BDI

INNONATION

POSITION | DIGITAL POLICY | EU SIMPLIFICATION

Simplifying the EU's Digital Rulebook

Proposals for the EU Commission's Digital Simplification Package.

15 July 2025

Executive Summary

Europe's competitiveness is under severe pressure, as the Draghi and Letta reports stressed recently. The EU has fallen behind the USA and China in terms of growth, productivity and innovative strength. Europe is at risk of being left behind in key technologies, such as artificial intelligence. The dictum "the US innovates, the EU regulates" becomes increasingly true: The EU has adopted a comprehensive regulatory framework in the digital sector – including the Artificial Intelligence Act (AI Act), the Data Act, the Chips Act, the NIS2 Directive, the Cyber Resilience Act (CRA), the Digital Services Act (DSA), the Gigabit Infrastructure Act (GIA), the Data Governance Act (DGA) and the Digital Markets Act (DMA). This regulatory framework has negative implications for companies' internal processes and the development of digital business models. Due to this sheer volume of digital regulatory acts, companies are confronted with an unprecedented amount of additional work that binds monetary and human resources that could otherwise be used to strengthen research, development and innovation to stay internationally competitive. Furthermore, they have to adapt their internal processes and hire specialised staff, which presents companies with additional challenges in the context of the acute shortage of skilled workers. Therefore, German industry highly appreciates the European Commission's announcement of an ample simplification package for digital regulation.

Policy recommendations at a glance

German industry urges the European Commission to include the following aspects in the digital package in order to reduce the regulatory burden, cut red-tape and reporting obligations, and thereby, to boost Europe's competitiveness by reaping the full potential of the digital transformation. To this end, we propose the following three overarching measures:

- **Reduce reporting obligations:** In several digital acts, the European co-legislators have included extensive reporting obligations. To reduce the overall regulatory burden and to free resources for research and innovation as well as the adoption of new business models, the reporting obligations must be streamlined and simplified.
- **Withdraw legislative act:** Since the CRA provides for harmonised and mandatory cybersecurity requirements for all products with digital elements the CSA's schemes are obsolete for such products, henceforth, the scheme-related Articles should be withdrawn.
- **Align timelines and ensure availability of standards:** The European co-legislators have implemented a vast set of regulatory acts. While these acts are highly interdependent, their

Steven Heckler | Digitalisation and Innovation | T: +49 30 2028-1523 | s.heckler@bdi.eu | www.bdi.eu

timelines and the availability of harmonised standards do not align. To reduce the burden for manufacturers and operators alike, the EU Commission should harmonise the implementation timeframes and postpone or ease the implementation until 36 months after standards are available. This could, for example, take the form of a 'stop-the-clock' mechanism.

In terms of regulation-specific measures, German industry urges the European Commission to consider the following simplifications in its Digital Package:

- **AI:** The AI Act should be simplified by shifting to sector specific regulation of Industrial AI by excluding Annex I. The Implementation Deadlines for Annex I and Annex III should be extended by at least 24 months. Transition periods should be linked to the availability of harmonised European standards. The GPAI Code of Practice needs to become more user oriented by revising the thresholds for systemic risk and avoid an inappropriate shifting of responsibilities from model providers to finetuners and users of these models. The AI Act should specify under which conditions finetuned models may be exempt from certain requirements, using clear definitions and thresholds. The AI Act should ensure that its transparency and data protection requirements are consistent with the General Data Protection Regulation (GDPR).
- **Cybersecurity:** The co-legislators should streamline reporting requirements for cybersecurity incidents and vulnerabilities to harmonise formats and contents and reduce the number of reports to avoid unnecessary administrative costs and overlaps. Documentation obligations should be simplified. The Commission should define realistic, technically sound timelines for the development and delivery of harmonised standards under the CRA. The CRA's mandatory conformity assessments must be delayed by 36 months for product categories whose vertical standards are not ready and harmonized in time. Tight implementation timelines risk negatively impacting existing supply chains. The Commission should focus its CRA implementation efforts on high-criticality products; ensuring that documentation requirements for low-criticality products are proportionate. Simplification measures should apply to all low-criticality products. The CRA's free-of-charge support period must be limited for B2B products.
- **Data protection:** To facilitate the data protection requirements, the Commission must help by publishing guidance on the detailed interplay between GDPR and the Data Act and how to protect the personal data of data subjects when such data is shared under the Data Act.
- **Data economy:** German industry urges policymakers at European and national level to adopt far-reaching changes to the Data Act to ensure that companies can implement the Data Act without unduly high costs. It is paramount to reduce regulatory uncertainty by clarifying definitions, clarifying the extent of information obligations, protecting trade secrets, limiting the exceptional need to use data to B2G, deleting Article 13 (4) and (5), and postponing the implementation of the Data Act by two years.
- **Digital infrastructure:** An ambitious reform of the current regulatory framework is essential with the upcoming Digital Networks Act (DNA) — including a shift towards horizontal consumer protection law, extended spectrum licences, and an overall more coherent and simpler regulatory framework. Moreover, to facilitate the rollout of gigabit networks, the Commission should cut unnecessary red tape and overly bureaucratic requirements. In the context of the GIA, this means reducing information obligations and speeding up authorisation procedures.
- **Semiconductors:** The Commission should implement significantly faster and more flexible funding procedures for microelectronics projects, aligned with the sector's rapid innovation cycles. It should reduce planning and technical detail requirements and focus on overarching European objectives. This would better support SMEs and ensure that funding remains relevant to evolving technological needs.

Table of contents

Simplifying the EU's digital rules 5

Artificial Intelligence 5

AI Act: Annex I + Recital 49 6

AI Act: Article 51 + 53 General Purpose AI 8

AI Act: Article 11 + Annex IV 8

AI Liability Directive: Stop Ongoing Legislation 8

Cybersecurity 9

CRA, NIS 2, GDPR and sectoral cybersecurity regulations: Common reporting mechanism for incidents and demonstration of conformity with regulatory requirements 9

Cyber Security Act: Withdraw the Act 10

Cyber Resilience Act: Transition Period 11

Cyber Resilience Act: Introduction and Exclusion of 'Benign Digital Products with digital elements' (Article 2 and 3) 12

Cyber Resilience Act: Reporting obligations (Article 14) 12

Cyber Resilience Act: Everlasting Monitoring and Reporting obligations (Article 14, Article 69.3) 13

Cyber Resilience Act and harmonised European standards: Regulatory complexity 13

Cyber Resilience Act: Recognize existing industry standards for conformity assessment 14

NIS 2 Directive: EU-wide harmonisation of implementation 15

NIS 2 Directive: Reporting obligations (Article 23) 15

NIS 2 Directive: Critical components (Article 24 paragraph 2) 16

RED Delegated Regulation: Implementation timeline 16

NIS 2 Directive: Simplify requirements for affiliated companies (Article 22 (5)) 16

Data protection 17

GDPR: Legal clarity on data anonymisation 17

GDPR: Risk-based approach 17

GDPR: Interplay between GDPR and Data Act 18

Data economy 19

Data Act: Reduce regulatory uncertainty and ensure practical implementation 19

Data Act: Protection of trade secrets 19

Data Act: Clarify definitions 20

Data Act: Limiting the scope of application for virtual assistants on B2C 20

Data Act: Right of the data holder to use data 20

Data Act: Clarify the extent of Information obligations 20
Data Act: Limiting the exceptional need to use data for B2G 21
Data Act: Profiling 21
Data Act: Deletion of Art. 13 (4) and (5) 21
Data Act: Transition Period and Reassessment 21

Digital Infrastructure 22
European Electronic Communications Code: Reducing the administrative burden 22
European Electronic Communications Code: Spectrum cost and duration 23
European Electronic Communications Code: Spectrum awarding / authorisation 24
Gigabit Infrastructure Act (GIA): Accelerating authorisation procedures 25
Funding & IPCEI: A simplified and coordinated support framework 26

Semiconductors 27
IPCEI and European Chips Act: Funding 27

Digital Services / Platform Economy 27

Imprint 28

Simplifying the EU's digital rules

To promote the digital transformation of Europe, the EU must work towards a harmonised, low-bureaucracy and technology-promoting implementation of the digital regulations that have been recently adopted. When developing European implementing acts, it should enter into a structured dialogue with industry to ensure that the regulatory requirements are designed in a practical manner.

Artificial Intelligence

The European economy needs a robust AI ecosystem. In economically and geopolitically difficult times in particular, sovereign AI innovations contribute to the transformation of industry towards resilience and future readiness. Many companies point to regulatory uncertainties as an investment hurdle. In view of the reduction of regulatory hurdles in the USA, a more business-friendly AI legal framework must also be created in the EU with regard to a level playing field. Overregulation through the AI Act can lead companies to allocate significant resources to comply with bureaucratic requirements, rather than focusing on the development and implementation of AI technologies. This can impair the competitiveness of European industry and jeopardize Europe's economic position. By simplifying the regulations, companies could better leverage their innovative capabilities and strengthen their position in the global market. This simplification however cannot be reached by reducing the rights of natural persons or any other rights that could be infringed by using AI but must be achieved by reducing irrelevant regulating parts that do not touch the transparency of AI systems.

