BDI

INNONATION

POSITION | DIGITAL POLICY | AI, DATA & CYBERSECURITY

Digital Fitness Check

Strengthening Europe's competitiveness through further targeted simplification of Europe's digital acquis.

10 March 2026

Executive Summary

It's important that the EU places competitiveness at the centre of its political reform agenda. The proposals for the Data and AI Omnibuses, the Regulation to establish EU Business Wallets, the Cybersecurity Package and the Digital Networks Act underline that the European Commission recognises in principle the necessity to cut unnecessary complexity, simplify regulatory requirements, and enhance coherence across the EU's digital rulebook to achieve this aim. With the above-mentioned legislative proposals, the European Commission has taken a first necessary step, however, this was not bold enough, since the EU Commission's proposal does not sufficiently address the regulatory burdens and risks that continue to undermine Europe's ability to foster innovation and enhance global competitiveness. Even worse, certain regulatory provisions continue to fundamentally erode the principles of fair competition.

German industry's policy recommendations

Therefore, as part of the Digital Fitness Check, the European Commission should continue its simplification agenda by proposing the following targeted amendments to the EU's digital acquis:

- **Artificial Intelligence:** Since early implementation experience shows the limits of applying horizontal AI rules to established sectoral frameworks, particularly those under Annex I Section A, high-risk requirements related to Annex I A should be integrated into sectoral legislation. No harmonised standards will be available for the transparency obligations under Article 50 of the AI Act. Therefore, a grace period of 12 months for AI deployers that need to disclose AI-generated content as such, should be introduced. Existing legislation – notably the AI Act, the General Data Protection Regulation and the Platform Work Directive – already provides comprehensive rules for the deployment and use of AI in the workplace, therefore, no additional AI-specific labour legislation should be introduced.
- **Cybersecurity**: We regret that the Digital Omnibus does not address the necessary reforms of the CRA. German industry urges the Commission to postpone the application of the CRA to allow industry to adapt, and ensure the availability of fit for purpose, consensus-based and cited harmonised standards. The implementation of the CRA is currently experiencing difficulties, including the development of a massive set of harmonised standards (+40) against unrealistic timelines, designation of notified bodies, and clarification of key questions around scope (e.g. placing software on the market, remote data processing solutions) and essential

Bundesverband der Deutschen Industrie e.V. / Federation of German Industries
EU Transparency Register: 1771817758-48 | German Lobbyregister: R000534
Dr Michael Dose, Mariia Halada, Steven Heckler and Polina Khubbeeva | Innovation, Security and Technology | www.bdi.eu

cybersecurity requirements. Removing non-critical – benign – products from the scope of the CRA would significantly reduce the burden on manufacturers while maintaining a high level of security and competitiveness within the EU. The implementation of the NIS2 Directive is characterised by fragmentation, with divergent national transpositions and instances of gold-plating. This has increased the regulatory burden for companies without necessarily enhancing cyber resilience. To ensure true simplification and legal certainty, further maximum harmonisation and clarification of key NIS2 concepts are essential. In addition, while the single reporting entry point introduced by the Digital Omnibus is a helpful first step to reduce the administrative burden from overlapping reporting obligations, the underlying regimes under NIS2, CRA, GDPR and others still diverge in what qualifies as a reportable incident, as well as in timelines, criteria and information requirements. Incident-reporting obligations should therefore be further harmonised.

- **Data protection:** While the proposal for amending the GDPR already entails some positive changes to the current regulatory framework. However, serious problems that continue to have a significant impact on the innovative capacity of European companies and entrepreneurs have not been adequately resolved and must be addressed urgently in the further legislative process or at the latest as part of the EU's Digital Fitness Check – in particular clarifications in Article 9 (1) of the GDPR and regarding the ePrivacy exemptions.
- **Data usage:** Since the proposal for the Data Omnibus unfortunately falls short of creating clarity and coherency both within the Data Act, e.g. further protection of trade secrets, clarifications regarding Chapter VI, utilising and monetising of data for data holder and regarding its interplay with further legislation such as the GDPR, a more ambitious reform agenda of the regulatory framework is required. Coherency, which in turn would provide more legal certainty, could be achieved by specifying key definitions. Conversely redundant regulation should be avoided as it could contradict coherency. Otherwise, the streamlining of the digital acquis into the Data Act creates new legal uncertainties.
- **Quantum Technology:** BDI welcomes the initiative of the European Commission to develop the EU Quantum Act to facilitate the implementation of the EU Quantum Strategy. The Act should focus on research and innovation, industrialisation and supply chain resilience. It must be ensure that the EU Quantum Act facilitates industrialisation activities, follows a technology-neutral approach and does not lead to increased bureaucratic burdens.

Table of Content

Artificial Intelligence

Separate the postponement from the rest of the proposal and postpone the high-risk requirements for 24 months

The Commission's proposal to postpone high-risk requirements is a step in the right direction but remains insufficient. The suggested postponements (up to 16 months for Annex III systems and up to 12 months for Annex I A systems) cannot be adopted in time through the ordinary legislative procedure. The lengthy negotiation cycles of past EU legislation demonstrate that a timely decision is unrealistic, leaving providers and deployers with only a few months before obligations enter into force in August 2026.

To ensure that the mechanism can be adopted swiftly, BDI calls for separating the timeline adjustments from the rest of the Omnibus and fast-tracking them through simplified parliamentary procedures. A standalone proposal would allow urgent adoption of points 30 and 31 and their recitals, while the remaining Omnibus provisions could proceed at normal pace.

