BDI

INNONATION

POSITION | DIGITAL POLICY | DATA & CYBERSECURITY

Omnibus for the digital acquis

The Data Act, GDPR and NIS 2 Directive must be less bureaucratic and more innovation-friendly to enhance Europe's competitiveness.

23 February 2026

Executive Summary

The European Commission's proposal for the Digital Omnibus is not the team bus we had hoped for, but neither is it the small car we feared. We welcome the Digital Omnibus and the European Commission's intention to streamline and simplify the digital rulebook. However, the proposals currently on the table do not deliver the relief and clarity that industry hoped for. While the European Commission's proposal for the Data Omnibus partly simplifies and reduces the bureaucracy of the EU's digital acquis, crucial structural reforms needed to genuinely strengthen the EU's competitiveness remain unaddressed. As it stands, the streamlining exercise appears to create more uncertainty than it removes.

To have a holistic simplification package, the European Commission should have simultaneously presented its proposals for simplification of rules for digital infrastructure with the Digital Networks Act and for cybersecurity with the Cyber Security Act 2 (CSA2). Furthermore, the proposal of the Digital Omnibus should have also addressed all relevant shortcomings and withdraw certain provisions of the Cyber Resilience Act (CRA), because in their current version they negatively affect the competitiveness of European companies on global markets. The European Parliament and the Council must not fall short of the European Commission's proposal and rather seize the opportunity created by the Commission's proposals to ensure that Europe remains competitive in the global innovation race. Innovation in Europe must no longer be held back by overly bureaucratic and burdensome rules that hinder our digital competitiveness. We urge for swift negotiations with close stakeholder involvement.

German industry's policy recommendations

It's important that the EU places competitiveness at the centre of its agenda. And the issuance of the Digital Omnibus as such shows that the European Commission recognises the necessity to cut unnecessary complexity, simplify regulatory requirements, and enhance coherence across the EU's digital rulebook to achieve this aim. While the EU Commission's current proposal for the Digital Omnibus tries to strike a good balance between targeted regulatory interventions and increasing regulatory clarity, German industry believes that 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 maintain global competitiveness. Even worse, certain regulatory provisions or formulations continue to fundamentally erode the principles of fair competition by mandating disclosure of essential competitive elements, including trade secrets, through legally imposed transparency obligations. In addition, stronger measures are required to ensure meaningful simplification and to safeguard the interests of European technology leaders.

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

Therefore, German industry proposes the following changes to the draft Data Omnibus:

Data Act

We support the Commission's approach to adjust the legal text at an early stage after Regulation 2023/2854 came into force. Although the changes proposed by the European Commission address some important aspects, the proposed changes however, still miss industrial needs or do not address them at all.

The proposals unfortunately fall short of creating clarity and coherency both within the Data Act, e.g. further protection of trade secrets, clarifications regarding Chapter VI, re-use of data for data holder and regarding its interplay with further legislation such as the GDPR. 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.

GDPR and ePrivacy

BDI supports the Commission's basic approach of specifically addressing problems in the practical applicability of the GDPR or in areas that seriously inhibit innovation, rather than opening up the entire GDPR. The proposal addresses many points that have also been identified by the business community as requiring reform, e.g. the clarification of personal data-definition as it enables a clearer picture of what anonymization of personal data entails or the abuse of data subjects' rights. This benefits both companies of all sizes as well as potential data subjects, without lowering the level of protection provided by the GDPR.

Unfortunately, serious problems that continue to have a significant impact on the innovative capacity of European companies have not been adequately resolved and must be addressed urgently in the further legislative process – in particular clarifications in Article 9 (1) of the GDPR and regarding the ePrivacy exemptions.

Single-Entry Point for Incident Reporting (SEP)

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.

Cyber Resilience Act

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 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.

Table of Content

Data Act

Article 1 – Amendments to Regulation (EU) 2023/2854

Article 2: Data Holder-Definiton

The definition of the term "data holder" is only marginally adjusted. Instead of "using and providing data", it should read "using or providing data". This is disappointing, and the amendment does not bring any clarity to the term whatsoever and thus does not help in evaluating under what circumstances an enterprise becomes a data holder. The definition is still circular and differs from the definition the EU Commission refers to in their FAQ document. It needs to be amended to reflect the Commission's view that data holder is who controls access to the data as the FAQ is no legally binding document. Companies need legal certainty to implement the Data Act successfully.

Article 4 (8)/ Article 5 (11): Trade-Secret Handbrake

Trade secrets are one of the most valuable strategic assets of companies to remain competitive. BDI welcomes the effort of the EU Commission to adress the insufficient trade secret protection measures, however, the extension of the protection of trade secrets as an ex-ante exception to cases where there is no adequate level of protection in third countries is no new development, as the enforcement of rights in third countries as objective reason to deny data sharing requests is already included in the current Data Act. Nevertheless, the provisions are in general still insufficient to ensure robust trade secret protection as the requirements for trade secret owners to prove imminent economic damage remain too high as the following points remain unchanged: Art. 4 (8)/ Art. 5 (11) are inadequate as they lack practical effectiveness and the refusal threshold (serious economic harm) is unrealistically high. Once disclosed, trade secrets are irreversibly lost, eliminating competitive advantage of EU based companies. Disclosure potentially causes severe economic harm and allows third parties to exploit proprietary knowledge, which undermines innovation, and poses global enforcement risks. Strong protection is therefore essential to safeguard investments and preserve Europe's competitiveness.

The requirement for trade secret owners to demonstrate a high likelihood of serious economic damage from disclosure or a high risk of unlawful disclosure etc. to a third country remains overly burdensome. We, therefore, strongly reiterate our request to exempt data that is itself a trade secret or from which a trade secret can be derived from any data sharing obligations to keep the competitive advantage of EU based companies. The current proposal is unacceptable and leads to competitive disadvantages of European companies. Forcing companies to share their trade secrets as the current wording still foresees, undermines the very purpose of the EU Regulations to keep European companies competitive against non-European companies.