Industrial AI must be viewed as an opportunity, not a risk. Hence, products that are already subject to European product regulation (Annex I) should be excluded from the scope of the AI Act (e.g. Medical Devices Regulation, Machinery Regulation. If there is a need for regulation, this should be included in the respective sector regulations.

The AI Act dates for the applicability of the provisions related to GPAI models and related CoPs need to be extended by 24 months (to 08/2027). The dates for the applicability of the provisions related to High-Risk AI Systems in Annex III and for High-Risk AI Systems in scope of existing Union legislation. Furthermore, the category of High-Risk AI needs to be clarified, e.g. it needs to be set out, that AI systems that do not impose a safety risk for users, like AI cybersecurity components for cybersecurity purposes, do not qualify as high-risk under Annex 1 or Annex 3.

AI Act: Implementation Deadlines for Annex I and Annex III

Status quo: The implementation of the AI Act is phased, with various provisions becoming applicable between February 2, 2025, and August 2, 2027.High-risk AI systems under Annex I must comply within 36 months from the entry into force of the AI Act, i.e., by August 1, 2027. High-risk AI systems under Annex III must comply within 24 months from the entry into force of the AI Act, i.e., by August 1, 2026. The standardization of the high-risk requirements is progressing much more slowly than originally planned. However, the availability of high-quality standards is essential for a practical and innovation-friendly implementation of the AI Act. If the current deadlines for the high-risk requirements are adhered to, many companies will postpone investments in high-risk AI systems, as the legal uncertainty is too great without standards being finalized in time. In addition, we see slow progress in establishing competent authorities at national level, in clarifying various points in the AI Act that require interpretation (high-risk definition, AI literacy, transparency requirements, materiality threshold for changes to AI systems, etc.) and in clarifying the interaction with other horizontal and sectoral legislation.

Proposed simplification: We propose an extension of the implementation deadlines for the high-risk requirements of the AI Act by 24 months each for Annex I and Annex III.

AI Act: Annex I + Recital 49

Status quo: 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 risk compounding delays and market disruption. This regulatory burden will weigh heaviest on manufacturers in sectors where Europe holds longstanding competitive advantage such as automotive, machinery or medical equipment.

Crucially, the products listed in Annex I present some of the lowest fundamental rights risks amongst systems covered by the AI Act. Yet they face some of the most extensive compliance obligations. This mismatch cuts against the risk-based foundation on which the AI Act is built.

Apart from the issues outlined above regarding the sectoral regulations in Annex I, Section A, many sectors, i.e. 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.

Proposed simplification: AI requirements should be progressively incorporated into sectoral framework, rather than applying immediately and in parallel with sectoral legislation, provided that the sectoral rules do not go beyond the current requirements of the AI Act. 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.[1]

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[2], and would strengthen the replicability of AI harmonised standards, maintaining a unified definition of 'state of the art' across sectors.

AI Act: Privilege intra-group scenarios

Status quo: Except for a narrow scope described e.g. in Recital 97, the AI Act also applies in intra-group scenarios. This means that when companies within the same corporate group provide and deploy services internally, they must comply with the same requirements as if they were providing AI services to external parties. Requiring compliance with the AI Act for intra-group services imposes unnecessary administrative and financial burdens on companies. This can divert resources from more mission-critical activities and stifle innovation within the company.

Proposed simplification: To alleviate these issues, a corporate privilege should be introduced, whereby the AI Act does not apply to intra-group scenarios, except for situation were a protection of employees is a valid goal of the regulation (e.g. prohibited practices and especially Annex III, Nr. 4 recruitment and performance evaluation). The rationale behind this exemption is that the protective measures mandated by the AI Act are mostly designed to address risks associated with public and consumer-facing services, which are not typically present in internal corporate environments.

AI Act: Legislative Interplay with horizontal legislation

Status quo: The overlapping requirements and potential conflicts between the AI Act, the Data Act, and the General Data Protection Regulation (GDPR) can create legal uncertainty and increase the compliance burden for companies. For example, the GDPR sets out comprehensive data protection obligations which apply to AI as well.

Proposed simplification: The AI Act should ensure that its transparency and data protection requirements are consistent with the General Data Protection Regulation (GDPR). This would provide clear guidelines for companies on how to handle personal data in AI systems without conflicting with GDPR obligations. We also call for regulatory clarification in the interpretation of cases involving the AI Act by the data protection supervisory authorities, for example in the use of AI in personnel management. Regarding the Data Act, the AI Act should align its provisions on data sharing and access with the Data

[1] This approach is better aligned with Recital 49 AI Act, which calls for sector-specific adaptations 'without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established' under EU product legislation.
[2] Attempts to alter the AI Act's classification logic have already emerged, notably in discussions around the Radio Equipment Directive (Directive 2014/53/EU) and the proposed Toy Safety Regulation (COM(2023) 462 final), such as wrongly classifying AI-based cybersecurity components as safety components and considering that third-party conformity assessments are mandatory even when internal assessments are allowed. It should be clarified that AI systems not constituting a safety component or part thereof in the strict sense fall outside the AI Act's scope. This is essential to prevent sectoral authorities from expanding high-risk obligations to AI systems not intended to be covered, based solely on hypothetical impacts on product performance.

Act to ensure a coherent framework for data-driven innovation. This would facilitate the use and exchange of data in AI systems while maintaining legal certainty for companies.

AI Act: Article 51 + 53 General Purpose AI

Status quo: The AI Act introduces arbitrary thresholds for systemic risk in General Purpose AI (GPAI) models, which are defined in Article 51(2). These thresholds are based on the computational power used to create GPAI, the number of users or the scale of deployment, without clear criteria for assessing the actual risk posed by the AI system, that has not been addressed by other regulations or safeguards. This can result in unnecessary regulatory burdens for AI providers as well as AI deployers as the definitions of roles along the value chain remain unclear. Many European companies will be in the position to finetune GPAI models, but currently there is no clarity as to the distribution of responsibilities.

Proposed simplification: German industry proposes revising the thresholds for systemic risk in GPAI models to be more flexible and based on actual risk not addressed in other regulation rather than arbitrary numbers.

Proposed simplification: The proposed clarification in the latest "GPAI Guidelines" draft is largely welcomed, with the goal to avoid an inappropriate shifting of responsibilities from model providers to finetuners and users of these models. The AI Act should clearly exclude finetuned models by providing clear definitions and appropriate thresholds.

AI Act: Article 11 + Annex IV

Status quo: The requirements for the documentation of high-risk use cases from Article 11 and its detailing in Annex 4 are too extensive (texts, system documentation, hardware requirements, possibly images of hardware components, design specification).

Proposed simplification: Simplification of documentation requirements for high-risk AI systems and provision of templates based on examples as a mandated template if no personal data is involved.

AI Liability Directive: Stop Ongoing Legislation

Status quo: The ongoing legislation on the Additional AI Liability Directive (AILD) could lead to significant overlaps with existing liability regimes, at least with the liability rules already in place in the Product Liability Directive (PLD), General Product Safety Regulation (GPSR), Automatic Exchange of Information framework (AEOI), GDPR, etc. This would result in a huge additional burden for companies and users of AI systems without any real benefits for the economy, EU citizens, and the EU (AI) ecosystem.

Proposed simplification: The current legislation on AILD should be immediately stopped and, if necessary, residual AI liability risks that are still inadequately covered (if proven to exist) should be handled by the AI Act or GPSR, PLD, GDPR.

Cybersecurity

Since 2016, the European Union has introduced a far-reaching cybersecurity regulatory framework covering both companies as well as products. The Network and Information Security Directive (NIS 1 (Directive 2016/1148)) significantly contributed to a first harmonisation of EU-wide applicable cybersecurity requirements for operators of critical infrastructures. Its recent update, i.e. the NIS 2 Directive (2022/2555), now requires a plethora of companies to implement cyber-risk management requirements and to report cybersecurity incidents. These organisation-focused directives have been complemented by the Cybersecurity Act (CSA, Regulation 2019/881) and the Cyber Resilience Act (CRA, Regulation 2024/2847), which cover the cyber resilience of products. These overarching cybersecurity requirements have been supplemented by several sector-specific regulatory requirements, such as Implementing Regulations (EU) 2019/1583, (EU) 2023/203 and (EU) 2022/1645. In light of the ever-increasing cyber-risk environment, German industry supports this holistic approach to enhancing Europe's cyber-resilience. However, the rise in regulatory requirements is making it increasingly difficult for companies to focus their resources on implementing cyber-risk mitigating measures to enhance their prevention. Varying interpretations of EU directives (esp. NIS 2) by Member States (MS) further fragment the security landscape. Today, due to the existing legal framework, entities have to invest scarce cybersecurity resources to comply with excessive reporting obligations and other bureaucratic duties. The lack of clear guidance on timelines and the absence of harmonised standards further complicates the implementation process, leaving providers to navigate a maze of inconsistent procedures and thresholds.