Substantively, the proposed postponements do not reflect the scale of implementation challenges. Companies will depend on up to 35 harmonised standards, each of which requires significant time for development and internal adoption. Even a single standard typically requires at least 12 months to implement. A transition period of only six months between finalisation of standards and applicability of Annex III requirements would slow product releases, reduce investment and undermine innovation. The dual timeline mechanism, which can be triggered unilaterally by the Commission, further reduces planning certainty.

To ensure workable implementation, BDI calls for a 24-month extension of all high-risk requirements under Annex I and Annex III, including a corresponding 24-month deferral of fines for non-compliance.

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

Early implementation experience shows the limits of applying horizontal AI rules to established sectoral frameworks, particularly those under Annex I Section A. The development of harmonised AI standards is progressing more slowly and with greater complexity than anticipated, leaving manufacturers uncertain about how new AI-specific standards will align or conflict with existing sectoral requirements. This ambiguity risks creating bottlenecks and destabilising long-standing compliance pathways.

The challenge is especially acute in conformity assessment. Notified bodies in highly regulated sectors such as automotive, machinery and medical devices are already operating at capacity. Adding AI-related obligations without a clear integration pathway could compound delays and disrupt market access, disproportionately affecting sectors where Europe holds global competitive advantages.

For these reasons, Annex I should be streamlined by merging Sections A and B and applying the more flexible Section B logic across the entire annex. This approach would allow AI requirements to be incorporated progressively into sectoral frameworks, ensuring that harmonised AI standards can be embedded into existing systems without undermining established conformity procedures.

Integration must follow a sequenced approach grounded in existing legislation. The objective is not to reopen functioning regulatory systems, but to align them with the AI Act in a way that preserves legal certainty. To achieve this, the simplification package must clarify the AI Act's role as a maximum-harmonisation instrument: sector-specific measures, whether delegated acts, implementing acts or technical specifications, must not introduce requirements beyond the AI Act. This is essential to prevent inconsistent obligations and to maintain a unified understanding of the 'state of the art' across sectors.

Refrain from introducing additional AI-specific labour legislation

There is currently no need for additional AI specific labour legislation, such as the planned Quality Jobs Act. Existing legislation – notably the AI Act, the General Data Protection Regulation and the Platform Work Directive – already provides comprehensive rules for the deployment and use of AI in the workplace, offering sufficient safeguards for workers' rights and safety. Before introducing new legislation, these frameworks must first be fully implemented and evaluated in terms of their effectiveness, practicality, and impact on European digital innovation and competitiveness.

Avoid unnecessarily burdensome notification processes

We welcome the Commission's intention to simplify the notification procedure for conformity assessment bodies. In its current form, however, the proposal does not achieve this goal and leaves important questions unresolved, particularly for bodies already notified under sectoral legislation.

A key gap concerns scope extensions. Although the draft refers to a single application and assessment procedure, it does not clearly state that existing notifications may be expanded through an AI-related gap assessment. Instead, the wording suggests that already-notified bodies may be required to undergo a full new notification process. This would contradict the objective of simplification and delay the availability of notified bodies for high-risk AI systems.

BDI also stresses that the internal control procedure under Article 43(3) must not be subject to optional deviations. Allowing exceptions would weaken the coherence of the conformity assessment system and create uncertainty for companies operating across multiple Member States. A uniform approach is essential for maintaining confidence and consistency in the internal market.

BDI therefore recommends three adjustments:

1. Establish a clear and straightforward process for extending existing sectoral notifications through an incremental gap application and gap assessment.

2. Remove the dependency on sectoral legislation for the availability of a single application or single assessment procedure.

3. Delete technology-based partial notifications in Annex XIV Section 2(3) to avoid unnecessary fragmentation.

Postponement of transparency obligations of 12 months must apply for both providers and deployers of GPAI-systems

No harmonised standards will be available for the transparency obligations under Article 50 of the AI Act. The Commission has begun drafting guidance and a code of practice, but these will not be finalised before May or June 2026, leaving only a few weeks before the rules apply. The AI Omnibus therefore proposes a six-month enforcement delay for certain obligations for legacy generative AI systems placed on the market before 2 August 2026, specifically those under Article 50(2), which require providers to mark AI-generated outputs.

However, no grace period is given to AI deployers that need to disclose AI-generated content as such, even though AI-marking may not be available at that time. For consistency, the proposed grace period should also cover Art. 50(4) and be extended to 12 months, to ensure that providers and deployers have sufficient time to analyse and implement the code of practice.

Moreover, the restriction of the grace period to 'systems placed on the market before 2 August 2026' creates an unworkable compliance gap. Providers and deployers will lack adequate time to align systems entering the market immediately after this date with the code of practice before requirements take effect. This could severely delay market entry for many generative AI systems planned to launch shortly after 2 August 2026, thereby distorting the market. The restriction to 'systems placed on the market before 2 August 2026' must therefore be removed.

Certain provisions of Article 50 will not be addressed by the code, but only via guidelines, including provider and deployer information obligations to natural persons either interacting with the AI or exposed to it. As these guidelines are also only expected just before the summer 2026, the grace period should also cover AI providers and deployers in scope of Art. 50(1)-(3), so that they have enough time to adapt their AI systems. BDI further calls for clarity regarding Article 50(7). Transparency requirements must be proportionate in B2B contexts. In industrial environments, transparency is already ensured through contractual obligations, documentation and established processes among professional operators. The regulation should explicitly recognise this and avoid imposing consumer-facing transparency requirements on purely B2B use cases.