It should be made clear that mandatory data sharing under the Data Act must not be construed as conferring trade secret ownership on the user. Even where such data access is made subject to the agreement of appropriate technical and organisational measures pursuant to Article 4(6) and Article 5(9), the user's entitlement to data access does not create any status as a holder or co-holder of trade secrets within the meaning of Directive (EU) 2016/943, nor should it be treated as doing so. It must therefore be expressly stated that the data holder is and remains the sole holder of the trade secrets concerned, and that the user's access to data neither establishes nor alters this legal position.

If Trade Secrets are not exempted from the scope of the Data Act, there should be made at least the following amendments:

Recital 31 shall be amended as follows:

In this context, data holders should be able to require users, or third parties of a user's choice, to preserve the confidentiality of data considered to be trade secrets. *The user shall not be considered a co-holder of the relevant trade secrets.*

Art. 4 (8) shall be worded as follows:

A data holder who is a trade secret holder may refuse, on a case-by-case basis, a user's request for access to data identified as trade secrets where the disclosure of such data would reasonably be expected to result in the loss of confidentiality, loss of control, loss of its commercial value, or any risk of inference or other forms of indirect acquisition of trade secrets.

The data holder's assessment shall be deemed sufficient where it is based on elements, including, but not limited to:

- *the sensitivity, structure, granularity and level of confidentiality of the data requested;*
- *the extent to which the data, alone or combined with other information accessible to the user, would allow inference of trade secrets, business logic, algorithms or processes;*
- *the foreseeable risk of misappropriation in aftermarket or competitive contexts.*

The refusal shall be communicated in writing to the user without undue delay. The competent authority pursuant to Article 37 shall be notified accordingly.

Art. 4 (8a) (NEW) Additional Safeguards for Data Disclosure to Third Country Entities

Where the data recipient is established in a third country, or is under the direct or indirect control of an entity established in a third country, the data holder may refuse access where there exist reasonable concerns that the applicable legal or enforcement framework does not provide effective, reliable and enforceable protection against the misappropriation or loss of confidentiality of trade secrets compared to the protection provided under Union law.

Such concerns shall be deemed reasonable where the data holder demonstrates objective elements such as:

- *the lack of effective judicial or administrative remedies against misappropriation;*
- *structural weakness in enforcement, oversight, or compliance obligations;*
- *the legal, political, or practical environment which may facilitate compelled disclosure, interception, or state access;*
- *the absence of binding agreements ensuring equal or higher levels of protection compared to those und Union law.*

Any refusal pursuant to this paragraph shall be communicated to the user in writing without undue delay. The competent authority pursuant to Article 37 shall be notified accordingly.

Art. 5 (11) shall be worded as follows:

A data holder who is a trade secret holder may refuse, on a case-by-case basis, a third party's request for access to data identified as trade secrets where the disclosure of such data would reasonably be expected to result in the loss of confidentiality, loss of its commercial value, loss of control, or any risk of inference or other forms of indirect acquisition of trade secrets.

The data holder's assessment shall be deemed sufficient where it is based on elements, including, but not limited to:

- *the sensitivity, structure, granularity and level of confidentiality of the data requested;*
- *the extent to which the data, alone or combined with other information accessible to the user, would allow inference of trade secrets, business logic, algorithms or processes;*
- *the foreseeable risk of misappropriation in aftermarket or competitive contexts.*

The refusal shall be communicated in writing to the user without undue delay. The competent authority pursuant to Article 37 shall be notified accordingly.

Art. 5 (11a) (NEW) Additional Safeguards for Data Disclosure to Third Country Entities

Where the data recipient is established in a third country, or is under the direct or indirect control of an entity established in a third country, the data holder may refuse access where there exist reasonable concerns that the applicable legal or enforcement framework does not provide effective, reliable and enforceable protection against the misappropriation or loss of confidentiality of trade secrets compared to the protection provided under Union law.

Such concerns shall be deemed reasonable where the data holder demonstrates objective elements such as:

- *the lack of effective judicial or administrative remedies against misappropriation;*
- *structural weakness in enforcement, oversight, or compliance obligations;*
- *the legal, political, or practical environment which may facilitate compelled disclosure, interception, or state access;*
- *the absence of binding agreements ensuring equal or higher levels of protection compared to those und Union law.*

Any refusal pursuant to this paragraph shall be communicated to the user in writing without undue delay. The competent authority pursuant to Article 37 shall be notified accordingly.

Article 14, 15, 15a, 20 – B2G Data Sharing

BDI welcomes that the B2G-data sharing obligations should be limited to public emergencies. At the same time, further clarification of key definitions are needed, in particular: the specific definition and scope of the term "public emergency", the duration and termination of such access powers and legal protection following the consolidation of the complaint mechanisms in Art. 22a.

Article 31 – Switching between data processing services

It is important to note that the prevailing legal view holds that existing contracts are not subject to changes in the law. As such, the proposed amendments might be seen as superfluous. A true step forward in terms of legal certainty and innovation-friendly regulation would be a fundamental exemption of PaaS and SaaS from the scope of Chapter VI for all companies, regardless of their size and to extent the exemptions in Articles 31 (1a and 1b) for contracts signed on or after 12 September 2025.

In general, BDI supports the idea to exempt “custom-made” services and “data processing services that are not off-the-shelf” for contracts signed before 12 September 2025 (“Legacy Contracts” in order to take account of the special features of certain data processing services. Custom-made services, such as SaaS and PaaS, require time-intensive preparatory work by customers, lengthy negotiations as well as interactions between customers and suppliers, and subsequent technical customization, making rapid provisioning impossible. The EU Commission rightly reconfirms that Chapter VI applies only to data processing services, where the digital service itself, incl. SaaS, can be rapidly provisioned or released with minimal management effort/service provider interaction (see FAQ 58a). However, in contrary to the Commission’s proposal, this exemption should also apply to digital services based on contracts signed on or after 12 Sept 2025 and for all companies, regardless their size.

However, the EU Commissions proposal raises some fundamental questions and leave out relevant aspects:

It is unclear what exactly is meant by " where the majority of features and functionalities of the data processing service have been adapted." In the accompanying Staff-Working Document, it is stated: *"As opposed to off-the-shelf solutions, contracts on the provision of these custom-made services are usually the outcome of dedicated negotiations."* However, the definitions of “off-the-shelf” vs. “custom-made” are also absent.

