Call for Evidence: Digital Fitness Check

bitkom

Call For Evidence: Digital Fitness Check

March 2026

Europe's digital economy stands at a critical crossroads. The European Union's digital regulatory landscape has expanded rapidly over the past decade, with the introduction of instruments such as the General Data Protection Regulation (GDPR), the Data Act (DA), the Data Governance Act (DGA), the Digital Services Act (DSA), the Digital Markets Act (DMA), and many more. While each of these initiatives pursues important and legitimate objectives, their cumulative effect has created a regulatory framework that is increasingly complex and difficult to navigate.

According to forecasts, the United States will account for 41% of the global Information and Communication Technology (ICT) market, China 11%, the EU (excluding Germany) 11%, and Germany 3.9%, while the rest of the world accounts for 36.2% (Bitkom, 2026). These figures send a clear message: Europe risks falling behind in a rapidly evolving global digital economy.

While the European Commission's Digital Omnibus represents an important step toward simplifying Europe's digital rulebook, it is not yet sufficient to remove the barriers that continue to hold back the full potential of Europe's digital economy today. The "Digital Fitness Check", announced alongside the Digital Omnibus in November 2025, provides an opportunity to go beyond the proposals of the Digital Omnibus and identify further regulatory overlaps and inconsistencies, to ensure that the European Union's digital rulebook is effective, proportionate, and fit for the future. It is essential that the European Commission fully seizes this opportunity to address the remaining obstacles to growth and innovation, rather than introducing additional regulatory layers, such as foreseen with the upcoming Quality Jobs Act targeting AI and algorithmic management in the workplace.

This position paper highlights concrete articles in numerous legislative acts where targeted action is needed to simplify rules and create a framework that truly supports innovation and competitiveness. We welcome the opportunity to contribute to the European Commission's ongoing call for evidence and provide practical insights and recommendations to ensure that any simplification measures are both effective and aligned with the needs of businesses operating in Europe's digital economy.

Content

1 General Information

Legal Act	Problem
Cross-regulatory	**Inconsistent definitions and differing interpretations of legal terms:** 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.
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. Instead, specific rules on precedence, a harmonized definition, and joint practical guidance and handbooks providing solutions are required.
Outdated digital regulation	**Copyright levies** National copyright levies on digital devices and storage media, intended to compensate for private copying, an activity that is steadily declining, have created a fragmented landscape of rules, higher costs, and additional compliance burdens for cross-border businesses. In light of the modernised EU copyright framework, this approach appears outdated, duplicative, and a source of legal uncertainty.

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	**'User' vs. 'data subject'** 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	**Data processing under the GDPR and the 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	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

Legal Act	Problem	Possible Solution
	incorrect classifications can lead to liability issues, competitive disadvantages, and uncertain legal consequences, for example if personal data is inadvertently disclosed without adequate safeguards.	compliance with these standards and strengthen trust in the applied procedures.
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

Legal Act	Problem	Possible Solution
		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 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.	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 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 and definition of key terminology in overlapping aspects 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	**Redundancies DPIAs and FRIAs** Article 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, Article 35 GDPR requires data protection impact assessments (DPIAs) to assess how the processing of personal data may affect individuals' rights and freedoms.	Best would be to remove the fundamental rights impact assessments (FRIAs) set in Art. 27 to safely avoid redundancy as suggested in our AI Act Omnibus feedback. A second best option would be to integrate the risk assessments of the AI Act (e.g., fundamental rights risk analyses) into the data protection impact assessments under Article 35 (see above).

Legal Act	Problem	Possible Solution
	Whilst the two assessments seem to differ in focus – FRIAs assess the AI system, whilst DPIAs assess personal data processing – in practice they cover practically the same concerns	
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.
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.

Legal Act	Problem	Possible Solution
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 Act 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). 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.	Harmonising regulatory obligations to prevent duplication and reduce excessive bureaucracy.