Therefore, German industry urges the European Commission, the European Parliament and EU Member States to significantly streamline Europe's cybersecurity regulatory framework. Harmonising and simplifying cybersecurity legislation will not only reduce administrative burdens but also significantly enhance the efficiency of security incident management, ensuring consistent, effective, and easier-to-implement cybersecurity measures across the EU.

CRA, NIS 2, GDPR and sectoral cybersecurity regulations: Common reporting mechanism for incidents and demonstration of conformity with regulatory requirements

Status quo: The current cybersecurity regulatory framework requires companies to report significant security incidents affecting an essential or important entity (cf. Article 23 NIS 2 Directive), and actively exploited vulnerabilities in products with digital elements (cf. Article 14 CRA). While the former must be reported to the national competent authority or Computer Security Incident Response Team (CSIRT) in each Member State, the latter must be reported to both the relevant national CSIRT and to ENISA via ENISA's reporting mechanism. Telecommunication operators, for example, must navigate and report incidents under twelve different pieces of EU legislation, including NIS2, Digital Operational Resilience Act (DORA), CRA, and GDPR, each with varying requirements, thresholds, and reporting timelines. If the same cybersecurity incident might also affect data protection and privacy or affects financial IT systems, additional reporting obligations may arise under GDPR and DORA. For sectoral cybersecurity regulations additional reporting mechanisms are foreseen like ECCAIRS2 for Part-IS and national portals for EU 2019/1583. Moreover, companies are obliged to demonstrate the implementation of regulatory requirements, such as the risk management measures, in each country separately.

Proposed simplification: German industry urges the European Commission, the European Parliament and all EU Member States to standardise definitions, reportable items, timelines, thresholds, reporting authorities, and tools (such as platforms and templates), and to operate a common reporting mechanism ("1-stop-shop") which enables companies to fulfil all their reporting obligations emanating from the CRA, the NIS 2 Directive, GDPR, DORA and sectoral regulations, such as EU 2019/1583 and

Part-IS. Such a reporting platform should be operated by ENISA. All national competent authorities as well as CSIRTs should be enabled to retrieve relevant information from this platform. Establishing such a single reporting mechanism would significantly reduce the bureaucratic costs associated with reporting incidents – particularly under NIS 2, where companies currently have to report the same incidents in all affected EU Member States in the respective official languages. By enabling companies to report incidents once for all EU Member States, companies would be able to focus their personnel on incident handling and mitigation rather than reporting. This would have both positive effects for the competitiveness of companies in Europe, and would constitute a more efficient use of taxpayers' money. To avoid double sanctions for incidents impacting multiple regulatory areas or entities across different Member States, ensure that a single report through the most relevant jurisdiction suffices for cross-border incidents. Until such an EU-wide one-stop-shop is developed, each Member State should provide a national one-stop-shop as a first step to reduce the bureaucratic burden emanating from reporting.

For demonstrating compliance with cybersecurity risk-management measures, German industry urges the European Commission and Member States to establish a common mechanism via which companies can demonstrate the responsible national authorities across the EU that they fulfil the European requirements against one or more clearly identified international cyber security standard (like the ISO270xx family). This would significantly reduce the implementation costs for companies. Notwithstanding the above stated arguments, companies should still have the possibility to directly report classified information to their national competent authority if deemed necessary.

Cyber Security Act: Withdraw the Act

Status quo: In 2019, the European Cyber Security Act (EU CSA) was enacted with a view to strengthen the EU Agency for cybersecurity (ENISA) and introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. To this end, ENISA together with a working group develops cybersecurity certification schemes specific for certain ICT products, services and processes, such as cloud or 5G. Considering the experience so far, the EU CSA has not been able to deliver on its original intention. While the EU Common Criteria Scheme (EUCC) has been finalised, the EU Member States still could not agree on the criteria to be integrated into the EU Cloud Scheme (EUCS). Since the enactment of the CRA, and thereby mandatory cybersecurity requirements for all products with digital elements that are placed on the European market, the EU CSA's cybersecurity certification schemes have become obsolete.

Proposed simplification: Considering the experience with the implementation of the EU CSA in terms of the drafting of product-group-specific cybersecurity certification schemes, German industry urges the European Commission to withdraw the EU CSA completely. We perceive the Cyber Resilience Act as better suited to enhance the cyber resilience of products throughout the EU since (1) the CRA introduces cybersecurity requirements that are binding for all products with digital elements placed on the European market, and since it (2) entails a more transparent and inclusive process in terms of stakeholder involvement for developing product-related requirements than the EU CSA. By withdrawing the EU CSA, the European Commission would comply with the "one-in, one-out rule". Moreover, withdrawing the CSA would streamline the EU's regulatory cybersecurity framework and the cybersecurity certification framework, thereby, it would significantly simplify the regulatory landscape for companies. It would also end the duplication of cybersecurity regulation for products that exists since the adoption of the CRA. All aspects regarding the establishment of ENISA should be addressed in a new ENISA Act.

Cyber Resilience Act: Transition Period

Status quo: Many necessary vertical standards for the timely implementation of the CRA are significantly in delay and far from finalised. Respective vertical standards are currently expected to be available no sooner than in the third quarter of 2026. At the same time, the CRA introduces mandatory conformity assessments for "important products" to be placed on the market according to these standards after December,11 2027.

Proposed simplification: To ensure the effective and practical implementation of the CRA, it is essential that the European Commission – in close cooperation with the European Standardisation Organisations (ESOs) as well as technical experts from industry and civil society – defines and agrees on realistic, technically sound timelines for the development and delivery of harmonised standards under the CRA.

This applies in particular to the vertical, product-specific standards that enable the presumption of conformity with the essential requirements of the CRA. These standards are not merely implementation tools. Rather, they are an integral legal basis for demonstrating compliance, especially for products with digital elements classified as "important" under Annex III (Class I), where third-party conformity assessment would otherwise be mandatory.

Therefore, it must be ensured that a minimum of 36 months elapses between the formal publication of the relevant harmonised standards in the Official Journal of the European Union and the end of the transitional implementation period of the CRA. Only this timeframe provides manufacturers with the necessary legal certainty and operational feasibility to meaningfully integrate the CRA requirements into product development and production processes.

Tight implementation timelines risk negatively impacting existing supply chains. Most products with digital elements currently in use were developed before the adoption of the CRA - in parts as general-purpose components without alignment to specific, risk-based cybersecurity requirements. To achieve conformity with the CRA and to be placed on the market beyond December 11th, 2027, parts of these product portfolios would require significant redesign. For certain product types already on the market, timely adaptation may not be technically or economically feasible. This could result in the withdrawal of established products, with far-reaching implications for supply chain continuity and the availability of products with digital elements within the EU. Particularly withdrawals in the semiconductor sector could lead to severe implications as they serve as a foundational technology across a broad spectrum of applications. The link of transition periods to the availability of harmonized European standards and the introduction of the concept of "benign products" (see below) would mitigate this risk.

If such an extension cannot be granted, manufacturers of all "important" products with digital elements (Annex III CRA) should temporarily be permitted to use Module A (internal production control) as a conformity assessment procedure, until the vertical harmonised standards are available. This pragmatic interim solution would safeguard legal certainty and market continuity without compromising cybersecurity objectives.

The CRA's reliance on the availability of harmonised standards as a precondition for using Module A has far-reaching consequences. In their absence, manufacturers are forced to involve a notified body, even where the product's risk profile is low. This dependency has already led to severe delays under other EU legal acts – such as the Radio Equipment Directive – and is expected again under the CRA. It imposes unpredictable and disproportionate burdens on both manufacturers and notified bodies, particularly during transitional phases.

Cyber Resilience Act: Introduction and Exclusion of 'Benign Digital Products with digital elements' (Article 2 and 3)

Status quo: The scope of the CRA will include also trivial products with digital elements like Analog-to-digital converter or products whose only 'digital interface' is an USB battery charging interface (e.g., electric toothbrushes). Even though the CRA will not require any additional cybersecurity protection measures due to the virtually non-existent cybersecurity risks, these products with digital elements will still have to go through the NLF formal conformity assessment to demonstrate CRA compliance with all processes, documents, and labelling requirements. Consequently, without any lower limits for such "benign products," costs are generated that have no discernible benefit for the manufacturer, the customer, or society.