To avoid uncertainties, we propose the following wording:

Art. 2 (8) (Definitions) shall be worded as follows:

“~~“~~data processing service” means a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralized, distributed or highly distributed nature ~~that~~ if and insofar the digital service itself is elastic, can be rapidly provisioned and released with minimal management effort or service provider interaction. Digital services provided in a SaaS delivery model shall only be considered as Data Processing Services if the main purpose of such service is the provision of access to computing resources other than those used to enable access to and use of the application.”

Art. 31 (1a) and (1b) shall be worded as follows:

(1a) Without prejudice to Article 2 (8) specifying all other characteristics of a data processing service, T~~t~~he obligations laid down in Chapter VI, ~~with the exception of Article 29, and in Article 34~~ shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer~~, if the provision of such services is based on a contract concluded before or on 12 September 2025~~.

~~The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry, if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.~~

(1b) A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).

~~Where the provider of data Processing services is a small and medium-sized enterprise or a small mid-cap, t~~ The obligations laid down in Chapter VI, ~~with the exception of Article 29, and in Article 34~~ shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.

~~Where the provider of data Processing services is a small and medium-sized enterprise or a small mid-cap, t~~ The provider shall not be required to renegotiate or amend a contract for the provision of a data processing service ~~other than those referred to in Article 30 (1)~~ before its expiry if that contract was concluded before or on 12 September 2025. ~~Any contractual provision contained in that contract that is contrary to Article 29 (1), (2), or (3) shall be considered null and void.~~

New Art. 31 (1c) to be included:

"1c. Chapter VI shall not apply in cases where the contract is not provided by the data processing service provider, but (i) by the customer, e.g. in the context of a public tender, or (ii) is negotiated by the parties."

Article 25 (1) – Contractual terms regarding switching

It should be clarified that Chapter VI does not apply in cases where the contract is not provided by the data processing service provider, but (i) by the customer, e.g. in a public tender, or (ii) is negotiated individually by the parties.

Article 42 – Role of the European Data Innovation Board

BDI generally supports the improved role of the European Data Innovation Board (EDIB) as foreseen by the proposal for the EDIB.

Chapter VII a – Data Intermediation Services and Data Altruism Organisations

It remains questionable whether the proposed compulsory notification regime for data intermediation services will have the desired effect of increasing attractiveness of data intermediation services.

Chapter VII c – Re-use of data and documents held by public sector bodies

BDI supports including concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests as part of consideration of the principle "open by default" intended for the availability of research data.

Additional Amendments necessary / What's Missing?

Article 2 – Definitions

Key definitions of the legal text should be specified, such as the definition of "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. 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) 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.

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. 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.

Furthermore, 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.

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.

Article 3 – Amendments to Regulation (EU) 2016/679

Article 4 – Scope of personal data

German industry supports clarifying the definition of personal data as proposed and the shift towards realistic identifiability and actual risk rather than hypothetical re-identification possibilities, which in principle takes up the definition as in the CJEU Case C-413/23 P. Nevertheless, further practical clarification on pseudonymisation and anonymisation would increase legal certainty. To make this work in practice, the proposal should clarify the relationship between controllers and processors. Where data are not personal from the recipient's perspective, there should be no need to enter into a processing agreement under Article 28 GDPR. Sector- or context-specific standards and optional certifiable approaches could help organisations determine data status reliably. It should also be clear that effectively anonymised data fall definitively outside the GDPR's scope and that anonymisation should not be treated as a standalone, continuously regulated processing operation.

While the proposed amendment is welcomed, it should also explicitly state that the assessment of whether the entity has reasonable means available to identify the data subject applies even in the case of data sharing within the same corporate group

Article 9 (2) (k) and (5) – Processing related to Artificial Intelligence

Enabling Artificial Intelligence (AI) to be trained and operated using special categories of personal data as well, is an important step to foster the development of AI in the EU, as it creates more legal certainty surrounding the use of such data. It provides for an easier use of biometrics for verification and clarifies permissible handling of inadvertently included sensitive data in AI pipelines, provided strong technical/ organizational controls are in place. Thus, risks in AI developments are reduced. However, the proposed addition of a possibility to process such data to develop or operate an AI system specifically is contrary to the principle of technological neutrality as well as the risk-based principle. The principle of technological neutrality principle, created to prevent a risk of circumvention of the GDPR (see Recital 15), also enables current and future technological innovation to be developed and operated in a GDPR-compliant manner. Instead of restricting the proposed Article 9 (2) (k) to AI systems the clear benefits of a technologically neutral GDPR should be upheld by enabling the use of such data e.g. for data-intensive and data-dependent technologies that offer clear benefits for society as a whole. Otherwise, there is a risk that comparable data-intensive technologies will be treated unequally in the future.

In addition, the implications of Article 9(5) GDPR-E require urgent clarification. It remains unclear what is meant by the requirement to take measures ensuring that the data is not used to generate output. Furthermore, the prohibition on disclosure to third parties could create significant practical challenges, for example when data needs to be shared within a corporate group or with cooperation partners. To avoid legal uncertainty and ensure workable solutions for legitimate data sharing, the legislator should provide clear guidance and explicitly address these scenarios.

Instead of avoidance and broad removal duties, Article 9(5) should be anchored in a risk-based approach aligned with Article 89 GDPR. What matters is reducing real risks through appropriate technical and organisational measures, not formalised "absence" of certain categories. Data removal duties should be reactive rather than proactive, and the output-filter requirement should be deleted.

Article 5 – Purpose limitation and the research privilege

BDI supports the proposed further processing for archiving in the public interest, scientific or historical research, and statistical purposes by removing the need for a separate compatibility test under Article 6(4) GDPR. This will materially reduce administrative burden and facilitate data-intensive research and development. For effectiveness, "research" should be interpreted in a technology-neutral and actor-neutral way, covering modern data-driven industrial and digital research, including preparatory and accompanying data-science activities.

It should also be clear that the privilege is not limited to fully anonymised data. Privacy-compliant use of pseudonymised data must be covered where appropriate safeguards under Article 89(1) are in place, often the only way to work with meaningful and valid datasets.

