for the processing of sensitive data so that they also apply to generative AI or non-high-risk systems, provided this explicitly serves the purpose of preventing discrimination. Clear safeguards would need to be established for this, such as strict purpose limitation, pseudonymized or anonymized data sets, and binding risk and impact assessments that protect the rights and freedoms of data subjects.

Legal Act	Problem	Possible Solution
AI Act	**Tension between data collection and performance:** There is a conflict between the performance requirements of the AI Act (Article 15) and the provisions of the GDPR (Article 9). Article 15(1) AI Act requires an «appropriate level of accuracy» for high-risk systems, where accuracy should rightly be interpreted as performance in terms of technical quality standards. However, for the development of powerful AI models, especially in the medical field, the processing of sensitive data (e. g., health data) is sometimes necessary. The use of such data may be required under the AI Act to ensure sufficient performance and coverage of diverse population groups by the AI model. Article 9 GDPR, on the other hand, generally prohibits the use of certain categories of sensitive data.	It would be possible to create a narrow exception that explicitly allows AI developers in high-risk applications or similarly sensitive fields to process sensitive data under strict conditions, provided this is absolutely necessary for the required accuracy and performance of the models. Robust safeguards such as pseudonymization, encryption, clear purpose limitation, and comprehensive risk and impact assessments could be prescribed to ensure data protection requirements are met.
AI Act	**Reuse of personal data for training AI models:** There is a lack of clear regulation regarding the reuse of personal data for training AI models. Whether the use is lawful depends-especially in light of the purpose limitation principle under Article 5(1)(b) GDPR – heavily on the individual case. Obtaining consent retrospectively for AI training would often not be practical.	Creation of a clear, uniform legal basis that allows, under certain conditions, the use of personal data from already collected datasets for AI training without the need to obtain new consent each time. This legal basis could be subject to strict conditions, such as purpose limitation, pseudonymization, risk assessments, and restricting use to cases where it is necessary to fulfill a legitimate, public-interest, or clearly defined purpose (e. g., research, improvement of systems for medical diagnosis).
AI Act	**Provider-operator reversal:** Under the GDPR, the operator of the AI system is responsible for compliance with data protection requirements. The AI Act places the main obligations on the provider of the AI system. This can lead to uncertainties regarding liability, e. g., in the case of errors in high-risk AI systems. In some cases, providers and operators may be held jointly liable. There is a lack of clear coordination of responsibilities here.	Clarifications are conceivable in both the AI Regulation and the GDPR.
AI Act	**Duplication of reporting obligations to supervisory authorities:** Article 33 GDPR: Notification of data breaches to the supervisory authority – notification within 72 hours. In high-risk cases, also to the data subject (Article 34 GDPR).	Harmonizing regulatory obligations to prevent duplication and reduce excessive bureaucracy.

Legal Act	Problem	Possible Solution
	Article 73 AI Act: Providers of high-risk AI systems are required to establish 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 simultaneously leads to a data breach (e. g., unauthorized access or loss of personal data), both the reporting obligations under Articles 33, 34 GDPR and the incident reporting under Article 61 AI Act apply → potentially resulting in duplicate reporting.	
AI Act	**Overlap of IT security requirements:** Article 32 o GDPR and Article 16 AI Act go hand in hand, as both require those responsible to implement appropriate security measures, without clarifying the relationship between the provisions.	Reporting obligations should be consolidated here.
AI Act	**Divergent high-risk classification:** High-risk applications under the AI Act and those considered high risk under the GDPR do not necessarily coincide. AI-based profiling systems are almost always classified as high risk under the GDPR, but not necessarily under the AI Act (see Article 5(1)(d) AI Act).	Integration of the data protection impact assessment under Article 35 GDPR with the fundamental rights risk analyses under Article 27 of the AI Act.
DSA and DMA	**Divergent profiling regulations:** There are numerous regulations on profiling that are not fully harmonized (see Recital 71, Article 22 GDPR, Recital 72, Article 15(1) DMA, and Recitals 68 ff., Article 26(3), Article 28(2), Article 38 DSA).	
DSA and DMA	**Conflicts between transparency obligations and data minimization:** Conflicts between transparency obligations (see DSA, DMA, and P2B Regulation) and the GDPR principle of data minimization under Article 5(1)(c) GDPR.	Open
GDPR and DORA	Pseudonymized Data: Article 16(5) RTS risk management under the DORA Regulation Pseudonymized data may be stored in non-production environments. Recital 26 GDPR. Pseudonymized data is considered personal data	DORA Regulation is in technical conflict with the GDPR. Under DORA, something is permitted that is generally prohibited under data protection law.