Adaptivity as an Essential AI Characteristic

BDI proposes clarifying in Article 3 that adaptivity constitutes an essential characteristic of AI systems. This includes the capacity of an AI system to adjust parameters or behaviour in response to environmental changes or new input data.

A clear definition is necessary to ensure consistent interpretation across sectors and to distinguish AI systems from static software components governed by existing product legislation.

Enshrine the legacy clause clarifications into the operative provisions

Recital 21 provides important clarification on the legacy clause in Article 111(2). It confirms that once an AI system has been placed on the market or put into service before the high-risk requirements apply, all units of the same type and model benefit from the legacy clause, including those placed on the market afterwards. It also confirms that substantial modifications trigger renewed compliance obligations for both future units and those already in use.

These clarifications are necessary because the concept of an “individual product unit” does not fit AI systems, which are often distributed as software through continuous update channels. In sectors with long development and certification cycles, market placement must be understood at model or type level rather than for each single unit.

To ensure legal certainty, the clarifications made in Recital 21 should be incorporated into the operative text of Article 111. This would also help address potential inconsistencies with NLF legislation under Annex I, which follows a different logic for placing products on the market.

In addition, the AI Act should harmonise the terminology around “substantial change” and “substantial modification” to ensure consistent interpretation throughout the Regulation and avoid diverging legal outcomes.

Remove the Fundamental Rights Impact Assessment from the AI Act

Art. 27 requires providers of high-risk AI systems to conduct fundamental rights impact assessments (FRIAs). These assessments evaluate how the AI system itself may impact individuals' fundamental rights, including human dignity, non-discrimination, and freedoms protected under the EU Charter. At

the same time, Art. 35 GDPR requires data protection impact assessments (DPIAs) to assess how the processing of personal data may affect individuals' rights and freedoms.

Whilst the two assessments seem to differ in focus – FRIAs assess the AI system, whilst DPIAs assess personal data processing – in practice they cover practically the same concerns. Conducting both assessments would lead to redundancy and obviously increase the compliance burden for public authorities and companies in scope, while not meaningfully contributing to better protection of fundamental rights. [4]

Therefore, we suggest removing Article 27 from the AI Act.

Align legal bases with the GDPR

The AI Omnibus introduces a new Article 4a to provide a legal basis for the exceptional processing of special categories of personal data for bias detection and mitigation. While we support the intention, the provision does not add substantial clarity compared to Article 10(5). Its main effect is to extend the scope from high-risk providers to high-risk deployers and to providers and deployers of other AI systems. Beyond that, the legal framework remains fragmented.

At the same time, the Commission's Digital Omnibus proposes amendments to the GDPR, including a new Article 88c that would allow the processing of personal data for the development and operation of AI systems on the basis of legitimate interest. This approach is more flexible than the AI Act and creates a risk of inconsistency between the two instruments. Alignment is therefore necessary. A clear and streamlined version of Article 88c should form the basis for revising Article 4a of the AI Act; otherwise, companies and public bodies may avoid using personal data needed to improve AI systems, weakening the effectiveness of bias-mitigation measures.

It must also be made clear that Article 88c is not limited to processing employee data. Restricting it to the employment context would not reflect industrial AI practice and would unnecessarily limit the lawful use of customer and operational data for development, testing and quality assurance.

Making an AI system available to other entities in the same corporate group does not constitute a 'placing on the market'

Clarification that entity does not become a provider of an AI model merely by making it available to other entities within the same corporate group (in the definition of "provider" in Article 3(3) or "placing on the market" in Article 3(9) AI Act).

We would welcome the inclusion of a definition of 'user' of an AI system as a negative demarcation. This definition should also be understood as broadly as possible and refer to AI systems that are 'deployed in non-product-related contexts.

Mediating role of the AI Office in case of diverging interpretation between member states

The competencies of the AI Office should be extended to include the resolution of inconsistencies between national supervisory authorities. Since AI deployment can occur EU-wide, differing interpretations by supervisory authorities are likely. However, no escalation mechanism currently exists. The AI Office, as a 'supervisory authority' overseeing supervisory authorities, should be granted a mandatory mediating function within a three-month period so that disputed legal questions can be resolved. After attempting clarification with national authorities, affected providers or operators should also have the right to escalate matters to the AI Office

Clarification and removal of specific application areas from Annex III

A review of Annex III is needed to clarify and, where appropriate, remove specific application areas. The Commission should make active use of the procedures under Article 6(6) and (7) and Article

7(3). As an immediate step, the guidelines should clarify that risk assessments in life and health insurance under Annex III(5)(c) that do not influence pricing, or the selection of policyholders are generally not considered high-risk.

Further clarification is also required for Annex III(5)(a). As currently drafted, there is a risk that AI systems used for purely organisational tasks in the healthcare sector, such as managing bed allocation or other administrative planning, could be interpreted as falling under the high-risk definition. Since such systems do not create material risks for fundamental rights, the provision should make clear that organisational and administrative functions are excluded. This can be achieved by removing the word “grant” and adding an explicit exclusion for organisational services such as billing and inventory management.

The provision should therefore read:

“***AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to reduce, revoke or reclaim such benefits and services, excluding organisational services such as billing and inventory management.***”

Article 11 and Annex IV

The requirements concerning documentation as set out in Article 11 and Annex IV remain too extensive. While BDI welcomes the addition of SMEs to the simplification, German industry reiterates its proposal to simplify the documentation requirements for high-risk AI systems in general. Additionally, templates should be provided that are based on examples. The use of templates should be mandatory if no personal data is involved

Article 51 and 54 – General Purpose AI

The threshold value for GPAI pursuant to Art. 51 II AI Act has not been adjusted. 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.