In addition, Article 5(1)(b) GDPR should explicitly recognise anonymisation, pseudonymisation and product improvement as purposes that are inherently compatible. Anonymisation and pseudonymisation do not represent a "new purpose" disconnected from the original collection; they are risk-mitigation measures aimed at ending or reducing identifiability.

Article 12 (5) – Handling of requests for Information

German industry welcomes the replacement of Article 12 (5) which enables companies to handle manifestly unfounded or excessive requests for information.

The new regulation creates more legal certainty in dealing with abusive, tactical, or high-frequency data subject requests, particularly access requests, such as those occurring in employment disputes, serial access requests, or automated mass submissions. By explicitly allowing consideration of improper use of the right of access as an indicator of abuse in Article 15 requests, a common practical case is addressed—for instance, when access requests are used as leverage or a tactical instrument. The option to charge a fee simultaneously acts as a deterrent against structural abuse.

The legislator's willingness to counter improper use of the right of access is expressly welcome. At the same time, this regulation could prove ineffective in practice if data subjects are not required to state the purpose of their request, making proof of misuse nearly impossible. It is essential that the draft provides for an alleviation of the burden of proof for controllers when requests are demonstrably aimed at purposes outside the scope of data protection.

To enable consistent application, the Commission or EDPB should clarify what is meant by "other purposes" and provide practical guidance, such as through examples or guidelines. It would also be worth considering that data subjects could, at least optionally or upon request, provide information about the purpose of their access request under Article 15, to enable fair assessment of abuse cases and give controllers a practicable documentation basis.

In practice it will be necessary to monitor the impact of the proposed limitation of the right of access, noting that inappropriate use may be very difficult to demonstrate in practice, which would render the proposed changes ineffective. To ensure consistent application, the Commission or EDPB should further specify the terms “manifestly unfounded” and “excessive,” for example through examples or criteria catalogs.

Article 13 (4) and (5) – Information requirements

German industry welcomes the proposed limitation of information obligations as these exemptions can materially reduce transparency burdens, particularly for SMEs, organisations with straightforward customer relationships and research institutions.

In order for this simplification and burden reduction for companies to be effective, the carve-back in Article 13(4) should be revised as it risks emptying the simplification of practical effect. To avoid undermining the intended reduction in burden, the carve-back should be deleted. In particular, the exemption should not be excluded merely because data are shared with processors under Article 28 GDPR or transferred to third countries on the basis of an adequacy decision (Article 45 GDPR) or appropriate safeguards (Article 46 GDPR). This matters for everyday low-risk situations, for example a craft business sending invoices by post, or a company using a hosting or IT provider to operate its website or email services. In such cases there is typically a clear relationship, and additional information about these standard steps adds little value for individuals.

Article 22 – Automated decision making

German industry appreciates the efforts made to clarify the conditions under which automated decision-making is permissible. The proposal is a step towards greater legal certainty for data-driven business models and the use of AI-supported decision-making. However, further clarification is needed to ensure that Article 22 adequately reflects technological developments in the field of automated decision-making, in particular the growing capabilities of AI systems to assess facts correctly and accurately. It is incompatible with technological progress to prohibit the automated filtering out of clearly unsuitable applicants in a recruitment process - for example, when a company is seeking an electrician and a doctor or lawyer without the relevant additional qualifications applies. Such preliminary and clearly rule-based exclusions should not be regarded as decisions with legal or similarly significant effects within the meaning of Article 22 GDPR.

German industry therefore supports a clarification that solely automated decisions may be permissible under the existing exceptions of Article 22(2) GDPR, in particular where they are necessary for entering into or performing a contract. The notion of “necessity” should be interpreted in a functional and practical manner and should not be excluded merely because a non-automated alternative would theoretically be possible.

In this context, “necessity” under Article 22(2)(a) GDPR should not be confined to the formal conclusion or narrow performance of a contract but should also cover pre-contractual decision-making processes and functionally involved third parties acting with a view to a potential contractual relationship.

To ensure coherence with the regulatory framework for artificial intelligence, compliance with the due diligence and risk management obligations under the AI Act should be recognised as a relevant factor when assessing the permissibility of automated decision-making under Article 22(2) GDPR. This would support a balanced interpretation of existing exceptions without introducing additional legal grounds.

It should also be clarified that preparatory, supporting or purely technical automated processing – including automated scoring or assessments provided by third parties, does not in itself constitute a

solely automated decision within the meaning of Article 22, where the final decision is not determined in a decisive and binding manner by such processing.

To further improve legal certainty, Article 22 should define when a decision is “legal” or “similarly significantly” affecting. The scope should be limited to decisions that decisively and durably determine a person’s legal status, contractual rights, or access to essential services. It should also be clarified that “necessity” under Article 22(2)(a) is not confined to contract conclusion or narrow contract performance, but can cover pre-contractual decision processes and functionally involved third parties aimed at a potential contractual relationship. Explanations in the recitals could support consistent and practice-oriented application.

Article 33 – Notification of a personal data breach to the supervisory authority

German industry welcomes the introduction of a SEP pursuant to several EU directives and regulations. It is a very sensible step to enable entities to report data breaches and significant cybersecurity incidents through the same reporting mechanism since cybersecurity incidents often also lead to data breaches. It would achieve a substantial reduction in low-risk breach notifications, improved harmonization and administrative efficiency. To ensure effective standardization. Art. 4 of the ePrivacy Directive should be repealed, as well as Regulation 611/2013 EU, which is currently missing in the Digital Omnibus.

For practical usability, “high risk to the rights and freedoms of natural persons” must be defined clearly, narrowly and predictably. Otherwise, organisations will continue to notify minor or obviously low-impact incidents defensively. It should be explicit that incidents without meaningful harm potential, such as inadvertent disclosure of publicly available or purely business contact details, do not amount to “high risk” under Article 33 GDPR. EU-wide consistency in applying this concept is key. It would also provide significant relief for companies if not every data protection incident had to be documented in minute detail, as Article 33(5) GDPR currently requires. This comprehensive documentation obligation is the biggest driver of effort in handling incidents.

