From Patchwork to Blueprint: Toward a Coherent EU Tech Framework

Version 2.0 – October 2025

bitkom

From Patchwork to Blueprint: Toward a Coherent EU Tech Framework

Version 2.0 – October 2025

The paper highlights key challenges arising from the diverse digital legal acts at the European level. The GDPR, Data Act, AI Act, DSA, and DMA each address distinct aspects of digital regulation, however, their overlaps, duplicative provisions, and inconsistent definitions give rise to legal uncertainty and increased administrative burdens.

The overview presented in this paper examines concrete conflict areas, potential points of tension, and presents initial proposals aimed at minimizing contradictions in existing and planned regulations. In some cases, it also identifies problems within individual legal acts. The paper is intended to be continuously updated.

Content

From Patchwork to Blueprint: Toward a Coherent EU Tech Framework 1

General Information 3

Between GDPR and 4

Between AI Act and 11

Between Data Act and 14

Between NIS-2 Directive and 17

Between CRA and 18

Between DMA and 19

Between DSA and 20

Between DGA and 21

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	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
	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 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.	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,

Legal Act	Problem	Possible Solution
	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.	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.
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:**	Clarifications are conceivable in both the AI Regulation and the GDPR.

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

Legal Act	Problem	Possible Solution
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.
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.	

Legal Act	Problem	Possible Solution
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	Open

Legal Act	Problem	Possible Solution
	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. 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:**	Open

Legal Act	Problem	Possible Solution
	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.	
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
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.

Legal Act	Problem	Possible Solution
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.
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	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
	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 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.

Legal Act	Problem	Possible Solution
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 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
Isabelle Stroot | Policy Officer Data Protection
T +49 30 27576-228 | i.stroot@bitkom.org

Responsible Bitkom-Committee
Data Protection Committee

Copyright
Bitkom 2025
This publication constitutes general, non-binding information. The contents reflect Bitkom's position at the time of publication. Although the information has been compiled with the greatest possible care, there is no claim to factual accuracy, completeness and/or timeliness; in particular, this publication cannot take into account the specific circumstances of individual cases. Use of this publication is therefore at the reader's own responsibility. Any liability is excluded. All rights, including partial reproduction, are reserved by Bitkom or the respective rights holders.

bitkom.org