Proposed simplification: To address this imbalance, we propose introducing a specific exemption for "inherently benign products" under the CRA. This category would apply to products that, due to their technical simplicity, cannot pose a cybersecurity risk. Examples include simple sensors, passive electronic components, or basic switching devices. A precedent for such an approach exists in Recital 12 of the EMC Directive (2014/30/EU), which refers to products "inherently benign in terms of electromagnetic compatibility." A similar reference – "inherently benign in terms of cybersecurity" – would be appropriate and beneficial in the context of the CRA.

To ensure legal certainty and prevent circumvention of the regulation, we propose the following definition:

Article 3(4a): *"benign product" means a product which cannot cause a cybersecurity risk because it is technically too limited to do so."*

Further clarification on the scope and application of this category could be provided through implementing guidelines or delegated acts, ensuring consistent interpretation and enforcement. Introducing this exemption would strengthen regulatory proportionality while safeguarding cybersecurity objectives.

Cyber Resilience Act: Reporting obligations (Article 14)

Status quo: According to Article 14, Manufacturers have to notify by using the designated single reporting platform any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. Manufacturers are required to (1) issue an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, (2) a more detailed vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, and (3) a final report, no later than 14 days after a corrective or mitigating measure is available. In addition, a manufacturer must notify any severe incident having an impact on the security of the product with digital elements (cf. Article 14 (3 and 4)).

Moreover, there are overlaps in terms of reporting obligations of incidents as well as vulnerabilities between CRA, GDPR and NIS 2.

Proposed simplification: German industry urges the European Commission to reduce the number of simultaneous reports to only one – ideally to the ENISA platform. Additionally, a manufacturer of a product with digital elements has to submit to two – one initial within 48 hours and a detailed no later than 14 days after a corrective or mitigating measure is available. This would significantly reduce the bureaucratic burden resulting from the Cyber Resilience Act without compromising the cyber-resilience

across the EU. The Commission must clarify the primacy of the legal bases when companies have to report incidents or vulnerabilities under more than one of the existing European digital regulatory acts (NIS 2, CRA, GDPR).

Cyber Resilience Act: Everlasting Monitoring and Reporting obligations (Article 14, Article 69.3)

Status quo: Unlike the vulnerability management obligations, which expire at the end of the last support period at the latest, the obligations to monitor products and report actively exploited vulnerabilities and severe incidents will be mandatory forever. Furthermore, these monitoring and reporting obligations also apply to existing products launched before the CRA became applicable (cf. Art. 69.3). This represents a disproportionate burden, especially for long-standing market participants with many new and especially many legacy products.

Proposed simplification: To reduce the bureaucratic implications emanating from the CRA, monitoring and reporting period should be finite and end, for example, five or ten years after the end of the support period.

Cyber Resilience Act and harmonised European standards: Regulatory complexity

Status quo: The CSA and CRA in conjunction with several harmonized European standards (hENs) create a very complex regulatory framework for products placed on the European market. Besides the horizontal regulation there are vertical, i.e. industry-related regulations like Radio Equipment Directive (EU) 2014/53, (EU) 2018/1139 and (EU) 2019/2144 which cover cybersecurity and corresponding certification of those systems and components. This increasingly complex situation makes it hard for the relevant industry to ensure compliance by understanding the different scope statements, interrelationships and interdependencies between the horizontal, vertical regulations and hENs in the right way.

Proposed simplification: German industry strongly recommends limiting the complexity of cybersecurity-related regulation and certification approaches to the minimum. Systems and components provided by suppliers who can prove that they have implemented and follow the vertical, industry-related regulation and certification and thus fulfil the technical specifications and cybersecurity measures and processes for their systems and components in accordance with the relevant standards are not subject to horizontal regulations. Otherwise, systems, components and separate technical units designed and constructed would be subject to the requirements of the horizontal Regulation.

Given the mandatory applicability of the horizontal cybersecurity requirements for products with digital elements (CRA) by 11 December 2027 set out in EU Regulation 2024/2847, we urge the European Commission to repeal the Delegated Regulation (EU) 2022/30, focusing on the avoidance of double regulation for manufacturers.

There is a notable lack of pragmatism in the harmonisation of standards to accept existing ones, even if only with restrictions. These restrictions could be formulated in corresponding EU Commission Decisions and then considered in the update of the corresponding standards. Accepted procedures (processes, standards, and conformity), as seen with medical devices, could be reused for "non-medical devices" – so-called health applications used in hospitals – which now fall under the EU CRA without requiring a clinical evaluation. This reuse would significantly reduce the burden on specific sectors. Similarities might also be found in other sector-specific regulations.

Cyber Resilience Act: Support Period

Status quo: During the support period of their products with digital elements, manufacturers are obliged to ensure that, where security updates are available, they are disseminated free of charge. Article 13 (8) CRA prescribes to include other relevant Union law when determining the support period of products with digital elements. This can pose significant challenges to manufacturers. Regulations like the Machinery Regulation or the Ecodesign for Sustainable Products Regulation require manufacturers to define the lifetime of products. Many industrial products have physical lifetimes exceeding ten years, while their digital components follow much shorter innovation and support cycles. Requiring cybersecurity support for the entire physical lifetime imposes disproportionate burdens on manufacturers.

Proposed simplification: We propose a clear regulatory distinction between the physical and digital lifetimes of products with digital elements under the Cyber Resilience Act (CRA). The European Commission should introduce a "digital lifetime" concept, defined and transparently declared by the manufacturer, to allow for risk-based and economically viable support obligations. This would enhance legal certainty, promote sustainable product use, and maintain the competitiveness of Europe's high-tech industry – without compromising the CRA's cybersecurity objectives

Cyber Resilience Act: Documentation Obligations

Status quo: Annex VII of the Cyber Resilience Act specifies detailed documentation obligations for manufacturers, forming a crucial component of the technical documentation required for demonstrating conformity. This annex has far-reaching implications, especially for manufacturers of non-important or non-critical products with digital elements, who will nonetheless face disproportionate obligations if no proportionality mechanisms are introduced. According to CRA Article 13 (7), manufacturers are obliged to "systematically document*, in a manner that is proportionate to the nature and the cybersecurity risks*, relevant cybersecurity aspects concerning the products with digital elements." At the same time, according to Article 33 (5) of the CRA "Microenterprises and small enterprises may provide all elements of the technical documentation specified in Annex VII by using a simplified format.".

Proposed simplification: The European Commission should focus its CRA implementation efforts on high-criticality products with digital elements, while ensuring that documentation requirements for low-criticality products remain proportionate. Although Article 13 (7) CRA already implies a risk-based approach, the Commission should emphasize proportionality and risk relevance more clearly through interpretative guidelines. Furthermore, the simplification measures for SMEs under Article 33 (5) could be extended to all low-criticality products – regardless of manufacturer size – particularly for non-"important," and non-"critical," products with digital elements. This approach would reduce unnecessary administrative and bureaucratic obligations.

Cyber Resilience Act: Recognize existing industry standards for conformity assessment

Status quo: Industry has established several worldwide recognized security standards, such as EMVCo and GSMA eSA. At the same time, the European Commission issues standardisation mandates within the framework of the CRA.

Proposed simplification: Established industry standards must be directly recognised for CRA conformity assessments without transferring them into European standards in order to reduce the bureaucratic burden and to speed up the implementation of the CRA.

NIS 2 Directive: EU-wide harmonisation of implementation

Status quo: Since the co-legislators agreed on the regulatory measure of a "Directive" when developing the NIS 2, the regulatory requirements are implemented differently across the EU's 27 Member States. For example, Member States are adopting varying approaches in terms of entity classification (ranging from single-tier to three-tier systems), sector coverage (with some states expanding scope), and size-cap thresholds. This regulatory fragmentation means organisations may face different compliance requirements across jurisdictions, even when providing identical services. Therefore, a company's NIS2 compliance in one country does not necessarily imply compliance in another.

Proposed simplification: The Directive based approach means companies must navigate varying national interpretations and implementation timelines across member states. Organisations must adapt to inconsistent scope interpretations, security frameworks, varying reporting thresholds and differences in supply chain provisions, creating operational complexity in cross-border security management and compliance monitoring. To reduce the implementation costs for companies and to ensure the risk-adequate level of cyber-resilience across the Union, each EU Member State should implement the NIS 2 Directive in a uniform manner without any additional regulatory requirements that companies have to fulfil. This should include central guidance for a pragmatic and harmonised interpretation of key definitions, like "establishment". Also, the principle of "main establishment" should be extended for other highly interconnected sectors, such as transport. To increase the harmonisation of entity-related cybersecurity requirements, the European Commission should opt for a regulation when revising the NIS 2-Directive.