Article 35 and 70 (1) (ha) -(hc)

German industry welcomes the proposed amendments, obligating the Board to prepare a List for processing operations which do, and which don’t require a Data Protection Impact Assessment (DPIA), as well as requiring the board to provide a template as well as a common methodology on how to conduct a DPIA. This guidance provides companies with more clarity and additionally will create a harmonized approach across the EU.

Article 41 a – Anonymisation and Pseudonymisation

German industry welcomes the proposal to enable the commission to adopt implementing acts to specify means and criteria as to when pseudonymised data may be considered anonymised for other entities thereby rendering the GDPR inapplicable for the entities processing such data. The implementing acts should be devised in a timely manner, as the use of anonymised data is an instrument of great significance to the industry that is able to adequately balance the interests between data use and data protection. Additionally, further Digital Acts have also built on the use of anonymised data (e.g. Article 18 (4) Data Act), thus providing a further reason to adopt implementing acts soon, to not create further legal uncertainty. To create effectiveness, “state of the art” must explicitly include modern privacy-enhancing technologies (PETs). Tools such as differential privacy, homomorphic encryption and synthetic data are central to enabling data-driven innovation and AI development while maintaining high data protection standards. The criteria should remain technology-neutral, flexible and future-proof, reflecting the evolving capabilities of re-identification techniques.

We support the proposal to clarify the definition of personal data so that information is *only* personal data for a given controller if that controller can reasonably identify the individual. This principle of relative identifiability aligns with recent CJEU case law and ensures that data a company which has truly no link to a person (e.g. properly anonymized or pseudonymised data with no realistic re-identification means) is not subject to GDPR obligations. We stress the importance of firmly adopting this approach – and providing clear criteria (per the new Article 41a empowerment) – so that controllers and regulators have a common understanding of "reasonably likely to be used" identification methods. Emphasizing relative identifiability will focus compliance on real privacy risks and relieve excessive burdens on data-driven innovation (for example, freeing up anonymized datasets for AI development or research that pose no threat to individuals' privacy).

Article 88a – Processing of personal data in the terminal equipment of natural persons

The EU Commission's proposal includes a reform of the ePrivacy rules in the GDPR, which is generally welcomed as it creates a uniform legal basis and harmonises transparency obligations. However, we believe that the proposed addition of Article 88a does not yet adequately address the shortcomings surrounding Cookies.

At first, a standardization within a browser could risk browsers becoming gatekeepers. Continuing to require consent with only very few exceptions, would uphold a significant barrier to innovation. While providing comparatively little protection of fundamental rights of the data subject, large amounts of data are lost which could otherwise be used to develop the terminal equipment concerned. The consideration of all equivalent legal bases under Article 6(1)(a) to (f) GDPR is disregarded and, as a consequence, all downstream data processing based on Article 6(1)(f) GDPR excluded. This could result in the German industry losing a significant share - sometimes up to 80% – of relevant data needed for the development of innovative systems.

The current focus on cookies is therefore too narrow and ignores the challenges of connected products. Instead of genuine legal harmonization, a two-tier regime for cookies threatens to emerge. The use of personal and non-personal data, balanced against the legitimate interests of the processor, must be enabled. As proposed by the EU Commission, Article 88a GDPR will apply as far as personal data is involved, while Article 5(3) ePrivacy Directive continues to apply to non-personal data. This split creates unnecessary complexity, as companies must assess for each device access whether data is personal — a distinction often difficult to draw with pseudonymous identifiers or telemetry data.

This different treatment of personal and non-personal data results in a considerable systematic contradiction. The exception provision in Article 88a(2) and its opening clause lack sufficient clarity. The dual-track regime and the opening clause for member state law can create significant differences between regulations for personal and non-personal cookies.

The exceptions in Article 88a(3)(c)-(d) for internal audience measurement and service security apply exclusively to personal data cookies. Non-personal data remains subject to Article 5(3) ePrivacy Directive's narrower "strictly necessary" exception. This creates a paradox: less intrusive technologies—such as anonymous telemetry from industrial PCs — face stricter requirements than the processing of personal data. This contradiction is systematically incomprehensible and problematic, especially in industrial contexts where anonymous telemetry and diagnostic data are indispensable. Either Article 88a exceptions should extend to non-personal data, or Article 5(3) should be modernized accordingly. The use of personal and non-personal data must be made possible, taking into account the legitimate interests of the processor. Instead of a primacy of consent, Article 5(3) ePD should incorporate a risk-based approach and the use of all legal bases of the GDPR. Only in this way can practical solutions be created that enable innovation while ensuring data protection.

Article 88a(5) requires respecting user decisions for six months. After cookie rejection, no consent banner should appear for at least 6 months. This creates a paradox: implementing rejection requires storing that decision — typically via a cookie. Questions arise whether this falls under Article 88a(3) or paragraph 2's opening clause. Additionally, decisions are stored device-dependently, while the legal wording requires person-specific decisions — raising practical implementation questions. Additionally, the envisaged six-month blocking period for a new request for consent following a refusal is too long and should be reduced to three months in order to meet practical requirements. The rule that a new request is not permitted if consent has already been given is also impractical. Particularly in the case of dynamic websites with frequently changing providers, it must be possible to easily obtain new consent for these partners. There is no explicit regulation on how to deal with the addition or removal of providers.

In addition, Article 88a GDPR equates the term “end user” (ePrivacy) with the term “data subject” (GDPR), which leads to discrimination against B2B constellations, because in many cases it is not possible to obtain consent, in cases where consent from the owner or authorised representative of the end device would no longer be sufficient.[1] B2B practice must be observed in such a way that consent given by the authorised representative is effective. This has been considered in the German Telecommunications Digital Services Data Protection Act (TDDDG), for example, as the “end user” can be both natural and legal persons and consent must be given by the person who has integrity expectations of the end device. Overall, the use of digital services ordered by a business must not depend on the consent of individual natural persons.

Furthermore, according to the EU Commission’s proposal, the exemption for digital services ordered by companies would also be abolished, as these would be commissioned by the companies and not by individuals.

Finally, the proposed cybersecurity exemption is too narrow, as even the remediation of recognised vulnerabilities would still require consent – even though the measures are essential e.g. for road safety. The legal exceptions for the detection, remediation and prevention of security vulnerabilities, including OTA updates, must be expanded. The same applies to exceptions for processing aggregated usage data (e.g. data required for product quality, predictive maintenance and fleet operation).