Data Act

Article 2 – Definitions

To support implementation, 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. 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.

More unclarity due to simply squeezing different regulations into the data act: In the context of the definition “permission”, Art. 2 (4b) states that ‘permission’ means giving *data users* the right to the processing of non- personal data. However, the concept of 'Data user' is not explicitly recognized in the Data Act. Same with Art. 2 (4c) ‘access’ means data use […]. The mere transfer of the definition of 'access' from the DGA creates additional uncertainties. According to the Data Act, the “use of data” is determined by the respective role through contractual agreements. The mere technical access to data does not, under the Data Act, provide a basis for someone to have the right to use or control that data. Furthermore, this definition of 'access' creates tension with the concept of 'on-device access' in the definition of 'connected product' and 'network access' in the definition of 'data processing services'. Both of these concepts involve different types of access that are subject to specific legal and regulatory conditions, which may not necessarily align with the broader understanding of 'access' in the DGA. This highlights potential inconsistencies and challenges in aligning the different regulatory definitions.

The concept of 'dynamic data' is not recognized in the Data Act. It should be clarified, how this definition fits into the cascade of existing data definitions that fall within the scope of the Data Act.

Article 4 (13, 14) – Right of the data holder to use data

The Digital Omnibus proposal of the European Commission so far misses the opportunity to amend Articles 4 (13) and 4 (14) of the EU Data Act. The Data Act's framework for non-personal data is considerably more restrictive than the GDPR’s regime for personal data. Although both regimes follow the same dogmatic structure (i.e. a general prohibition with a reservation of permission), the Data Act only provides for a single legal basis, namely the contractual consent of the user. Paradoxically, this regulatory design creates a strong factual incentive for organisations to rely more heavily on personal data – despite its inherently higher sensitivity – rather than on non-personal data.

Further, in many cases, the requirement to conclude a contract with the user is not only burdensome but commercially and technically unfeasible for data holders as they often do not know who the end-user is. Data Holders should therefore be legally granted the right to use and share data for purposes such as quality control, safety, research and development and diagnostics, except to the extent Users have informed the Data Holders that they are using the connected products and related services for research and development purposes (e.g. laboratory equipment).

To address these issues, we propose consolidating Articles 4 (13) and 4 (14) into a single, comprehensive provision under Article 4 (13) and redraft the respective Recitals:

(13) [1]*A data holder shall only use any readily available data that is non-personal data only if and to the extent that at least one of the following applies:*

(a) the user has given permission to the use of the non-personal data for one or more specific or general purposes;

(b) the use is necessary for the performance of a contract to which the user is party or from which the user benefits or in order to take steps at the request of the user prior to entering into a contract;

(c) the use is necessary for compliance with a legal obligation to which the data holder is subject;

(d) the data holder pursues a legitimate interest, including, but not limited to, developing new products or services, improving the functioning of any product or service, monitoring or maintaining the product or service.

[2]A data holder shall not use the data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any manner that could undermine the commercial position of that user on the markets in which the user is active. [3]Where a data holder makes data available to a third party on the basis of this paragraph, the data holder shall, where relevant, contractually bind the third party not to further share data received.

(14) (deleted)

Article 7 (13) – Exceptions for Small Mid Cap Entities on Chapter II obligations

In accordance with the "Omnibus IV-proposal" 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.

Article 13 (4, 5) – Limiting the scope of unfair contractual terms

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.

Interplay with the GDPR

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.

Application of the Data Act on used products

The Data Act does not contain any explicit clarification that used products placed on the market before the deadline pursuant to Article 50 (3) and now resold are not subject to the Data Act. While such used connected products placed on the market before the deadline are therefore not subject to the obligation under Article 3 (1), this does not exclude the applicability of the other provisions of the Data Act, e.g. the information obligations pursuant to Article 3 (2) of the Data Act – just like a manufacturer or retailer who is placing a connected product on the market for the first time. Anyone who wishes to sell a connected product that is several years old will be confronted with an unforeseeable additional requirement and the associated bureaucracy. This could significantly restrict the resale of used connected products. Therefore, it must be clarified that the EU Data Act does not apply to connected products placed on the market before 12 September 2025, when resold.

Application of Article 3(1)

BDI urges to reconsider the timeline for the application of the direct access obligation under Article 3(1) DA, which is currently set to become applicable in September 2026. At that point in time, key interoperability and data format standards relevant for the practical implementation of direct access are still under development and are not expected to be adopted before the end of 2026 or the beginning of 2027.

These standards are essential to enable companies to provide data in a structured, interoperable, and scalable manner and to unlock the intended value of the Data Act. However, their implementation will require substantial technical and organisational efforts. Holding companies accountable for compliance with Article 3(1) before such standards are available would therefore be unreasonable and would significantly increase legal and operational risks.

Moreover, even after the publication of relevant standards, companies will require a reasonable transition period, estimated at approximately 12 months, to analyse, implement, and operationalise them across their product portfolios and data infrastructures.

Without a corresponding adjustment of the applicability timeline, there is a significant risk that manufacturers would be forced to implement interim solutions and subsequently re-engineer their systems once standards become available, resulting in duplicated efforts, unnecessary costs, and inefficient use of resources. This risk exists even if the standards are formally non-binding, as they may still be incorporated into contractual requirements by customers or business partners.