Legal Act	Problem	Possible Solution
AI Act	**Overlap of IT security requirements:** Article 32 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.
DSA and DMA	**Divergent profiling regulations:** There are numerous regulations on profiling that are not fully harmonised (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).	Open
DSA and DMA	**Conflicts between transparency obligations and data minimisation:** Conflicts between transparency obligations (see DSA, DMA, and P2B Regulation) and the GDPR principle of data minimisation under Article 5(1)(c) GDPR.	Open
GDPR and DORA	**Pseudonymised Data**: DORA explicitly promotes the use of pseudonymized data in test and development environments to strengthen ICT security and protect production systems. At the same time, the GDPR continues to treat pseudonymised data as personal data, due to strict purpose limitation and data minimisation requirements. This creates legal uncertainty for financial entities, as a security measure encouraged under DORA may be considered problematic from a data protection perspective. In practice, this tension often leads to overly cautious compliance approaches and unnecessary operational complexity.	DORA and the GDPR should be interpreted in a complementary, risked-based manner. The use of pseudonymised data for clearly defined testing and security purposes should be recognized as a legitimate safeguard, without triggering additional bureaucratic requirements. Existing technical and organisational measures should be considered sufficient to meet both frameworks. This approach would strengthen ICT security while preserving legal certainty and innovation capacity.
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.	The same matter is reported to the same supervisory authority under two different "legal regimes."

Legal Act	Problem	Possible Solution
	Notification of serious ICT incidents to BaFin under Article 19 DORA Regulation, in parallel with the notification obligation under § 47 No. 9 VAG.	
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
Finance	**Unclear Alignment with Existing Financial Regulations:** 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	**Legal Uncertainty over recital 106 AI Act:** Reference to individual provisions of the DSFM Directive is generally acceptable. However, 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.	Clarification, that the Recital is related to Art. 53 AI Act. According to Art. 53 AI Act, the provider is obliged. to develop and maintain a copyright compliance strategy, Recital 106 does not create an autonomous or generally enforceable rule, nor does it affect the territorial scope of copyright law.
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.	Prioritize the definition set forth in the Machinery Regulation — in particular by clarifying that the criterion of "self-evolving behaviour" is decisive in determining whether a component qualifies as an AI safety component at all.

Legal Act	Problem	Possible Solution
Platform Work Directive (PWD)	Algorithmic management systems used by digital labour platforms may fall within the scope of the AI Act and be classified as high-risk AI systems in the area of 'employment, workers' management and access to self-employment' (Article 6(2), in conjunction with Annex III, Number 4 of the AI Act). Therefore, there is an overlap between the two legislative acts. This is particularly the case with regard to **transparency and information rights** (Art. 13, Art. 26 (7), Art. 26 (11), Art. 50 AI Act and Art. 9 PWD), **human oversight** (Art. 14, Art. 26 (2) AI Act and Art. 10 PWD) and **human review** (Art. 86 AI Act and Art. 11 PWD).	In order to achieve more legal certainty and reduce administrative burden, the extensive requirements of the Platform Work Directive regarding transparency, human oversight and human review should be streamlined. Furthermore, overlapping obligations between the AI Act and PWD must be applied consistently.

4 Between Data Act and ...

Legal Act	Problem	Possible Solution
GDPR	The distinction between personal and non-personal data under the 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 section 2).	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	**Profiling obligations under the Data Act and the 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	**Unclear alignment of high-risk AI data governance requirements:** 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)	**Data sharing under the Data Act vs. antitrust prohibitions:** It remains unclear how mandatory data-sharing obligations under Chapter II of the Data Act interact with EU competition law, particularly the rules on anti-competitive information exchange under Articles 101 and 102 TFEU and Chapter 6 of the Horizontal Guidelines. While Recital 116 states that the Data Act is without prejudice to competition law, this may create legal uncertainty for data holders required to disclose commercially sensitive data to third parties, including potential competitors.	Data sharing required under the Data Act shall not in itself constitute an infringement of Articles 101 or 102 TFEU.