Article 88b – Automated and machine-readable indications of data subject’s choices with respect to processing of personal data in the terminal equipment of natural persons

The proposed concept in Art. 88b is unconvincing both legally and practically and misses its stated objective. The introduction of machine-readable signals in accordance with Art. 88b GDPR poses risks and ambiguities in practice. For example, it is to be feared that browser providers will implement negative default settings, which would lead to falling consent rates. It also remains unclear whether the technical standards enable granular consent for individual processing purposes or only provide for an ‘all-or-nothing’ decision, which would restrict users' freedom of choice. Furthermore, the scope of application is not clear: does the regulation only refer to access to end devices or also to downstream data processing? The proposed exemption for media providers is also problematic, as its broad definition could undermine the standardisation objectives. Finally, there is no regulation for the

[1] See recital 44, according to which the rules apply regardless of ownership of the terminal equipment (‘... whether the terminal equipment is owned by the natural person or by another legal or natural person’).

implementation of the standards in mobile apps, as the obligation is primarily aimed at web browser manufacturers.

On this background, BDI recommends deleting Article 88b and focusing legislative efforts on a clear, risk-based and GDPR-compliant Article 88a. European internet. At least, Article 88b (5) should be extended to also include a date as to when standards – as mentioned in Article 88b (4) – should be available.

Article 88c – Processing in the context of the development and operation of AI

German Industry welcomes the proposal to enable the development and operation of AI systems or AI models based on legitimate interest within the meaning of Article 6 (1) (f). This constitutes an important clarification that the development and operation of data-driven systems with significant social and economic value are, in principle, legitimate activities, provided they are carried out responsibly and subject to appropriate safeguards. To achieve its intended purpose, Article 88c must function as a reliable and EU-wide uniform legal basis. Ambiguous wordings such as “where appropriate” and broad openings for national consent requirements risk divergent interpretations and undermine the GDPR’s harmonisation objective. In particular, allowing national laws to effectively override Article 88c by imposing consent, beyond cases where Union or sector-specific law explicitly and narrowly requires consent, would run counter to the GDPR’s structure and CJEU case law (including ASNEF), would re-fragment the internal market and would significantly reduce the provision’s practical value. Article 88c should therefore operate as a self-standing, directly applicable legal basis that cannot be hollowed out by national special rules.

Article 88c should also not be viewed as a narrow technology-specific exception, but as an expression of a broader principle: data-driven systems with significant societal value require a clear, risk-based legal framework. New data-intensive technologies beyond today’s AI systems will emerge; an overly narrow focus on “AI systems under the AI Act” risks pushing future innovations back into legal grey zones. A technology-neutral interpretation and development of Article 88c would therefore be preferable, covering data-driven development, modelling and automation processes more generally, where pursued for legitimate purposes and subject to appropriate safeguards.

Additional Amendments necessary / What’s Missing?

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

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.

ePrivacy

Necessary provisions contained in the ePrivacy Directive should be moved to the GDPR, while the ePrivacy Directive itself should be repealed fully.

Article 3 – Amendments to and Directive 2002/58/EC (ePrivacy Directive)

Art. 5 (3)

The approach taken in the published proposal still requires, with very few and completely inadequate exceptions, the consent of users when accessing data in a terminal device. This also includes modern vehicles, for example. E.g. the automotive industry has clearly stated that this will result in the loss of 60 to 80 percent of relevant data for the development of safety-related and/or autonomous driving systems. This offers no advantages for the protection of the fundamental rights of those affected. Instead, it severely restricts the innovative capacity of these core technologies, which offer considerable benefits for society. Furthermore, this leads to the contradictory and objectively unjustifiable situation that the processing of non-personal data stored in the terminal equipment is potentially subject to stricter rules than the processing of personal data. Such fragmentation of the legal framework creates legal uncertainty and is difficult to implement in practice.

Furthermore, the current provision appears to have been designed primarily for single-user devices and is therefore not suitable for multi-user environments such as connected vehicles. Article 5(3) ePD and its national implementation in § 25 TDDDG currently refer to the “end user” or “user” as the person required to express the explicit wish, whereas the GDPR draft now refers to the “data subject.” This shift could have significant implications in multi-user contexts: while today the owner or primary user of a connected vehicle can make key settings – sometimes with effect for other users – the new approach might require consent from every secondary user as a “data subject.” In fleet scenarios, this raises fundamental questions regarding the extent of decision-making authority for fleet owners and whether existing user concepts would need to be redesigned. The wording indicates a tightening of the legal framework compared to the status quo, likely because the provisions were drafted with cookies in mind, without adequately considering their application to connected vehicles.

Urgent improvements are needed here, to ensure that the reform does not lead to a blockade of security-relevant data or data relevant for the development of innovative systems. To this end Article 5(3) ePD should incorporate a risk-based approach and the use of all legal bases of the GDPR instead of a primacy of consent.

Single-Entry Point for Incident Reporting (SEP)

Recitals

Recital 49

Since reporting obligations are a significant bureaucratic burden for companies, we appreciate that the SEP will allow entities to fulfil reporting obligations under Directive (EU) 2022/2555, Regulation (EU) 2016/679, Regulation (EU) 2022/2554, Regulation (EU) 910/2014 and Directive (EU) 2022/2557 by submitting notifications to a single interface. We also support the idea that the SEP will allow entities to retrieve information previously submitted through the SEP. However, this is not the significant breakthrough hoped for in simplifying cybersecurity regulations and reducing bureaucracy:

1. **Exclusion of the EU CRA:** The CRA is not covered by the planned new regulation. The urgently needed amendments in this regard are not being addressed by the Commission. The Single Reporting Platform under the CRA (SRP) and the SEP must be merged.

2. **Unclear Interplay between Reporting Mechanisms:** It remains unclear how the different reporting mechanisms under NIS2, DORA, GDPR and CRA interact with each other and how the SEP will interact with the single reporting platform to be established under Article 16 CRA for notifications of actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements. It must be clarified what is meant by "the single-entry point builds on the single reporting platform established under that Regulation" as stated in the new Article 23a(1) of the NIS2.