NIS 2 Directive: Reporting obligations (Article 23)

Status quo: Article 23 of the NIS 2 Directive requires all essential and important entities to report every cybersecurity incident which has significant implications for their services. In case of a significant cyber security incident, companies must fulfil three to five reporting obligations. The first report must be submitted within 24 hours after becoming aware of the incident and the second must follow within 72 hours after becoming aware of the incident. Upon request of a CSIRT or, where appropriate, the competent authority, can request an interim report on relevant status updates. Moreover, companies have to submit a final report no later than one month after the submission of the notification of the incident. In case of an ongoing security incident at the time of submission of the final report, the organisation concerned must submit a progress report at that time and a final report within one month of the handling of the security incident.

Proposed simplification: Sharing information of current cyberattack vectors is crucial to enhance Europe's cyber resilience. However, incident reporting will only contribute to this goal if the information reported to the national component authority is analysed by the national competent authority and incorporated into a daily cybersecurity situation picture. The current requirement of handing in up to five reports per incident is overly bureaucratic. Moreover, the diverging scope of reportable incidents across countries, with some requiring reporting beyond significant incidents and others applying different cross-border impact criteria, forces companies to implement broader monitoring capabilities and maintain country-specific incident response procedures, leading to increased resource requirements and compliance risks.

Apart from harmonising the requirements of reportable incidents and respective definitions across the EU's 27 Member States, German industry urges the European co-legislators to reduce the number of reports per incident to a maximum of three:

- First Report: Companies should issue within 48 hours of becoming aware of the significant incident, an early warning to the national competent authority. In contrast to NIS Cooperation Group's current proposal, such an early warning should comprise only very basic information, such as the name of the company and the currently visible implications.

- Intermediary Report: Upon request of the national competent authority, companies should be required to submit one intermediary report including relevant status updates.

- Final Report: One month after the handling of the incident, companies should submit a final report including the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; and (iv) where applicable, the cross-border impact of the incident.

This simplification would massively reduce the bureaucratic costs associated with the implementation of the NIS 2 Directive without reducing Europe's cyber resilience. In addition, standardised reporting templates and data formats based on unambiguous definitions would facilitate the reporting process. Overall, this simplification would ensure that companies could focus their scarce cybersecurity resources on the incident handling as well as prevention and detection. Ultimately, this could even increase Europe's overall cyber resilience.

NIS 2 Directive: Critical components (Article 24 paragraph 2)

Status quo: In case of insufficient levels of cybersecurity, under NIS 2 Article 24 paragraph 2 the European Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement the NIS 2 Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. This could lead to overlaps with the horizontal requirements under the CRA.

Proposed simplification: The CE marking according to CRA should be recognised as a sufficient requirement for ICT products under NIS-2.

RED Delegated Regulation: Implementation timeline

Status quo: Delegated Regulation (EU) 2022/30 specifies which categories or classes of radio equipment are concerned by each of the additional essential safety requirements laid down in Article 3(3).

Proposed simplification: Given the mandatory applicability of the horizontal cybersecurity requirements for products with digital elements (CRA) by 11 December 2027 set out in EU Regulation 2024/2847, we urge the European Commission to repeal the Delegated Regulation (EU) 2022/30, focusing on the avoidance of double regulation for manufacturers. For the time being, the Commission should postpone the enforcement of the RED Delegated Regulation until 2026. This delay will provide businesses with sufficient time to implement the harmonised standard (published on January 28, 2025) and to address RED and CRA compliance in a holistic, effective, and cost-efficient manner. This will ensure that businesses are adequately prepared and can integrate compliance measures seamlessly.

NIS 2 Directive: Simplify requirements for affiliated companies (Article 22 (5))

Status quo: Currently, affiliated companies within a corporate group are treated like independent companies in the open market under NIS2.

Proposed simplification: If a company offers services that are regulated under NIS2 Article 22 (5) in conjunction with Implementing Directive 2024/2690 exclusively to affiliated companies within the corporate group, then the company and its services should be exempt from the requirements of NIS2 Article 22 (5) and Implementing Directive 2024/2690.

Data protection

Effective and practicable data protection is an important requirement for a functioning digitalisation. Unfortunately, the GDPR requirements still result in a great deal of bureaucracy that burdens companies. There is also an urgent need to balance the interaction between data protection and data usage under the new EU digital acts.

GDPR: Legal clarity on data anonymisation

Status quo: Legal certainty on the requirements to use anonymised data is important in order to both ensure a high level of data protection and the added value of data usage. The GDPR contains neither a legal definition of "anonymisation" nor a minimum standard that specifies when personal data is no longer identifiable. This is made even more difficult by the broad interpretation of the term 'personal data' by courts and data protection authorities (DPA) and a lack of practical guidelines by the DPAs.

Proposed simplification: There is a need for reliable legal standards and practical guidelines to enable the use of anonymised data in compliance with data protection regulations and to reduce administrative costs. The anonymisation of personal data should be assessed using a relative approach and based on the ability of data processors to actually access the data. A legally defined presumption rule – such as the US HIPAA regulations (Health Insurance Portability and Accountability Acts), for example – would be a feasible option.

GDPR: Risk-based approach

Status quo: The GDPR has a uniform data protection approach. The Regulation doesn't make a difference between data processing activities but rather sets the same prerequisites for any processing of personal data, irrelevant of the risk for the data subject affected. This approach is appropriate for companies which business models rely on the processing of large volumes of personal data. In such cases data privacy should be thought and practiced in a comprehensive way to ensure that natural persons and their personal data are protected. However, when it comes to situations where personal data is merely a byproduct and isn't processed any further, there should be exemptions from certain provisions of the GDPR, which impose a huge organisational burden on all kinds of enterprises, especially for SMEs.

Proposed simplification: A clearer focus on the risk-based approach and a clarification which is considered as personal data (and what not) would be welcomed. The GDPR should differentiate between processing activities based on the risk they pose to the rights of the data subjects. Where the processing of personal data means no to little risk for the data subject, there is no need for the same protection measures the processing of personal data that poses high risks to the rights of data subjects requires. For example, where the processing of personal data is a mere byproduct, e.g. when a staff number of a natural person is stored on a machine, which is operated by that person, and that number isn't processed any further, the risk could be considered little, if not non-existent. Another example is the processing of data in the context of technical, logistical or quality assurance processes where the only reason for the processing of that data is to identify the technical information behind it (e.g.

"technical identifiers"). However, due to the very broad definition of "personal data" technical identifiers are considered personal data and the technical related processes also need to be adapted in order to comply with the GDPR which entails a large number of compliance obligations for the enterprises. However, in these cases there is no need for the extensive information obligations or a record of processing activities to protect such personal data. A risk-based approach and legal certainty that f.i. technical identifiers are not considered persona data according to the GDPR would mean a more manageable and consequently more efficient implementation of data protection mechanisms, so that resources can be concentrated on processes with a genuine personal reference and therefore ultimately lead to wider acceptance of data privacy legislation overall. It would reduce the risk of data privacy being seen as a burden more often than as a prerequisite for secure data processing.

GDPR: Interplay between GDPR and Data Act

Status quo: There is no reliable information on the interplay between the GDPR and the Data Act. While the GDPR (e.g. Art. 5, 6 and 7) with its "Privacy-by-Design"-approach sets out strict requirements for the processing of personal data, the Data Act with its "Access-by-Design"-approach aims to facilitate access to and sharing of data – often from connected devices. The EU Commission states in its FAQ on the Data Act, that the GDPR is fully applicable to all personal data processing activities under the Data Act. These objectives can come into conflict during product development, as unrestricted access to data cannot be realized without risking the privacy of users. In the event of a conflict between the GDPR and the Data Act, the GDPR rules on the protection of personal data should prevail (cf. Article 1(5) of the Data Act). However, there are numerous unanswered questions, e.g. does the third party become a Controller under the GDPR when the Data Holder shares product data or related service data with them, in cases where these contain personal data. If so, who is responsible for informing the data subject and to make sure that the data subject stays informed how their personal data is being processed. The obligation to differentiate between personal and non-personal data as well as trade secrets bears a huge risk potential for data owners. Unclear or incorrect classifications of datasets can lead to liability issues, competitive disadvantages and uncertain legal consequences if, for example, personal data is inadvertently passed on with insufficient protection.

Proposed simplification: The Data Act (spec. Article 4 (1) and Article 5 (1) DA) should be accepted as a basis for processing personal data within the meaning of Article 6 (1) (c) of Regulation (EU) 2016/679**.** Consequently, the statement in Recital 7 of the Data Act asserting that the regulation does not create a legal basis for access to personal data or its sharing with third parties should be removed.