Legal Act	Problem	Possible Solution
DORA Regulation and Solvency II duplication	Notification of outsourcing according to §§ 32 and 47 No. 8 VAG and, in parallel, notification obligations under Article 28(3) DORA Regulation. Notification of serious ICT incidents to BaFin under Article 19 DORA Regulation, in parallel with the notification obligation under § 47 No. 9 VAG.	The same matter is reported to the same supervisory authority under two different »legal regimes.«
AI Act and Data Act	Create unified documentation of processing activities and product/data inventory.	
ePrivacy Directive	**Different reporting obligations for data protection incidents:** Data protection incidents must be reported to the competent data protection supervisory authority within 72 hours in accordance with Article 33 GDPR. Data protection incidents in the field of electronic communications must, however, be reported to the BNetzA and the BfDI within 24 hours in accordance with §169 TKG in conjunction with Regulation 611/2023 EU.	Elimination of sector-specific special regulations for electronic communications.

3 Between AI Act and ...

Legal Act	Problem	Possible Solution
AI Act	**Risk of Absence of grandfathering provisions for legacy products** The absence of grandfathering provisions in the EU AI Act poses a significant risk to the continued availability of well-established NFL-products on the EU market. For AI systems whose development demonstrably began before 1 August 2024, the development-related requirements of the EU AI Act should be waived during conformity assessment procedures. This approach would prevent undue disadvantage to EU-based manufacturers with legacy products and reinforce trust in the stability and predictability of the EU regulatory environment.	Modify Art. 111 (2) as follows: Therefore, we propose to modify Art. 111 (2) as follows: «Without prejudice to the application of Article 5 as referred to in Article 113, ~~(3)~~ *3rd sentence*, point (a), *those type of* ~~this Regulation shall apply to operators of~~ (a) high-risk AI systems *pursuant to Annex III,* other than the systems referred to in paragraph 1 of this Article, that have been *legally* placed on the market or put into service before 2 August 2026, *and* *(b) high-risk AI systems pursuant to Annex I, other than the systems referred to in paragraph 1 of this Article, that have been legally placed on the market or put into service before 2 August 2027,* *all in accordance with the applicable rules in force at the time of their placing on the market or putting into service, may continue to be placed on the market or put into service* ~~only if, as from that date ,~~ *unless* those systems are subject to significant changes in their designs, *in which later case this Regulation shall apply to those systems*. In any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps to comply with the requirements and obligations of this Regulation by 2 August 2030.»
Medical Devices Regulation	**Insufficient coordination of risk classifications:** According to the AI Act, all AI systems that are either themselves subject to third-party certification or constitute safety components of such a product pursuant to Annex Ia AI Act are considered high-risk AI systems. However, the regulations and directives listed under Annex Ia also include the Medical Devices Regulation. This stipulates that software products in the medical field are subject to third-party certification regardless of their inherent medical risk. As a result, such software products are invariably classified as high-risk under the AI Act, regardless of their actual risk potential.	Open

Legal Act	Problem	Possible Solution
	The interplay between Rule 11 of the MDR and the risk classification under the AI Act runs counter to the risk-based approach of both sets of rules and represents a disproportionate regulatory burden for medically harmless products. This issue needs to be clarified at the EU level.	
Finance	There is no provision regulating which elements of the data and data governance requirements (Art. 10 AI Act) for high-risk AI systems in the financial sector are already covered by the data governance requirements set out in Article 174 of the Capital Requirements Regulation (CRR). Furthermore, it is unclear to what extent existing documentation and transparency requirements in the banking sector, such as those set out in MaRisk, already fulfill the requirements of the AI Act. The same applies to the cybersecurity requirements under DORA.	Establish legal certainty by ensuring the broadest possible recognition of existing sector-specific regulatory practices and by introducing rules to avoid duplicate reporting obligations.
DSM-Directive/ EU Copyright Law	Reference to individual provisions of the DSM Directive is generally acceptable. Problem: Recital 106 of the AI Act presents a challenge, as it introduces a provision within a product safety regulation that directly contradicts the copyright principle of territoriality. It remains unclear whether this is a safety – related or a copyright - related provision – this has, among other things, a significant impact on who can assert the «obligation» set out in Recital 106.	TBD: Recital is related to Art. 53 AI Act. According to Art. 53 AI Act, the provider is obliged.
Machinery Regulation	**Different handling of the term safety component:** Under the AI Act, an AI system functioning as a safety component is only regulated as part of a product, whereas the Machinery Regulation always provides for the separate regulation of a safety component apart from the product.	Open
Product Liability Directive	If a company violates the AI Act, this generally also leads to liability under product liability law or general tort law. However, companies could also be liable in individual cases even if they comply with the AI Act. This would mean double and potentially conflicting requirements for companies.	Open