Data economy – Overarching EU Commission responsibility

The Data Act has the potential to serve as a powerful framework and enable the joint European Data Market. The Data Acts core provisions - such as the definitions governing access to data from connected products, the obligations for manufacturers and service providers, and the rules for data sharing (including financial compensation) - must not lead to legal uncertainty by over-lapping with/overriding existing horizontal or vertical legislation. Therefor we recommend that DG CNECT should be established as the overarching authority for data legislation within the EU Commission.

Renewable Energy Directive III (RED III): Repeal Article 20a (3) (EU) 2018/2001 amended by Directive (EU) 2023/2413 of 18 October 2023

Status quo: Art. 20a paragraph 3 of the Renewable Energy Directive brings new and significant requirements which have partly been laid down by previous Regulation, e. g. the EU Data Act. This introduces an unclear scope of requirements for manufacturers and confuses customers and third parties in many ways, creating legal uncertainty for all European data market participants. Additionally, Art. 20a RED contains a deviant compensation regime to the one of the Data Act. Moreover, since this is a directive, a worst-case scenario could be 27 different national implementations, each with varying obligations.

Proposed simplification: If new requirements regarding data provisioning of Battery Management System data were to be introduced, this should be done by changing (EU) 2023/1542, EUBR, whilst adhering to the Data Act with respect to governance and compensation regimes.

Further, sufficient lead time has to be allowed, taking into consideration that various horizontal and sectoral legislations with respect to data have recently been introduced with a considerable impact on large, medium and small businesses as well as Startups in one of Europe’s key industries: Automotive.

GDPR

German Industry supports the targeted approach of amending the GDPR with respect to practical problems and barriers to innovation. Several issues in need of reform have been addressed by the omnibus proposal (e.g. the relative identifiability in Article 4 or new measures to reduce abusive or excessive data subject requests); however, many more issues remain unsolved. To truly enable Innovation more needs to be done and some parts of the proposal must be adjusted and seriously reconsidered, such as the proposed amendments in Articles 88a and b GDPR.

In general, the principles of data protection require modernization to reflect technological developments and modern methods of data processing. This applies in particular to the principles of purpose limitation, storage limitation, data minimization, and the unlimited accountability of the controller, which are increasingly at odds with processing operations in the light of Big Data, Artificial Intelligence. Furthermore, implementing a general risk-based approach is widely considered as a suitable amendment to resolve prevailing issues. In addition, the legislative process should include an extension of the powers of the European Commission to adopt implementing acts for sector-specific, innovation-relevant interpretations of the GDPR.

Missing risk-based principles and weak innovation orientation

The omnibus picks up risk-based elements in places but does not embed them systematically. The GDPR's principles in Article 5 still lack an explicit risk-based approach, leaving room for very strict, sometimes absolute, interpretations in non-harmonised areas (e.g., legitimate interests, profiling, new data-intensive technologies). The GDPR also lacks an explicit reference to innovation in its objectives. Innovation capacity, efficiency and competitiveness are not recognised as legitimate factors in balancing, even though the omnibus (e.g., Articles 88c and 41a) shows that such a balance is possible and politically intended.

Article 9 (1) – Scope of special categories of personal data

Currently the scope of application for information protected by Article 9 (1) is frequently interpreted broadly. However, such an interpretation prevents innovation outright, where such innovation is dependent on information that is subsequently prohibited to be processed. While the information may result in the identification of a person, it often is collected without the intention or even necessity of identifying the person. This is the case, for example, where image or video data is needed to develop autonomous driving systems. If the potential for such systems is to be used for the whole of society, they must be able to include all of society, for example by recognising a person depending on the use of a wheelchair or other. To achieve this, Article 9 (1) should be amended, so that the scope is clearly limited to instances where the information directly reveals special categories of personal data.

NIS 2 Directive (NIS2)

The requirements for companies under NIS-2 should be simplified. If a company provides services in accordance with the Digital Services Implementation Regulation exclusively within its own group of companies, these internal services should be assessed differently. Such intra-group services should be exempt from the requirements of the Digital Services Implementation Regulation.

In addition, while the Digital Omnibus and the proposal for a Directive amending the NIS2 Directive introduces helpful measures such as the introduction of the single reporting entry point and maximum harmonization for cybersecurity risk management measures, additional key elements would also benefit from maximum harmonization and clarification.

Clarify relation of data disclosure between EU Data Act and NIS2

Status quo: The Data Act requires the disclosure of data, even in security-critical contexts. This may conflict with the NIS-2 Directive's requirements for confidentiality and encryption. Especially in critical infrastructures, unregulated data access can pose severe cybersecurity risks.

Proposed simplification: The EU Commission should clarify that in case of conflict, national implementation of the NIS-2 Directive takes precedence.

Ensuring consistent application of the main establishment principle and expanding its application to Annex II entities

Status quo: The main establishment principle remains a cornerstone of NIS2. It enables the one-stop-shop mechanism by ensuring that entities within scope interact primarily with a single competent authority in the Member State where key cybersecurity risk-management decisions are taken. This principle is essential for reducing administrative burden and avoiding fragmented supervision.

However, in practice, Member States have adopted differing interpretations of the concept. Some apply an expanded notion of "main establishment" that goes beyond NIS2, while others do not apply the concept at all. Different interpretations of 'main establishment' lead to additional complexity for companies operating cross-border as they need to register in several Member States sometimes even multiple legal entities which undermines the simplification efforts and harmonization objectives of NIS2.

Further complexity arises for entities that simultaneously provide ICT and fall under a service category listed in Annex II. It is unclear whether legal entities concerned should rely on the main establishment principle under Article 26(2), registering only in the Member State where cybersecurity risk-management decisions are made, or whether they must register in each Member State where they have an establishment, thereby triggering multiple supervisory regimes.