Furthermore, the Commission and the European Data Protection Board (EDPB) must help by publishing guidance on the detailed interplay between GDPR and the Data Act and how to protect the personal data of data subjects when such data is shared under the Data Act. For example, the introduction of standardised, technical procedures for the automated classification of data would help the data holder to categorize their data correctly. Certification programs for data management systems can serve as proof of compliance with these standards and strengthen confidence in the procedures used. In a second step, if the GDPR is revised with regard to the adoption a risk-based approach, the data sharing obligations under the Data Act must be taken into account and should prevail the GDPR rules. It might be necessary to include exceptions for certain processing activities related to data sharing obligations under the Data Act. Art. 20 GDPR (right to data portability) must be rebalanced in the context of the Data Act, which may provide for broader data access rights. An adaptation should extend the scope of application or integrate differentiated protection mechanisms that take into account the extended access rights in the Data Act.

Data economy

With the EU-Data Strategy in 2020, the European Commission set an ambitious vision for creating a European Single Market for Data. BDI strongly supports the idea on fostering the use and exchange of non-personal data for data-driven innovation. In recent years, the implementation of the EU data strategy has focused far too heavily on regulation. Companies must implement the numerous new legal requirements in their business processes under high pressure. It is therefore important that the new EU Commission focuses on incentives in support of voluntary data sharing. German industry urges policymakers at European and national level to adopt far-reaching changes to the Data Act to ensure that companies can implement the Data Act without unduly high costs. Therefore, we propose the following changes which we perceive as a precondition to ensure that the Data Act enhances rather than hampers Europe's competitiveness. However, we want to note that there are also stakeholders within the BDI membership who would like to see a bolder decision on or even a removal of the Data Act. We encourage the European Commission to implement the following changes:

Data Act: Reduce regulatory uncertainty and ensure practical implementation

Status quo: The Data Act is the key legislative element of the EU-Data Strategy with new legal provisions on B2B and B2C data sharing of IoT-devices, B2G data sharing obligations, switching requirement between data procession services, new contractual provisions regarding data and international data transfer. It came into force on 11 January 2024 and shall apply from 12 September 2025. Since the beginning of the legislative process, BDI has criticised the fact that the Data Act suffers from a structural deficit in form of an undifferentiated one-size-fits-all approach, which leads to many legal uncertainties for industry companies. There are still numerous aspects that create legal uncertainty within the data act provisions and especially with regards to other legal acts, especially the GDPR or the Trade Secrets Directive. For significant parts of the German industry the Data Act is primarily causing considerable costs Due to the high implementation costs and the existing legal uncertainties without providing a discernible economic benefit. There are great concerns that companies may be incentivized to design their products in a more data-efficient manner, thereby undermining the very objectives the Data Act aims to achieve. Against this background, we strongly recommend legal adjustments.

Proposed simplification: In the next years, the focus must be on the implementation of the new Data Act provisions and creating legal certainty by adjusting some of the key provisions of the Data Act. In addition to the concrete measures detailed below, the Commission must help by publishing guidance for the foreseen implementing acts. The European Data Innovation Board (EDIB) must be strengthened in order to ensure harmonisation of implementation within Europe and a close exchange with industry stakeholders. After the application of the EU Data Act, the EU Commission must review, in close consultation with the industry, where harmonization of the existing EU legal framework is necessary to strengthen the EU data economy and foster voluntary incentives for data use and data sharing in industry. An important element is fostering the implementation of the Common European Data Spaces as proposed in the EU-Data Strategy while considering national data space initiatives.

Data Act: Protection of trade secrets

Status quo: Trade secrets are of critical importance for most of the German industry. The risk of loss of such trade secrets due to becoming publicly available remains. Additionally, the exchange of such trade secrets possibly contradicts the antitrust prohibitions set out in Art. 101 and 102 TFEU.

Proposed simplification: The protection of trade secrets as well as IPR protection should prevail in a proportionate manner to the economic significance of trade secrets. For this reason, an ex-ante

exception to the obligation to provide data must be implemented accompanied by realistic requirements for claiming this exemption. For the event of a conflict of laws, it should be clarified, that antitrust regulations shall prevail.

Data Act: Clarify definitions

Status quo: Unclear definitions remain a key point of contention. They create enormous legal uncertainty for companies and have not yet been fully addressed.

Proposed simplification: Key definitions of the legal text should be specified, such as the definition of "data holder", "user" or the various definitions of the "data" in scope. Furthermore, a clear distinction should be provided in regard to "data processing services", which currently comprises the three common, but vastly different services IaaS, PaaS and SaaS. Finally, the definition of 'placing on the market' set in Art. 2 (22) should be specified to recognise that for certain categories of products with long development and certification cycles, market placement should be considered at product-model or -type level, rather than for each individual unit. In addition, it should be made clear that safety and security legislation take precedence over data sharing obligations.

Data Act: Limiting the scope of application for virtual assistants on B2C

Status quo: Virtual assistants according to Art. 1 (4) currently encompass all types of virtual assistants regardless of their field of use in B2B and B2C.

Proposed simplification: Art. 1 (4) should be limited to virtual assistants with regards to consumers. *"Where this Regulation refers to connected products or related services, such references are also understood to include virtual assistants for consumers insofar as they interact with a connected product or related service."*

Data Act: Right of the data holder to use data

Status quo: Currently the right to use and share data is centred around the user. This significantly amplifies the position of the user. While we fully support the goal to further innovation through data sharing, the data holder is de facto dependent of the user's decision whether and with whom data should be shared. This creates a new imbalance.

Proposed simplification: Data Holders should be legally granted the right to use and share data for purposes such as quality control, safety, research and development and diagnostics.

Data Act: Clarify the extent of Information obligations

Status Quo: The Data Act stipulates several information obligations towards the customer or data recipient (see Art. 3 (2) and (3), Art. 9 (7), Art. 26, Art. 28).

Proposed simplification: The extent of said obligations should be clarified. Additionally, the Data Act should account for overlapping information obligations.

Data Act: Exceptions for Small Mid Cap Entities on Chapter II obligations

Status Quo: Art 7 (1) provides some exceptions for small and micro-enterprises on the obligations of Chapter II.

Proposed simplification: In accordance with the "Omnibus IV-proposal"[3] the exemptions in Art. 7 (1) should also apply to medium-sized and small mid-cap enterprises. These enterprises are the engine of German and European industry and drivers of innovation and should not be restricted in the development of new innovations by excessive regulation.

Data Act: Limiting the exceptional need to use data for B2G

Status quo: The exceptional need to use data for non-emergency situations as grounds for public sector bodies to request the sharing of Data is far-reaching due to its broad nature, regardless of the prerequisites set in Article 15 (1) (b) DA.

Proposed simplification: Mandatory data sharing requirements should be limited to sharing requests resulting from public emergencies (Article 15 (1) (b) DA) only.

Data Act: Profiling

Status Quo: Currently Art. 6 (2) (b) DA prohibits third parties from profiling. As a result, the processing of non-personal data could be more restrictive than the processing of more sensitive personal data.

Proposed simplification: Art. 6 (2) (b) DA should be reevaluated and should be adapted to the requirements of the GDPR.

Data Act: Deletion of Art. 13 (4) and (5)

Status Quo: Chapter 4 provides special obligations regarding unfair contractual terms in B2B-data contracts.

Proposed simplification: What is considered unfair is generally determined by the law of the Member State that is to apply to the contract concluded. Art. 13 (4) and (5) are redundant in German law in particular, as German law on general terms and conditions already provides for effective control of unfair contractual terms, including B2B contracts. Art. 13 (4) and (5) also go far beyond what is necessary and severely restrict the freedom of contract between companies. Alternatively, the word 'in particular' in Art. (4) 1 should be deleted to create more legal clarity.

Data Act: Transition Period and Reassessment

Status quo: The Data Act is set to change industrial use as well as usability of data in an unprecedented manner. The implementation of the new requirements has not yet been completed in major parts of the industry.[4] In addition, many member states have not yet designated competent authorities. As such, many operative questions remain unanswered. Nonetheless, the Data Act is set to be applicable starting 12 September 2025.

Proposed simplification: The respective entries into force as set in Article 50 DA should be postponed by at least 2 years. Alternatively, due to many remaining uncertainties and the extent to which the Data Act is set to change industrial use as well as usability of data we propose an early reassessment of the Data Act within 18 Months of it taking effect.

[3] COM(2025) 501 final.
[4] Bitkom-Survey (2025): Only 5 percent of the companies have implemented the Data Act.