Legal Act	Problem	Possible Solution
	Without further clarification, companies may invoke competition law risks to refuse data access requests, potentially undermining the effectiveness of the Data Act.	
Data Act	**Unclarity of pre-contractual information obligations:** 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 only need to be provided in English.
Data Act	**Transparency Obligations for Data Holders:** 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.	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	**Unclear Scope of Articles 4(13) and 5 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 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.

Legal Act	Problem	Possible Solution
Data Act	**Tensions between cost disclosure and antitrust rules:** 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 components—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 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.	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.
Data Act	**Information obligations under Article 26 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	**Transparency obligations under Article 28 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.

Legal Act	Problem	Possible Solution
UCPD et al	**Overlaps in existing dark pattern laws:** In recital 38 the DA bans "dark patterns"' in digital interfaces. It is unclear how this and the other multiple laws that already regulate "dark patterns" interact. The recital also gives a definition that differs from those in other contexts.	Clarify how this interacts with the other regulation on 'dark patterns'.

5 Between NIS-2 Directive and ...

Legal Act	Problem	Possible Solution
Data Act	**Disclosure of data in security-critical contexts:** 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, unregulated data access can pose severe cybersecurity risks.	Clarify that in case of conflict, national implementation of the NIS-2 Directive takes precedence.
CRA	**Potential overlap between NIS-2 delegated acts and CRA:** The NIS-2 Directive permits the adoption of delegated acts according to Article 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	**Conflicting obligations for security and data protection incidents:** 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.
Among others GDPR/CRA	**Overlapping cyber incident reporting:** Article 23 NIS-2 Directive mandates multi-stage reporting for significant cyber incidents, within 24 hours, 72 hours, and a month to national CSIRTs/authorities. This may overlap with Article 33 GDPR and Articles 14(1) and (3) CRA.	Align reporting process and time limits, formats etc. between all cyber regulations with similar reporting requirements like CRA, NIS2, DORA, AI Act, GDPR etc. Introduce a single reporting platform which allows continues communication in English.

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 Article 23 NIS-2 Directive.	Align reporting process and time limits, formats etc. between all cyber regulations with similar reporting requirements like CRA, NIS2, DORA, AI Act, GDPR etc. Introduce a single reporting platform which allows continues communication in English.
DORA	**Regulatory overlap for financial sector companies:** 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.
CSA/NLF	**NLF unsuitability for intangible products and agile software:** NLF was mainly developed for tangible products, but not for intangible products such as software, especially not for software downloads. This leads to legal uncertainty for concepts such as "making available", "recall of a product", "software as a service", "product version" or agile software development with new software versions every day. Re-certification requirements for Module H (after a "significant update") currently rule out this specific module as a solution. Due to these flaws, security requirements reduce competitiveness of the EU software industry.	All requirements and processes under the NLF should be reviewed with regard to their practical applicability to (online-distributed) software products. The fundamental concepts of a software "product" and a "product version" need to be adapted to reflect continuous updates. Where legal uncertainty exists, clear and unambiguous definitions should be introduced. The NLF and the conformity assessment procedures currently lack a module that enables a shift from a static «product version" perspective towards a process-based approach. Alternatively, Module H should be revised to allow for software updates and significant changes without requiring full re-certification. In addition, documentation requirements need to be adjusted, as it is not feasible to reasonably document an object that is subject to continuous change.

Legal Act	Problem	Possible Solution
NIS-2/CRA	**Regulatory overlap for digital-only software products:** CRA focuses on products with digital elements, including software and its cloud components. Pure cloud software is handled by NIS-2 in terms of security. However, for software without a physical component, there is a continuous transition between cloud and on-premises products. In essence, the same product can be pure cloud software, pure on-premises software, or anything in between. This transition is inherently problematic because the requirements of NIS-2 and the CRA are not harmonized, leading to inconsistent and often conflicting compliance paths for the same service ecosystem.	Establish a materiality threshold under the CRA for products that consist predominantly of cloud-based services and only include negligible amounts of distributed software, or alternatively a presumption of conformity between NIS-2 and the CRA, possibly facilitated through the European Cybersecurity Certification Framework (ECCF). This would allow for a more seamless integration of requirements without imposing redundant bureaucratic hurdles. Furthermore, a clarifying interpretation of the system of placing products on the market could be helpful. Neither a change in the distribution channel nor provision via the cloud should be considered a new placing on the market; clear guidelines must be provided for this.
NIS-2, AI Act, CSA, NLF	**Excessive compliance costs:** Implementation costs in total are too high, especially for SMEs, and reduce competitiveness of EU companies worldwide.	Drastic reduction of documentation requirements. Standard setters should be required to include relief measures for SMEs and even somewhat larger companies directly in the technical standards, and to prescribe a certain minimum scope in this regard.
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