Proposed simplification: To further reduce regulatory complexity, we recommend extending the main establishment principle to Annex II entities and introducing maximum harmonization so that Member States cannot diverge in its interpretation or application.

Harmonising incident reporting timelines and significant incident thresholds

Status quo: Further harmonisation is required regarding incident reporting obligations. Under the NIS2 Directive, the timeline for initial incident notification is established at 24 hours. Nevertheless, some Member States have introduced shorter timelines. These earlier deadlines place additional constraints on entities, as in some cases they require reporting before sufficient situational awareness is available

and divert critical resources during the early stages of incident response. This ultimately limits the value of the information provided to CSIRTs.

Similarly, while the NIS2 implementing regulation on critical entities and networks sets the thresholds for defining a “significant incident”, some Member States have not adhered to these thresholds and require that any type of incident be reported to the relevant authorities and CSIRTs. This risks leading to overreporting, which can quickly overwhelm both regulators and companies.

Proposed simplification: We recommend introducing maximum harmonization of reporting timelines and reporting thresholds.

Ensuring greater harmonization and alignment of incident-reporting obligations

Status quo: The introduction of a single-entry reporting point in the Digital Omnibus is a welcome development. However, incident-reporting obligations across NIS2, GDPR, DORA, the AI Act and the CRA still diverge in terms of definitions and scope of what constitutes a reportable incident, thresholds and timelines. Moreover, the Digital Omnibus does not render the single reporting entry point the one-stop-shop for the AI Act and does not explicitly do that for the CRA. Information requirement and reporting templates still vary across legal frameworks and, in the case of NIS2, according to the law of the Member State. As a result, reporting of the same incident under one regime will often not fulfil obligations under another, for example, between CRA and NIS2, or even between different NIS2 national transpositions, where Member States may request different levels or categories of information. This lack of harmonization means that, even with a single platform, entities would still be obliged to prepare multiple tailored reports for a single incident. In practice, this diverts valuable resources away from mitigation, response, and recovery efforts.

Proposed simplification: To ensure genuine simplification, further harmonisation is needed regarding definitions and the scope of reportable incidents, timelines, core data fields and reporting templates.

Cyber Resilience Act (CRA)

German industry is disappointed that the European Commission did not utilise the Digital Omnibus for targeted changes to the CRA, which would have been however paramount to ensure the availability of certain products on the European market and to minimise legal uncertainty. We call on the European Commission to address the following areas of concern at the latest during the fitness check:

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 while most underlying horizontal standards for ‘security requirements relating the properties of the products with digital elements’ are not even due until October 2027. If standards that trigger a presumption of conformity are not available in time, essential products such as routers, operating systems or microprocessors with security-related functionalities would have to be certified by an external conformity assessment body - a significant bottle neck when it comes to placing a product on the market.

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 – 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 as across all levels challenges remain regarding whether all actors will be fully prepared to implement the expected requirements and harmonised standards in time. As mentioned above, harmonised standards are still under development, leaving limited time for every supply chain participant, from component manufacturers to system integrators, to adapt processes once these standards are finalised. In addition, the CRA adds CE marking requirements obligations for certain components with digital elements that are now classified as stand-alone products. These components have not previously been CE marked separately from the finished product. This marks a significant shift in conformity assessment, requiring all supply chain actors to adjust their strategies during the transition. Achieving this will demand close collaboration across the entire supply chain, which will be challenging given the short compliance timeframe. Meeting CRA requirements will involve extensive due diligence on third-party components, ensuring compliance with cybersecurity obligations at every supplier tier. If any part of the chain is unprepared, delays or shortages of essential components could impact critical projects and infrastructure.

In addition, 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 11, 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) or Annex VIII Modul H 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 for “important” products 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.

Introduction and Exclusion of 'Benign Digital Products with digital elements' (Articles 2 and 3)

Status quo: Many connected products – such as DAB radios, bike computers, radio clocks, barcode scanners, analogue-to-digital converters or integrated microchips – do not pose a relevant cybersecurity risk. Although they transmit data and are therefore covered by the CRA, this data is exclusively trivial and often processed within a single device. 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 (and that are also unable to implement any meaningful cybersecurity measures). 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.

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.

Currently, the CRA requires manufacturers to notify any actively exploited vulnerability or severe incidents they become aware of, even if the vulnerability does not affect products or services provided within the Union. This can lead to unnecessary reporting for issues with no impact on EU users.

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

Manufacturers should only be obliged to notify exploited vulnerabilities and severe incidents when the vulnerability or incident materially affects the security or functionality of products with digital elements within the Union. This would ensure proportionality and reduce administrative burden while maintaining strong protection for Union-based consumers and systems.

Article 14:

1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements ***affecting users in the Union*** that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.'

CRA 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.

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. The number of hEN to be defined for EU CRA shall be considerably reduced. Instead, established and existing standards from vertical, industry-related regulation shall be considered. 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 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.

Definition of "becoming aware" of an actively exploited vulnerability and severe incident (Article 14)

Status quo: Currently, the CRA requires manufacturers to notify when they "become aware" of an actively exploited vulnerability and a severe incident but does not define what "awareness" means. This lack of clarity creates legal uncertainty and risks premature or inconsistent reporting based on unverified suspicions. The NIS2 implementing act 2024/2690 Recital 31 provides a detailed definition and pathway for "becoming aware" for significant incidents. Since the majority of European companies in manufacturing has to fulfil both obligations, this already agreed pathway should be promoted for the CRA obligations to report several incidents and actively exploited vulnerabilities. The pathway sees "becoming aware" after a timely initial assessment.