Data Act: Balance fixed term-contracts under Art. 23 & 25 Data Act

Status Quo: According to Art. 23 (a) Data Act, *"providers of data processing services shall not impose and shall remove […] obstacles, which inhibit customers from terminating, after the maximum notice period and the successful completion of the switching process, in accordance with Article 25, the contract of the data processing service".*

Proposed simplification: For fixed term contracts, contracts with a minimum term or self-renewing contracts, the Data Act permits that the contractual parties agree upon a contractual clause according to which the customer can initiate the switching process with effect to the contractually agreed end of the minimum or applicable contract term with a notice period of two months. The Data Act does not obligate the provider of a data processing service to accept a termination before the contractually agreed end of the minimum or applicable contract term. Alternatively, for fixed term contracts, contracts with a minimum term or self-renewing contracts, the parties may agree that the customer has the right to switch to another provider even before the end of the minimum or applicable contract term, but has to pay an early termination penalty to compensate the early termination of the contract. Which of the two alternatives is chosen remains fully subject to the parties' contractual freedom.

Digital Infrastructure

German industry has very much appreciated the attention to digital infrastructures attributed by the European Commission through the White Paper "How to master Europe's digital infrastructure needs", the Letta Report and the Draghi Report. The assessments correctly describe the status quo of digital infrastructures in terms of facing investment challenges, the need to stay resilient and technologically future-proof. They rightfully acknowledge the need for a more harmonized regulatory approach to digital networks, with the ultimate goal of achieving the Digital Single Market, which was also highlighted in the Letta Report. They also rightly identified the low profitability of the electronic communications sector and the resulting inability to fund the substantial investments required for modernizing the digital infrastructure as a key problem that has to be addressed. BDI fears that if these issues are not swiftly addressed, Europe's communication infrastructure will not enable European companies to develop and utilize the digital solutions necessary for maintaining European industry's global competitiveness. Recognizing the importance of digital networks for European industry's competitiveness as well as access to needs-based connectivity, the Digital Networks Act (DNA) should be the key digital policy initiative of the current European Commission and not only include ambitious deregulation but also foster further innovation in the sector.

European Electronic Communications Code: Reducing the administrative burden

Status quo: The EU Electronic Communications Code (ECC) was adopted in December 2018 as Directive (EU) 2018/1972. It consolidated and updated previous telecommunications regulations. Member States were required to transpose the Code into national law by 2020. Against the background of increased importance of state-of-the-art connectivity (Digital Decade targets), the EU Commission has published the EU White Paper "How to master Europe's digital infrastructure needs?" in February 2024. It identifies necessary policy reforms to improve the investment climate and structural market conditions to achieve the EU's digital objectives and create the digital networks of the future.

The roadmap of the EU Commission's legislative agenda for the telecom sector is further shaped by the Draghi Report, which critically assesses the decline of European competitiveness. The telecom sector in Europe suffers from a high level of fragmentation and low returns on capital invested compared to its peers. The report recommends significant reforms in the telecommunications sector, such

as in the current regulatory framework, in the area of merger control, and spectrum policy. The report also includes a concrete call to create a level playing field with Big Tech.

Proposed simplification: An urgent and ambitious reform of the current regulatory framework with the upcoming DNA is needed, as proposed by the European Commission in its White Paper as well as in Mario Draghi's report. To put it in his words, we should be "increasing legal certainty and reducing regulatory and administrative burden by ensuring that there are fewer, clearer, more fit-for-purpose, future-proof and coherent rules." Since the telecommunications sector is highly regulated, the European Commission should therefore reduce outdated, unnecessary red-tape and overtly bureaucratic requirements, improving framework conditions for investment in digital infrastructures. Moreover, the inter-linkages between various sector-specific as well as horizontal European (e.g. consumer law or cybersecurity law) and national regulatory approaches must be thoroughly assessed and fully considered when modifying the regulatory framework. Concretely, it is necessary to delete those overlapping sector-specific obligations that can be better covered by the horizontal legal framework, such as consumer law. Infrastructure-based competition must remain a cornerstone of the legal framework, enabling different infrastructure providers to coexist, and at the same time best safeguarding innovation, and continuous and efficient investments in infrastructure. Parallel infrastructures also create a resilient digital backbone that enables industrial processes to continue operating even in the event of crises and enemy attacks.

European Electronic Communications Code: Spectrum cost and duration

Status quo: The high costs of acquiring spectrum licenses through auctions have been a heavy burden for the European telecommunications sector in the past. While other markets around the world allow network operators to purchase spectrum licenses for longer time periods or even for permanent use, rights in Europe expire after 10 to 15 years and then have to be bought again. These recurring costs of spectrum licenses have deprived companies of the necessary investment funds needed to finance expansion of gigabit networks as well as to tackle current technological challenges.

Proposed simplification: The duration of spectrum usage rights is an important lever for the competitiveness of European telecommunication network operators. German Industries supports indefinite spectrum licenses or at least a longer duration of frequency usage rights of with a minimum of 40 years. Additionally, the right of spectrum prolongations by default should be introduced into the Digital Networks Act (DNA) and such prolongations should become the standard mechanism, for example as 40+40-year-licenses. This leads to greater investment security for companies and in turn boosts the quality, affordability and sustainability of networks. Enhanced coverage and bandwidth are integral for Europe's industry to harness the benefits of digital technologies. To also achieve more efficient spectrum usage in the future, we find that the principle of 'use it or lose it' is a sensible way forward, if it is applied equally to spectrum holders (e.g. broadcast). However, telecommunication network operators should always be consulted before losing spectrum rights since there might be good reasons for a slow network expansion. Additionally, spectrum policy should address the interests of telecommunication operators as well as the manufacturers of wireless equipment. Therefore, when looking at spectrum distribution, the usability of devices such as wireless microphones should be ensured through the provision of adequate frequencies.

Auctions are the best approach for the initial assignment of spectrum licenses. Thereafter, prolongations are the preferred way to support network expansions and updates. Regarding auction design, they should be configured to foster investments instead of extracting additional revenue for state budgets. Additionally, discriminatory auction designs that benefit market players due to their size or structure

have to be avoided. A future DNA, therefore, must support the goal of lowering the costs of spectrum licenses – as outlined in the White Paper – and underpin it with measures to reach it.

European Electronic Communications Code: Spectrum awarding / authorisation

Status quo: The general authorization regime established in 2002 and maintained in the Code replaced the previous regime of individual licenses / authorizations, by pre-establishing generally applicable conditions for the provision of electronic communication networks and services (ECNS). Yet, given the local character of the physical networks, and the fact that spectrum is deemed to be a national resource, authorizations are subject to conditions established by the Member States' competent authorities and granted and implemented at national level.

Proposed simplification: We generally support a more coordinated approach to the awarding procedure of spectrum in Europe. However, there is a delicate balance to be struck between a more centralized approach, which could limit local ability to respond quickly to changing market conditions or technological innovation, and the need to achieve large economies of scale, which are important for the introduction of new technologies. German industry believes that spectrum management and authorization procedures, including concrete timelines, have to remain the responsibility of Member States, while a certain level of coordination at EU level – e. g. on license duration being long enough, pro-investment auction design, early and coordinated availability of spectrum resources to create scale – must be ensured and further strengthened. German industry also generally supports a more coordinated approach to authorization. It has not yet been possible to create a single European market for telecommunications, in particular due to the sometimes widely divergent regulatory systems in MS. However, while the solution of a simplified and more harmonized European regulatory framework for networks and related services is a step in the right direction, it is not clear yet, if the deep fragmentation can be overcome.

As mentioned above, we also advocate for further measures to tackle the excessive bureaucracy for network operators, including a shift from the telecommunications sector consumer law towards a horizontal consumer law. In general, we believe that a significant reduction of the current regulatory framework addressing operators of digital infrastructures would have far more positive implications for the entire market than the harmonization of authorization can have.

In order to facilitate the deployment of small area wireless access points, Article 57 (1) third paragraph (providing for derogations from permit-free deployment) should be deleted. When it comes to reducing red tape, a large majority of the elements of Article 22 should be deleted, with only those directly inevitable for the regulatory decisions staying. Extensive information on broadband coverage is already widely available in the market, and transparency regarding consumer offerings is inherently in the interest of telecommunications companies. In general (and also with respect to Art. 20 & 21), data inquiries and usage purposes must be critically examined within a cost-benefit analysis and assessed in terms of their contribution to achieving set goals, such as accelerating fiber optic and mobile network expansion. It is crucial to limit these inquiries and purposes to the necessary minimum concerning scope, level of detail, format, and frequency. Any bureaucratic and planned economy approaches should be entirely avoided.