8 Between DSA and ...

Legal Act	Problem	Possible Solution
GDPR	DSA prohibits dark patterns, including in cookie banners, but its interplay with GDPR consent requirements creates interpretation challenges rather than outright contradiction. DSA Article 25(1) bans dark patterns—designs that "numb, diminish, restrict, discourage, or deceive users" into decisions they wouldn't otherwise make, explicitly applying to cookie banners via manipulative opt-ins. Key Provisions: DSA Art. 25(1): Prohibits dark patterns impairing autonomous decisions; examples include prominent "Accept All" buttons, hidden "Reject All," pre-checked boxes, or false urgency in cookie banners. Non-prejudice clause DSA Art. 2(4)(g): DSA does not affect GDPR application to personal data processing (including consent for cookies) GDPR linkage: Cookie consent falls under GDPR Art. 6(1)(a)/Art. 7 (freely given, informed consent) + ePrivacy Directive Art. 5(3); dark patterns invalidate consent (EDPB Guidelines 05/2020) (Art. 7 GDPR). Both DSA and GDPR target manipulative cookie banners, but DSA's broader design prohibition overlaps with GDPR's consent validity rules without clear precedence—leading to uncertainty on whether DSA's general ban supplements or potentially conflicts with GDPR's specific consent mechanisms; the Art. 2(4)(g) non-prejudice clause preserves GDPR primacy but doesn't resolve design ambiguities	Open
UCP Directive	**Scope uncertainty of dark pattern exemption:** According to Art. 25(2) DSA, the prohibition of "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

Legal Act	Problem	Possible Solution
AVMSD	**Overlapping youth protection obligations:** In the realm of youth protection, the horizontal obligations set out in the DSA overlap with sector specific requirements of the AVMSD. The AVMSD requires to put in place appropriate protection measures from harmful audiovisual content (Article 28b AVMSD), while the DSA establishes a comprehensive, risk-based framework for addressing illegal content, systemic risks and the protection of minors (notably Articles 14, 16, 28, 34 and 35 DSA).	Open
EMFA	**Overlap in moderation of sensitive media content:** EMFA overlaps with the DSA in moderation decisions affecting lawful but sensitive media content. While the DSA serves as the primary regime for determining content lawfulness and platform obligations (Arts. 14, 16, 17, 34 and 35 DSA), the EMFA operates as a lex specialis, ensuring that DSA-based enforcement does not undermine media freedom, editorial independence, or pluralism (Art. 17 EMFA).	Open

9 Between DGA and ...

Legal Act	Problem	Possible Solution
Data Act	**Complex overlap of data intermediation, altruism, and data space duties:** 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	**Parallel obligations for data exchange and format descriptions:** 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	**Data transfer obligations under the DGA and 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	With regard to technical and organizational measures under Art. 12(j) DGA, refer to those under Art. 32 DA.

Legal Act	Problem	Possible Solution
	transfers of or access to non-personal data under Art. 32 DA also apply. The relationship between these obligations is neither explained nor structured.	
GDPR	**Distinction between personal and non-personal data under the GDPR and DGA:** 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 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.	Establish clear and legally binding requirements for pseudonymization and anonymization.

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 key driver of digital change in Europe and the world.

Publisher
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact
Jana Gaulke | Head of Brussels Office
T +32 471 92 97 43 | j.gaulke@bitkom.org

Responsible Bitkom-Committee
Public Affairs Committee