Legal Act	Problem	Possible Solution
Product Liability Guideline	When is an AI model considered a product, especially if it is not an AI system? Is placing on the market sufficient, or is actual commissioning required? Highly relevant in the R&D sector.	As soon as there is an intended purpose for commissioning in the sense of a specific application.

4 Between Data Act and ...

Legal Act	Problem	Possible Solution
GDPR	The distinction between personal and non-personal data under the Data Act (DA) and the GDPR carries significantly different consequences. This distinction is often unclear, creating substantial compliance risks. The Data Act does not provide a legal basis for processing – what applies to mixed datasets? (see above).	Introduce a legal basis under the GDPR in the Data Act for the processing of personal data. According to Recital 34, the GDPR applies. A provision in the regulatory text itself, not just in the recitals, would be preferable.
GDPR	Third parties are generally prohibited from profiling based on received data under Article 6(2)(b) DA. This prohibition applies without prejudice to Article 22(2)(a) + (c) and Recital 71 GDPR. Depending on the interpretation of these provisions, profiling rules for non-personal data could be stricter than for personal data, which is counterintuitive.	Critically evaluate Article 6(2)(b) DA and delete it if necessary, or at least align it with the GDPR.
AI Act	Article 10 AI Act regulates data quality, data management, and data governance requirements for high-risk AI systems. It is unclear how these requirements relate to the data governance requirements in Article 33 Data Act and how both regulatory areas are operationalized.	Open
Article 101/102 TFEU (Antitrust rules)	It is not entirely clear how data-sharing claims under Chapter II DA (particularly the exceptions in Articles 4(6) ff. and 5(9) ff. DA) interact with antitrust prohibitions under Articles 101 and 102 TFEU, especially Chapter VI of the HBER Guidelines (Information Exchange). The former requires disclosure of sensitive data (including trade secrets) under certain conditions, while the latter aims to prohibit the exchange of sensitive data. Recital 116 DA ostensibly resolves this («This Regulation should not affect the application of competition rules [...]»). However, it is disputed whether Recital 116 DA prohibits any disclosure of trade secrets to third parties, as this would render the «safeguard mechanisms» (e. g., Articles 4(6) ff., 5(9) ff. DA) redundant.	Clarify that antitrust rules under the TFEU take precedence in case of conflict.
Data Act	The language and scope of pre-contractual information obligations under Article 3(2)-(3) DA are unclear. Compatibility with other information obligations is also unresolved.	Clarify at the regulatory level that pre-contractual information obligations may be combined with those set out in other EU legal acts and that they need only be provided in English.