Gigabit Infrastructure Act (GIA): Accelerating authorisation procedures

Status quo: To achieve the goal of providing EU-wide high-performance internet access to companies and citizens – and thereby to reach the EU's targets for digital infrastructures – a vast amount of fiber optic cable and towers for mobile networks will have to be installed. This will only succeed within the targeted timeframe if existing expansion hurdles are reduced and the full potential for acceleration is exploited. Currently, the authorization procedures for new towers take on average 18 to 20 months in Germany. Such lengthy permit procedures significantly hinder a speedy expansion and modernization of digital infrastructures. The Gigabit Infrastructure Act, entering into effect in November 2025, aims to streamline permit procedures and accelerate the rollout of gigabit networks through accompanying measures. Yet, while containing various improvements which can accelerate network rollout, the GIA also introduces new burdensome bureaucracy. Such measures include the new requirement of Art. 6 (1) GIA for digital network operators to provide comprehensive information on a planned rollout in advance via a single information point. Art. 7 (4) foresees that authorities may refuse rollout permits in case operators have not previously notified their rollout plans acc. to Art. 6 (1) GIA. This new requirement hampers and slows down the authorisation time by two months rather than accelerating gigabit infrastructure rollout.

Proposed simplification: Fast authorization procedures are of utmost importance. To achieve the ambitious infrastructure targets that have been set, permit procedures must be streamlined, consistently digitalized and drastically shortened. The Gigabit Infrastructure Act has failed in introducing a binding tacit approval mechanism and allows Member States to derogate. Therefore, the GIA should be amended in the following aspects:

- Binding, fully digital administrative procedures for the authorization of digital infrastructure rollout should be introduced.
- Full-fledged tacit approval within two months after the submission of a respective building request should be introduced without any exceptions. Therefore, Art. 8 (2), (3) GIA should be deleted. The discretion for MS to require permits in specific situations (Art. 7 (8) and Art. 9 (3) a, b GIA) should likewise be abolished.
- Art. 7 (4) should be deleted, and the transparency requirements of Art. 6 (1) should be streamlined: A proactive notification requirement should only apply to projects financed exclusively with public money or otherwise supported with public resources.
- The approval / authorization of using public buildings for the deployment of VHCNs or associated facilities should be facilitated further. This is of utmost importance for the deployment of mobile network masts and antennas in particular. For this purpose, Art. 3 (10) GIA should be deleted, or at least the list of exceptions from the access obligations drastically shortened. Otherwise, substantial synergy potential for the necessary network rollout would remain untapped. This runs counter to the aims of the GIA.
- Art. 5 (3) allowing MS to deem unreasonable coordination requests targeted at wholesale-only operators in rural areas owned or controlled by public sector bodies should be deleted or changed in a way that in such cases, public WS-only networks have to deliver such passive infrastructure at fair, reasonable and non-discriminatory conditions.

Otherwise, operators of digital infrastructures will not be able to expand or modernize their infrastructures, and European industry will not be able to reap the benefits of state-of-the-art infrastructures for digital business models.

Funding & IPCEI: A simplified and coordinated support framework

Status quo: The transformation of the EU's connectivity industry requires significant investment capacities, in particular when compared to the massive investments made by large cloud providers into cloud, edge, and AI capacities. There are several EU funding instruments and programs that support private investments in R&I in relation to the communications sector. These include the Smart Networks and Services Joint Undertaking (SNS JU) under Horizon Europe, but also InvestEU, the Digital Europe Programme (DEP), Important Projects of Common European Interest (IPCEIs) and the Connecting Europe Facility (CEF) Digital.

Proposed simplification: A future DNA must substantiate the goals drawn up in the White Paper and underpin them with measures to reach those goals. Moreover, an industrial policy approach cannot just stand in isolation. To be effective, it should be integrated and streamlined horizontally across various policy areas impacting the digital infrastructure sector. A more simplified and coordinated infrastructure-related support framework would lead to a more efficient usage of resources – in terms of finances as well as personnel in both public institutions and private industry – resulting in enhanced connectivity for society and industry. Current programs, such as the IPCEIs, are often inefficient and over bureaucratic. Therefore, a more coherent approach, which provides a single point of entry for funding and brings together relevant actors of the ecosystem, is very desirable. Additionally, we support the idea of identifying strategic technologies and the build-up of technological capacities in those areas in Europe. A clear and coordinated industry strategy would enable synergy effects and leverage more private investment. For example, a new infrastructure focused IPCEI incorporated into a more active industrial policy, would be welcomed, as this would provide the funds necessary for the large-scale deployment of advanced digital infrastructure and support the goal of bringing Europe technologically back on par with the US and China.

To make a real difference in the roll-out of advanced digital infrastructure and support European companies in a meaningful way, a prospective IPCEI for infrastructure must be less bureaucratic, more streamlined and efficient. Especially, the time from announcement of the programme to the notification of the funding decisions must be significantly shortened if the project shall attract applications from interested companies. To achieve this goal, approval procedures must be simplified, digitized and accelerated. The European Commission should provide sufficient capacity for this. The IPCEI processes in individual Member States are currently not coordinated in terms of timing and are sometimes carried out in several, unaligned phases. There is an urgent need for better coordination and appropriate harmonization, even in the prenotification and notification phase. In addition, the funding must be substantial. In the past, IPCEIs had comparatively low funding volumes in the single-digit billion range per technology field compared to huge investment programmes adopted by global competitors, such as North America and China. Therefore, a future infrastructure focused IPCEI has to receive a designated budget within the EU budget, which is high enough to enable Europe to compete on a global scale. It is also important that the funding is not pulled out of already existing programs like Horizon Europe since this would weaken the support of other key technological areas.

Semiconductors

IPCEI and European Chips Act: Funding

Status quo: The first two Important Projects of Common European Interest (IPCEIs) already carried out and the third planned IPCEI on microelectronics as well as the funding under Pillar II of the European Chips Act are of outstanding importance for the European microelectronics ecosystem. However, the processes are lengthy and bureaucratic, which poses challenges for companies – SMEs in particular: It can take over two years from the first submission of documents to the grant notification. The uncertainty of funding and long delivery times for equipment largely reduced the applicable funding costs due to a reduction of the depreciation costs during the project runtime. Due to late project approvals, also the technological focus and the requirements for the equipment may have changed. This requires a constant update to the initially submitted financing plan and equipment plan and is still a major issue as regular official change requests must be submitted for every change.

Proposed simplification: Microelectronics has very short innovation cycles and is thus moving at very high speed. Long ap-plication processes, multi-level notification processes, together with long delivery times for equipment are in contradiction to these realities. The application, approval, and review of projects must be carried out quickly. The requirements for planning depth and technical details must be reduced to an appropriate level. The processes must be flexible to take changing conditions into account – they should be aligned rather with overarching European objectives and less focused on detailed rules.

Digital Services / Platform Economy

Digital Services Act (DSA): Impact on Intra-Group Hosting

Status quo: The Digital Services Act (DSA) applies even in cases of intra-group hosting. This means that when companies within the same corporate group host services or data internally, they must comply with the same requirements as if they were providing services to external parties. This poses significant challenges for businesses because internal operations are often subject to different dynamics and risks compared to external services. Requiring compliance with the DSA for intra-group hosting imposes unnecessary administrative and financial burdens on companies. They need to implement extensive compliance measures, such as content moderation, transparency reporting, and a single point of contact, even when these measures may not be relevant or necessary for internal operations. This can divert resources from more mission-critical activities and stifle innovation within the company.

Proposed simplification: To alleviate these issues, a corporate privilege should be introduced, whereby the DSA does not apply to intra-group hosting. This means that companies would not have to adhere to the stringent requirements of the DSA for services and data hosted within their own corporate group. The rationale behind this exemption is that the protective measures mandated by the DSA are designed to address risks associated with public and consumer-facing services, which are not typically present in internal corporate environments. Intra-group hosting does not expose personal data or content to the same level of risk as external hosting, rendering many of the DSA's provisions redundant. By exempting intra-group hosting from the DSA, companies can streamline their internal operations, reduce compliance costs, and focus on maintaining robust security measures tailored to their specific internal needs. This approach would ensure that the DSA's protections are applied where they are most needed, without imposing unnecessary burdens on intra-group activities.

Imprint

Bundesverband der Deutschen Industrie e.V. / Federation of German Industries (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobbying Register: R000534

Editors

Steven Heckler
Deputy Head of Department
Digitalisation and Innovation
T: +49 30 2028-1523
M: s.heckler@bdi.eu

Dr Michael Dose
Senior Manager
Digitalisation and Innovation
T: +49 30 2028-1560
M: m.dose@bdi.eu

Polina Khubbeeva
Senior Manager
Digitalisation and Innovation
T: +49 30 2028-1415
M: p.khubbeeva@bdi.eu

Philipp Schweikle
Senior Manager
Digitalisation and Innovation
T: +49 30 2028-1632
M: p.schweikle@bdi.eu

Adib Mehran (until 30th June 2025)
Student Assistant
Digitalisation and Innovation
T: +49 30 2028-1502
M: a.mehran@bdi.eu

Florian Puehl
Student Assistant
Digitalisation and Innovation
T: +49 30 2028-1603
M: f.puehl@ifg.bdi.eu

BDI document number: D2081