Proposed simplification: Defining “becoming aware” as the manufacturer having a reasonable degree of certainty based on sufficient and reliable information ensures that notifications are triggered only when there is a substantiated basis, not mere preliminary indications. The process should foresee a timely assessment by the manufacturer on the severity, nature and exploitation of incidents and vulnerabilities. This approach aligns with the principle of proportionality, supports effective incident and vulnerability management, and reflects established regulatory practice in similar contexts, thereby improving legal certainty and reducing unnecessary compliance burdens.

German industry would welcome the implementation of the following amendments to the current draft law:

11. *With regard to the first paragraph, when a manufacturer has detected a suspicious event or vulnerability, or after a potential incident or vulnerability has been brought to its attention by a third party, such as an individual, a customer, an entity, an authority, a media organisation, or another source, the manufacturer should assess in a timely manner the suspicious event or vulnerability to determine whether it constitutes an incident or vulnerability and, if so, determine its nature and severity or exploitation. The relevant entity is therefore to be regarded as having become ‘aware’ of the severe incident or actively exploited vulnerability when, after such initial assessment, the manufacturer has a reasonable degree of certainty that a severe incident has occurred or a vulnerability is actively exploited.*

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 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

Documentation Obligations

Status quo: Annex VII of the CRA 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 Article 13(7) CRA, 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) 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) CRA 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.

Recognise 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 to reduce the bureaucratic burden and to speed up the implementation of the CRA.

Level playing field for CRA Market Surveillance

Status quo: Effective CRA market surveillance demands a level playing field. The existing landscape is fractured by a complex web of digital legislation (CRA, NIS2, CSA, AI Act, etc.), leading to varied national implementations and interpretations. Crucially, the disparate resources and competence levels of national market surveillance authorities create a postcode lottery for manufacturers, resulting in inconsistent oversight depending on their Member State. This uneven enforcement undermines the CRA's goals, and necessitates harmonisation.

Proposed simplification: Addressing the current disparities in CRA market surveillance demands a harmonised approach. Firstly, joint interpretative guidelines and standardised implementation frameworks are crucial to minimise national divergences across the CRA and its overlapping digital legislation. Secondly, the EU must facilitate necessary resource and competence building initiatives, potentially through a central EU body or coordinated national efforts. This includes dedicated funding, cross-border training programmes, or the establishment of common technical toolkits. Thirdly, regular peer reviews for national surveillance outcomes would ensure consistent enforcement and prevent regulatory arbitrage, ultimately creating a truly level playing field for CRA market surveillance across the EU. Finally, The lead market surveillance authority, which acts as the central coordination point for regulatory enquiries, should be designated based on the location of a manufacturer's main establishment in the EU.

Reporting obligations

Status quo: Currently, reporting obligations vary across legal acts. This results in unnecessary regulatory burden for entities effected.

Proposed simplification: To avoid duplicate reporting processes, the reporting requirements under CRA, NIS-2, DORA and GDPR should be fully harmonised. Consequently, German industry welcomes the European Commission's proposal to set up a SEP under NIS 2, DORA, CER and eIDAS as it will significantly reduce the bureaucratic burden emanating from reporting obligations. We support the "report once, share many" principle. Incident reporting through a SEP can facilitate the establishment of a daily situational incident report, which would help private entities and public institutions to counter

cyber-attacks and thereby enhance Europe's resilience. However, an even more ambitious approach, which also integrates the CRA and which harmonises reporting obligations themselves, is necessary.

To improve efficiency, the reporting procedure should be streamlined to two steps: an initial report within 72 hours with the essential information and a comprehensive report within 14 days after the corrective action. All reports should be submitted only once at EU-level, ideally via the ENISA platform, to avoid parallel processes. In addition, we advocate making the simplified documentation requirements for SMEs applicable to all manufacturers.

Quantum Act

General Remarks

BDI welcomes the initiative of the European Commission to develop the EU Quantum Act as an initiative, facilitating the implementation of the Quantum Strategy of the EU. BDI welcomes the suggested focus on research and innovation, industrialisation and supply chain resilience, and supports the focal role played by industrialisation activities.

The EU Quantum Act should not lead to increased bureaucratic burdens but rather focus on increasing unification of the legislation and coordinating efforts among Member States. Such coordination is especially important when developing and updating the roadmaps, envisaged by the Quantum Europe Strategy. The roadmaps should be coordinated with the national efforts in this area (e. g., for the case of Germany – with the Hightech Agenda).

The EU Quantum Act should cover the full range of quantum technologies, including quantum computing, quantum communication and quantum sensing. The further development and expansion of EuroHPC JU and EuroQCI should be supported. However, speed is of utmost importance in order to gain on competitiveness with respect to other regions. The rapidly expanding quantum ecosystem requires efficient coordination to prevent processes from slowing down. Furthermore, it is important to fund algorithms, software and applications as well as the quantum hardware. Prioritising the development of European open-source software frameworks, standardised APIs and interoperability will allow wide ecosystem participation in technology development and implementation.

The Quantum Act should take a technology open approach, given that it is unclear which specific technology will dominate the market, particularly in the case of the quantum computing hardware. At the same time, funding should be targeted at areas where the chances of success are particularly high. This enables existing resources to be utilised effectively. Industrial applicability should always be a central criterion in order to avoid diversifying the funds too widely. Benchmarking should be established for technology comparison, and a system of KPIs should be developed, for example including the number of industrial pilot projects related to quantum technology, the transfer rate of research into industrial applications or scaling targets for quantum hardware and software.