3. **Vagueness of Implementation of the SEP:** The amendments to NIS2, GDPR, eIDAS, DORA, and CER are purely technical in nature. How the SEP will be concretely designed remains vague.

4. **Lack of Harmonisation and the need for standardisation of reporting formats**: The Digital Omnibus establishes a technical routing mechanism rather than delivering true harmonisation or standardisation of the reporting process. The type of information required, reporting formats, and accepted languages still vary across legal frameworks and, in the case of NIS2, according to applicable Member State law. As a result, reporting under one regime will often not fulfil obligations under another, e.g. between the CRA and NIS2, or even between different NIS2 national transpositions, where Member States may request different levels or categories of information. This lack of harmonisation 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. To fully realise the potential of the SEP, the Digital Omnibus should harmonise reporting requirements across legal regimes and, in addition, standardise both the type of information and the reporting format. This standardisation should apply both between different national NIS2 implementations and across legal regimes such as NIS2 and the CRA.

5. **Lack of Immediate Bureaucratic Relief and Timing Issues:**

   - In light of the current economic downturn, companies require a speedy reduction of bureaucratic obligations, which is absent from the current proposal. Apart from streamlining the reporting channel, streamlining of reporting timelines across regulatory acts is paramount to reduce the overall bureaucratic burden.

   - Reporting obligations under the CRA apply from September 11, 2026, meaning the single reporting platform (Art. 16 CRA) must be established by this date. If the SEP can only be used 18 months at the earliest after the new regulation enters into force, this is too late. Chaos is then pre-programmed: Will reports under the CRA initially have to be made via the single reporting platform (Art. 16 CRA) and then (partially, i.e., only for certain significant incidents) also or only via the SEP? How should the industry handle multiple reporting channels/tools if the SEP is technically unavailable or not available on time?

   - What about the reporting of actively exploited vulnerabilities under the CRA? Are these to be reported via the single reporting platform (Art. 16 CRA)? Why not also via the SEP?

- Reporting obligations under the other legal acts to be amended (GDPR, eIDAS, DORA, NIS2, and CER) are largely already in effect. How is it ensured that the SEP is compatible with existing tools (interoperability)? What about the continuity and stability of existing reporting channels? Will there be secure interfaces for reporting companies? What about user-friendly, concise reporting templates?

While the SEP can in principle support a reduction in administrative burden, the proposal does not harmonise the reporting obligations themselves. The obligations therefore remain inconsistent across the different acts and entities continue to face divergent timelines, thresholds, formats, and procedural requirements. A single-entry point that leaves these discrepancies unchanged risks creating an additional procedural step instead of reducing complexity. Since work on the CRA reporting platform is still at an early stage, any approach to a single-entry point must consider the requirements, timelines and technical architecture of this future system to avoid duplication and to ensure practical usability for reporting entities.

To maximise efficiency and oversight, the SEP should automatically route incident notifications to all relevant authorities – such as national CSIRTs, market-surveillance authorities and other competent bodies. This would prevent parallel investigations, reduce inconsistent queries and help Member States coordinate responses and identify cross-sectoral trends. A centralised EU-level platform will accelerate information sharing and support a coherent understanding of emerging cybersecurity risks.

Recital 50

Since entities will submit highly sensitive information through the SEP, it is paramount that ENISA takes appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the SEP and the information submitted or disseminated via the SEP.

Recital 53

German industry welcomes the Commission's recognition that ENISA should consult the Commission, the CSIRTs Network, and competent authorities when developing the technical specifications for the SEP but emphasises that structured engagement with private sector stakeholders must also be embedded throughout the SEP's development and maintenance. To ensure regulatory coherence and practical utility, ENISA should establish a regular consultation mechanism – such as a stakeholder forum or expert group – with opportunities for industry feedback via public consultations, written input, and technical workshops, following a transparent model like the CRA Expert Group process. Direct engagement with private-sector entities is crucial, as their technical expertise and operational insight are essential for designing interoperable, secure, and user-friendly reporting mechanisms. Such collaboration will strengthen shared responsibility for cybersecurity, foster innovation, and help anticipate and mitigate unintended compliance burden.

Recital 55

It is of utmost importance that the SEP accommodates the possibility to report incident-specific information at a certain stage to ensure that all reporting can be conducted through the SEP. Thereby, it would be ensured that no additional system must be operated at national level.

In addition, German industry emphasises that the SEP should be designed to facilitate rapid and comprehensive information sharing with all relevant competent authorities. By allowing providers to submit a single notification automatically routed to CSIRTs, national market-surveillance authorities, and other relevant authorities, the SEP would prevent multiple parallel investigations and reduce inconsistent or uninformed queries. A centralised EU-level platform would provide clear efficiency and oversight benefits: national CSIRTs could easily identify cross-sectoral trends, detect cross-border risks, and coordinate responses. It would eliminate the need for Member States to manually reconcile overlapping

legislative requirements and accelerate information sharing across cyber and product-safety regulators.

All reporting points should always be able to communicate in English to be able to exchange important information with security experts and companies from all EU countries quickly, directly, and without misunderstandings.

Article 6: Amendments to Directive (EU) 2022/2555

Article 23a: Single-Entry Point for Incident Reporting

German industry welcomes the European Commission's proposal to set up a SEP at EU level as it will significantly reduce the bureaucratic burden emanating from reporting obligations and will facilitate the establishment of a daily situational incident report. Especially for companies operating in more than one EU Member State, having one entry point for all incident reporting will allow to streamline internal processes. The SEP should also make it possible to report a single incident only once it should trigger reporting obligations under multiple legal acts. However, companies can only reap the full benefits of the SEP if incident reporting is possible in English, i.e. that entities do not have to report in various EU languages.

To fully realise the simplification goals of the Digital Omnibus, it is essential that the SEP is accompanied by harmonised definitions, formats, timelines, reporting templates and thresholds across EU frameworks. Only with clear, uniform criteria can the SEP reduce administrative burden and legal uncertainty. We therefore recommend that ENISA conducts a comprehensive review of overlaps and inconsistencies in current EU reporting requirements, with the aim of developing harmonised templates, aligned procedures, and interoperable technical standards for the SEP. This approach would create a coherent, streamlined, and operationally efficient incident reporting system, ultimately easing compliance for all stakeholders.