Legal Act	Problem	Possible Solution
Data Act	Even in the absence of anyone's dissatisfaction, complaint or other specific reason, the entirety of data holders is supposed to supply the competent authorities with transparency concerning circumstances around (prima facie justified) withholding of data, which seems rather inappropriate for data holders and difficult if not impossible to digest for competent authorities. In fact, even without these extensive bureaucratic reporting obligations, if there is a potential initial suspicion, data recipients can use all usual legal instruments to claim their rights. In addition, Article 37 (14) DA already mandates relevant supervisory authorities to gather information about DA compliance from data holders: In case of a substantiated complaint to the relevant supervisory authority (Article 37 (5)(b), 38 DA) comprehensive information from the data holder to validate the complaint can already be requested	Tee reporting obligations foreseen in the following articles of the DA should be deleted: ▪ Article 4 (2) last sentence, (7) last sentence, (8) last sentence DA ▪ Article 5 (10) last sentence, (11) last sentence DA ▪ Article 8 (3) last sentence DA ▪ Article 20 (2) last sentence DA.
Data Act	Regarding the contractual requirement under Article 4(13) DA, the language and scope are unclear. In addition, it remains open whether data transfer agreements can be combined with other clauses. Article 5 DA also does not clearly specify that a contractual relationship is required between data holders and data recipients.	At the latest at the regulatory level, it must be clarified that the contract may be combined with other contracts and that it only needs to be provided in English. Note: The EU Commission has already attempted to address this through model contracts under Article 41 DA.
Data Act	Article 9(7) DA requires data holders to disclose their cost structures (including cost calculations) – without any handbrakes or thresholds. A requirement that is not only frequently difficult or impossible to fulfil due to contractual confidentiality obligations, but is, in many cases, outright prohibited under EU competition law. It is a well-established principle of antitrust law that the disclosure of purchase prices between competitors is problematic. However, this is precisely what Art. 9 (7) DA appears to mandate. It must be taken into account that data holders and data recipients are often direct competitors with respect to key cost com-ponents – for instance, when procuring data storage capacity from providers such as large cloud providers. Moreover, beyond the demand-side markets, data holders and recipients frequently compete in downstream markets as well (e. g., OEM and OES in the market for data-driven	The extensive disclosure obligations of data holders under Article 9(7) DA – that is the whole paragraph – should be removed. In the event of disputes regarding this matter, the ordinary legal process remains fully accessible.

Legal Act	Problem	Possible Solution
	products for automotive repair services). As a result, data holders are placed in a legal dilemma created by two conflicting EU legal instruments. If they comply with the transparency obligation under the DA, they risk violating competition law. Conversely, if they refrain from disclosing their cost calculations, they face the risk that, in the event of a dispute, a court may consider their fees to be excessive.	
Data Act	Article 26 DA: Information obligations on switching methods and online registers. How can these be integrated with other obligations? Language? Scope?	Clarify at the regulatory level that information obligations may be combined with others and only need to be provided in English.
Data Act	Article 28 DA: Transparency obligations for providers on their websites. How can these be integrated with other obligations? Language? Scope?	Clarify at the regulatory level that information obligations may be combined with others and only need to be provided in English.

5 Between NIS-2 Directive and ...

Legal Act	Problem	Possible Solution
Data Act	The Data Act requires the disclosure of data, even in security-critical contexts. This may conflict with the NIS-2 Directive's requirements for confidentiality and encryption. Especially in critical infrastructures, data access can pose cybersecurity risks if there is no unified regulation.	Clarify that in case of conflict, national implementation of the NIS-2 Directive takes precedence.
CRA	The NIS-2 Directive permits the adoption of delegated acts according to Art. 24(2) NIS-2 Directive regarding the mandatory use of certified ICT products. This can directly overlap with the CRA and increase administrative effort.	CE marking in accordance with the CRA should be sufficient as a requirement for ICT products.
GDPR	Significant security incidents under the NIS-2 Directive may also constitute a data protection incident under the GDPR. As a result, affected companies in Germany are bound to report to various authorities. NIS2 focuses on restoring information security and cybersecurity, while the GDPR centers on protecting the rights and freedoms of natural persons and enabling them to minimize risks. This can lead to conflicts, particularly when both frameworks apply simultaneously to the same incident.	GDPR and NIS2 protect different legal interests. Rather than a blanket precedence of NIS2, a unified notification would be preferable.

6 Between CRA and ...

Legal Act	Problem	Possible Solution
among others GDPR/ NIS-2 Directive	**Reporting obligations (GDPR, NIS-2 Directive, etc.):** Articles 14(1) and (3) CRA require manufacturers to report serious incidents affecting the security of the product and actively exploited vulnerabilities to ENISA. This may overlap with Article 33 GDPR and Articles 7, 21 NIS-2 Directive.	Clarify which legal basis takes precedence in the event of a conflict. Ideally, introduce a one-stop-shop for reporting.
DORA	Companies in the financial sector, especially those offering digital services or products, may fall under several regulations at the same time, leading to overlapping compliance requirements.	Use delegated acts to determine that DORA takes precedence as lex specialis in the event of overlap.
AI Act	Overlaps and potential inconsistencies in cybersecurity requirements between the AI Act and CRA. Possible overlaps and contradictions between Article 15 AI Act on accuracy, robustness, and cybersecurity for AI systems and the requirements of the CRA.	Harmonization of standardization work.
Ecodesign Regulation	Updates of software and firmware must not lead to a deterioration in product performance. This creates a conflict of objectives with the Cyber Resilience Act.	
NIS2	Uniform understanding of direct or indirect material damage.	