Research & innovation framework

The Quantum Act must address the clear gap between research and industry application. It is important to consolidate the research strengths in the application-oriented technology hubs (Quantum Competence Clusters planned to be expanded by the Quantum Europe Strategy). These clusters should aim to integrate science, start-ups and industry more closely. It is also important that these clusters are connected to facilitate collaboration. To ensure continuous and cost-efficient progress, it is essential that the clusters are institutionally anchored within existing national and European ecosystems (e. g. the European Quantum Industry Consortium – QuIC or Quantum Technology & Application Consortium

– QUTAC). Existing bilateral and multilateral collaborations (e. g. the Franco-German dialogue on quantum technologies and the trilateral collaboration between France, Germany, and the Netherlands) should be continued and developed further.

As suggested by the Quantum Europe Strategy, EU-wide testbeds should be introduced, with specific focus on commercialisation activities – for example, for robust qubit systems, scalable quantum communication networks, or portable, high-precision quantum sensor systems.

The number of quantum-related patent applications in Europe has grown significantly in the last years, with a recent QuIC white paper reporting the growth of 33 per cent in 2024 compared to 2023[1]. Nevertheless, Europe's patent statistics still lag behind those of the USA and China. Thus, simplified IP regulations appropriate for quantum technology should be developed. While traditional IP instruments such as patents are well established, particularly in the hardware sector, software-dominated fields may require other concepts, such as copyrights and trade secrets. When establishing the guidelines for IP transfer, the expertise and best practices of industry, industry associations, and research institutions should be utilised.

Industrial capacity & investment (Made in the EU)

As the commercial market for quantum technologies remains limited, establishing use cases to demonstrate quantum advantage is essential. In this regard, the rapid development of the six planned quantum pilot lines through the Chips Joint Undertaking is crucial. Here, industrial players have to be the key contributors as otherwise the industrialization cannot be timely achieved.

To further support the development of use cases, it is important to recognise the role of the government as anchor customer. It is therefore necessary to identify the government's specific needs (e. g. in the areas of mobility, cryptography and security) at an early stage, and to address these needs in a targeted manner with the relevant innovation stakeholders. In this case, aligning with the policy documents of specific European countries (e. g. Germany's Hightech Agenda) is essential.

To exploit synergies between quantum technologies and manufacturing, cross-technology platforms must be established. In addition, flagship projects in key sectors such as chemicals, health, logistics, finance and industrial manufacturing should be established to promote low-threshold access to infrastructure and advance the targeted application of quantum technologies.

Supply-chain resilience & governance

As set out in the Quantum Europe Strategy, inclusive governance at the EU level is essential to foster the development of the technology. It is important that the dedicated expert group and the high-level advisory board, both of which are acting in line with the strategy, coordinate their efforts with the national bodies.

To ensure European sovereignty, it is important to secure key positions in the supply chain. Further investment in the development of enabling technologies is crucial in order to take on strategically relevant leadership positions. Critical technologies that are crucial to securing the resilience of value chains (e. g. quantum chips, cryogenics, lasers and photonic components) must be systematically identified and addressed.

Considering the dual use of many quantum technologies, including quantum communication, sensor technology, and encryption, an early EU-wide legal framework is needed that includes guidance on export controls and model procedures for international pilot projects. This will help to increase planning security and avoid unnecessarily slowing down research.

Digital Fairness Act

With regard to the announced Digital Fairness Act it is paramount to avoid the creation of an additional layer of regulation that creates unnecessary overlaps and complexities. In line with its commitment to simplification and better regulation, the Commission should focus its efforts on improving and enforcing the existing consumer acquis and only propose new regulation, when there is a genuine legislative gap. We see no need for new legislative measures to deal with dark patterns or addictive design, as the existing legal consumer framework already adequately covers misleading or aggressive practices towards consumers online. In particular, the UCP Directive already offers comprehensive protection with its clauses on unfair practices in Articles 5-9 and its blacklist in Annex 1. In the past, it has proven to be sufficiently flexible and technology-neutral to be applied also to new (digital) markets and practices. In addition, other legislative frameworks, such as the Digital Services Act, the Digital Markets Act, the AI Act, the GDPR and the Consumer Rights Directive also contain provisions to protect consumers from misleading practices online. If there is empirical evidence to show that the applicable law does not adequately cover a particular misleading practice, then the legal framework should be expanded as minimally as possible, for example by amending Annex 1 of the UCP Directive, rather than by proposing additional new legislation.

Imprint

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

EU Transparency Register: 1771817758-48

German Lobbyregister: R000534

Editors
Dr Michael Dose
Senior Expert Data Economy and Data Protection
Directorate Innovation, Security and Technology
T: +49 30 2028-1560
m.dose@bdi.eu

Mariia Halada
Expert DeepTech and Quantum Technology
Directorate Innovation, Security and Technology
T: +49 30 2028-1623
m.halada@bdi.eu

Steven Heckler
Senior Expert Cybersecurity and eGovernment
Directorate Innovation, Security and Technology
T: +49 30 2028-1523
s.heckler@bdi.eu

Polina Khubbeeva
Senior Expert Artificial Intelligence and Microelectronics
Directorate Innovation, Security and Technology
T: +49 30 2028-1586
p.khubbeeva@bdi.eu

Nadine Rossmann
Senior Representative
Law and Tax
T: +32 2792-1005
n.rossmann@bdi.eu

Document number: D 2241