Building on this, German industry considers it crucial that the technical implementation of the SEP is not only user-friendly and accessible, but also fully integrated with existing EU-level reporting platforms to avoid fragmentation and maximise efficiency. Hence, the SEP, as set out in Article 23a, should be intertwined with the existing CRA Single-Reporting Platform (SRP) to ensure a unified EU reporting system. While Article 4(1) of the Omnibus proposal allows ENISA to use the CRA single-reporting platform, there is a risk of parallel infrastructures and fragmented governance if the CRA SRP and the SEP evolve independently and are not fully interoperable. German industry recommends the development of a secure and efficient mechanism within the SEP to facilitate follow-up communications, allowing authorities to share information, reduce redundant requests, and improve regulatory coordination.

According to Article 23a (2) and (3 b) all relevant competent authorities will have access to reported information. While we very much appreciate this step in general, the European Commission must ensure that competent authorities only receive access to reported information based on the need-to-know principle.

Article 23a (3 d) foresees an interoperability of the SEP with the European Business Wallet (EBW). This is an essential step as it provides a very concrete use case for the EUBW. Since only very specific persons within a company have the necessary qualifications to report a cybersecurity incident, it is of utmost importance that the EBW provides for a power of attorney and the delegation of authorisations. The delegation of authorisations and the establishment of proxy authorisations is a central function of the EBW, as many different employees within a company act on behalf of a company. This enables certain employees to act on behalf of the organisation based on the rights assigned to them. The EU

must ensure that the EBW provides for the delegation of authorisations within the framework of a comprehensive management of permissions and user roles. Therefore, the EBW's user management system must allow multiple members of the organisation to receive, store and present these credentials when required.

The provision that entities can retrieve and supplement information previously submitted via the SEP (cf. Article 23a (3 e)) is very important as companies will receive more information about an incident while handling it. Not having to fill in information from scratch several times, will increase the efficiency of the reporting process.

According to Article 23a (3 f) a single notification of information submitted by an entity via the SEP can be used to fulfil reporting obligations as set under any of the other legal acts providing for incident reporting to the SEP. As a cybersecurity incident can also lead to data breaches under the GDPR or might constitute a hybrid threat with interlinkages to the Critical Entities Resilience Directive, having to report an incident only once is a very important feature.

German industry appreciates that Article 23a (4) requires ENISA to pilot incident notification through the SEP before roll-out. To ensure that the SEP is fit for purpose companies should be closely integrated in the process of developing and piloting the SEP.

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

(5) Within [18] months from the entry into force of this Regulation, ENISA shall pilot the functioning of the single-entry point for each added Union legal act, including testing that takes into account the specificities and requirements for the notifications set out by each respective Union legal act, and after consulting the Commission*, representatives from entities pursuant to Article 3 of Directive (EU) 2022/2555* and the relevant competent authorities under the respective Union legal acts. ENISA shall enable the notification of incidents under each Union legal act referred to in paragraph (1) only after piloting the functioning and after the Commission published a notice pursuant to paragraph 6. *ENISA must closely liaise with representatives from entities pursuant to Article 3 of Directive (EU) 2022/2555 to ensure that the single-entry point for incident reporting is interoperable with standard systems utilised by these entities.*

Ultimately, to ensure the SEP operates securely, reliably, and interoperability across Member States, it is essential that ENISA is adequately resourced for its expanded technical and operational responsibilities. Since the 2019 Cybersecurity Act, ENISA's mandate has grown significantly, now covering certification, operational cooperation, threat analysis, and oversight of new instruments. German industry therefore recommends that any additional responsibilities for ENISA in developing and managing the SEP be matched by increased budgetary and staffing levels. This will also be a key consideration in the upcoming revision of the Cybersecurity Act, which should reflect ENISA's broader role within the EU cybersecurity framework

Article 23 (1)

German industry appreciates that each Member State shall ensure that essential and important entities notify CSIRT or the competent authority of significant incidents by utilising the SEP. All Member States should be obliged to offer the utilisation of the SEP already 12 months after the entry into force of the Digital Omnibus Regulation to maximise the benefits emanating from the European Commission's simplification agenda and thereby to reduce the bureaucratic burden for companies.

Article 23 (12)

German industry welcomes that when a manufacturer notifies a severe incident pursuant to Article 14(3) of Regulation (EU) 2024/2847 and the incident reporting contains relevant information as required under paragraph Article 23 (4) of Directive (EU) 2022/2555 shall constitute reporting of information under the latter paragraph. Establishing the SEP pursuant to Article 23a as the one SEP will significantly reduce the bureaucratic burden emanating from incident reporting. Moreover, having one single-entry point for all incident reporting will also facilitate the establishment of a holistic situational security picture.

Article 30 (1)

To establish a holistic cyber threat situational picture, enabling entities to voluntarily report incidents through the SEP established pursuant to Article 23a is much appreciated.

Article 9: Amendments of CER

Article 15

In light of the increase in hybrid attacks as well as simultaneous digital and analogue attacks against the same entity, German industry appreciates that Member States must ensure that entities notify via the SEP established pursuant to Article 23a of Directive (EU) 2022/2555 the competent authorities of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. Having one entry point for both analogue, digital and hybrid attacks will facilitate the establishment of a holistic daily situational picture. Such a holistic daily situational picture has the potential to significantly augment Europe's resilience. However, this will only be the case if competent authorities jointly analyse the incident information available.

What's Missing?

… 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.

… 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) 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 product"s, 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, e.g. five or ten years 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.

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 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.

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. This approach aligns with the principle of proportionality, supports effective incident 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, a manufacturer becomes aware of an actively exploited vulnerability when it has sufficient and reliable information. Preliminary indications or unverified suspicions shall not constitute awareness.*

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. Finally, 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.

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

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

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

Florian Pühl (until December 2025)
Student Assistant in the Department Digitalisation and Innovation
T: +49 30 2028-1603
f.puehl@ifg.bdi.eu

Document number: D 2216