7 Between DMA and ...

Legal Act	Problem	Possible Solution
GDPR	**Conflict of objectives between service openness and security/protection regulations:** Various access rights and interoperability obligations under the DMA may conflict with cybersecurity and GDPR provisions (e. g., Privacy by Design) if the (newer) DMA provisions are not interpreted consistently with existing regulations.	Open
Data Act, DSA and P2B Regulation	Dark patterns (see above), profiling (see above), and a multitude of other overlaps	See above

8 Between DSA and ...

Legal Act	Problem	Possible Solution
GDPR	The DSA contains a provision prohibiting the use of dark patterns, which also applies to the design of cookie banners. However, the relationship to the GDPR is not clear or unambiguous. The EU repeatedly addresses this by stating that requirements from the GDPR or other legal acts do not apply. Some of these contradict the new provisions. The non-prejudice clause under Art. 2(4)(g) DSA does not help in this regard.	Open
P2B Regulation	There are initial deviations in the definitions in Art. 2(2) P2B Regulation and Art. 3(a) DSA. In addition, there are overlaps between Arts. 20, 21 DSA and Arts. 11 and 12 P2B Regulation. The non-prejudice clause in Art. 2(4)(e) DSA does not help in this regard.	Open
UCP Directive	According to Art. 25(2) DSA, the prohibition of so-called «dark patterns» does not apply to practices covered by the UCP Directive 2005/29/EC. However, it remains unclear what the remaining scope of the provision should be in this case.	Open

9 Between DGA and ...

Legal Act	Problem	Possible Solution
Data Act	A company can simultaneously be a) a provider of a data intermediation service under Art. 2(11), Arts. 10 et seq. DGA, b) a data altruism organization under Art. 2(16), Arts. 16 et seq. DGA, and c) an operator of a data space under DA Art. 33. It is also conceivable that the data space or a system within it qualifies as a data processing service under Art. 2(8) DA. While a), b), and c) directly entail different rights and obligations, the rights and obligations for d) lie with the participants of such a data space, which will very likely also require certain adjustments by the data space operator. In total, this means that, under the Data Act and DGA alone, four concepts may apply to a company simultaneously, without their relationship to each other being explained or structured.	Replace the concept of data intermediation services in the DGA with the concept of data spaces. Retain the concept of data altruism organizations. Clarify that entities can be data spaces or, alternatively, data altruism organizations or neither. The objectives and underlying principles of the DGA must be preserved.
Data Act	Art. 12(d) DGA stipulates that the provider of a data intermediation service must support data exchange and, in certain cases, convert data into specific formats. Art. 33(1) DA, in turn, stipulates that the description of «data structures, data formats, vocabularies, classification systems [etc.]» must be provided by the participant in data spaces. Against this background, it is unclear why both are required in parallel.	Resolve by aligning the material scope: replace data intermediation services in the DGA with the concept of data spaces.
Data Act	Art. 12(j) DGA requires the provider of a data intermediation service to take certain measures to prevent unlawful transfer of non-personal data to third countries. If a data intermediation service or its subsystems (e. g., for pseudonymization or temporary storage, cf. Art. 12(e) DGA) qualify as a data processing service under the DA, then the obligations to prevent unlawful transfers of or access to non-personal data under Art. 32 DA also apply. The relationship between these obligations is neither explained nor structured.	With regard to technical and organizational measures under Art. 12(j) DGA, refer to those under Art. 32 DA.
GDPR	It is unclear how Art. 12(j) DGA and the GDPR relate to each other. The former protects non-personal data, the latter protects personal data. This is a problem when both personal and non-personal data are processed in parallel and separation is not	Establish clear and legally binding requirements for pseudonymization and anonymization.

Legal Act	Problem	Possible Solution
	practically possible. The distinction between personal and non-personal data under the DGA and GDPR entails significantly different consequences. This distinction is often uncertain and leads to major compliance risks.	

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Jana Gaulke | Head of Brussels Office
P +49 30 27576-315 | j.gaulke@bitkom.org

Responsible Bitkom Committee
WG Public Affairs