Digital Omnibus

Position Paper

bitkom

At a glance

Simplification for Europe's Digital Economy

The Digital Omnibus is a cornerstone of the EU's simplification agenda. Europe's digital economy has long awaited this proposal, as companies are increasingly constrained by a fragmented regulatory framework and excessive reporting obligations. In the area of data protection alone, 79 % of companies support reform at European level, and 71 % believe data protection rules must be adapted to the age of artificial intelligence (Bitkom, 2025). The need for change enjoys broad support and is becoming increasingly urgent.

Simplifying the digital rulebook has been a priority of this mandate well before recent geopolitical tensions over European digital legislation emerged with the current US administration. In her political guidelines of July 2024, Commission President Ursula von der Leyen explicitly called for legislation to be »simplified, consolidated and codified to eliminate overlaps and contradictions«.[1] This call was reinforced by the Draghi Report of September 2024, which concluded that the productivity gap between the EU and the United States is largely driven by the technology sector. Regulatory barriers were identified as a key factor limiting innovation, particularly for startups and scaleups, and contributing to the relocation of innovation outside Europe. Closing this innovation gap is crucial for Europe' economic strength.[2]

The conclusion is clear: simplifying Europe's digital rules is essential to sustaining European competitiveness. Competitiveness, in turn, underpins Europe's prosperity, strategic autonomy and way of life. If Europe fails to act, it risks becoming increasingly dependent on technologies developed outside the Union and shaped by non-European frameworks, according to values and standards not its own.

If Europe wants technology to be developed in line with European values, innovation must be enabled within Europe. This requires harmonised regulation, legal clarity and a meaningful reduction of unnecessary rules and administrative burdens. Without this, Europe will continue to fall behind in the global tech race.

Against this background, we welcome the European Commission's Digital Omnibus proposal as an important step in the right direction. However, it does not yet deliver the level of ambition required to reverse the current trend. While the proposed amendments are necessary, they remain cautious. We therefore call on the European Parliament and the Council to significantly strengthen the proposal during the legislative process and deliver tangible, measurable simplification. What Europe cannot afford is a diluted outcome that falls short of the ambition needed and results in only minimal change.

[1] European Commission, ↗ Political Guidelines for the Next European Commission 2024-2029, 2024.
[2] European Commission, ↗ The Future of European Competitiveness – A Competitiveness Strategy for Europe, 2024.

Key Priorities for the Forthcoming Negotiations:

- **Fast-Track »Stop-the-Clock« for High-Risk AI Obligations**
  To ensure adoption before the deadline, the timeline changes for the application of high-risk systems under Annexes I and III should be fast-tracked by separating them from the remaining provision of the AI Act Omnibus. Additionally, their application should be postponed by at least 24 months to allow for the development of high-quality standards and to provide sufficient time for effective implementation.

- **Integrate Horizontal AI Act Obligations into Sectoral Legislation**
  Horizontal AI Act obligations should be embedded into sectoral legislation, with Annex I operating as *lex specialis*. In parallel, the scope of Annex III should be clarified and narrowed to exclude low-risk and organisational uses, thereby avoiding the duplication and the over-classification of high-risk AI systems.

- **Beyond a Single Entry Point and Towards Harmonized Cyber Reporting Obligations**
  While the Single Entry Point (SEP) can in principle support a reduction in administrative burden in cybersecurity reporting, the proposal does not harmonise the reporting obligations themselves. The obligations remain inconsistent across the different acts. Instead, divergent timelines, thresholds, formats and procedural requirements need to be harmonized across different legal acts. These discrepancies risk creating an additional procedural step instead of reducing complexity.

- **Ensure Legal Certainty and Feasible Application of the Data Act**
  The Data Act must clearly exclude retroactive effects on existing contracts and ensure that obligations, particularly on cloud switching and data access, are technically feasible for complex B2B SaaS models. To provide legal clarity, the omnibus should introduce explicit non-retroactivity, clear scoping of obligations, and proportionate transition periods that are aligned with the availability of standards, to avoid forced re-engineering and investment uncertainty.

- **Provide Effective Protection of Trade Secrets without Underpinning Innovation**
  Strengthened protection mechanisms are welcome, but they require objective criteria, proportionate reporting obligations, and a coherent alignment with GDPR logic, especially for the use of non-personal data and public-sector data reuse. Without such clarifications, there is a risk of discouraging data-driven innovation and distorting competition to the detriment of Europe's competitiveness.

- **Embed a Truly Risk-Based and Innovation-Enabling GDPR Framework**
  Despite targeted improvements in the Digital Omnibus, documentation, accountability and transparency obligations still largely apply irrespective of actual risk. The omnibus should therefore be used to systematically differentiate obligations according to real risks for individuals, strengthen legitimate interests as a viable legal basis beyond isolated use cases, and introduce innovation-enabling legal openings. Only a genuinely risk-oriented GDPR can reduce unnecessary compliance burdens while safeguarding fundamental rights.

- **Establish a Coherent, Risk-Based Regime for Cookies and Device Access**
  A coherent, risk-based cookie and device-access regime should be established through the introduction of the new Article 88a GDPR. Device access should follow the GDPR's overall logic and allow reliance on all legal bases under Article 6 GDPR, in particular legitimate interests. Low-risk uses such as audience measurement, fraud

prevention or contextual advertising must be possible without a blanket consent requirement. This is essential to resolve the structural inconsistency between the GDPR and the ePrivacy framework, reduce consent fatigue in practice, and create a workable, innovation-friendly basis for digital business models.

- **Enable Data-Driven Innovation and AI Development with Legal Certainty**
  Article 88c GDPR is an important step towards providing a clear legal basis for processing personal data for the development and operation of AI systems, particularly through its recognition of legitimate interests as the central legal basis. To deliver in practice, however, Article 88c must apply uniformly across the EU and must not be undermined by national carve-outs or additional consent requirements. The provision should also be technology-neutral so that it remains fit for purpose as new data-intensive innovations emerge.

Inhalt

1 AI Act

Significant implementation challenges and unclear requirements threaten the AI Act's goal of mitigating AI-related risks while fostering AI innovation in Europe. This is clearly reflected in the fact that 93 % of German companies affected by the AI Act report that the effort required for its implementation is considered either rather high or very high.[3]

To realign the Act with its original intent, the European Commission published a proposal to simplify the AI Act. While the proposal introduces sensible measures to improve practical implementability and foster innovation, it still falls short on several relevant aspects.

Nonetheless, Bitkom explicitly welcomes several of the proposed simplification measures, including the reduction of the registration burden for AI systems used in high-risk areas where providers have concluded that such systems are not in fact high-risk, as they are deployed only for narrow or purely procedural tasks. We also welcome the removal of the mandatory Commission-issued template for post-market monitoring plans, which will instead be replaced by guidance. Furthermore, we support the introduction of an EU-level regulatory sandbox for AI systems under the Commission's exclusive supervision, alongside strengthened cross-border cooperation between national sandboxes. Other positive developments include the introduction of a new legal basis to facilitate real-world testing under Annex I, Section B (likely for autonomous vehicles) through Article 60a, as well as stronger enforcement powers for the Commission, including AI Office-centralised enforcement for AI systems based on GPAI models (GPAI systems) and AI services under the DSA (embedded in VLOPs, etc.).

The proposal provides further clarifications that are essential for consistent application of the AI Act. In particular, the proposal clarifies that if an AI system falls under Annex I and III, the conformity assessment procedure of Annex I is the one that supersedes. Furthermore, it clarifies that notification under any of the legislative acts listed in Annex I is sufficient to perform a conformity assessment of AI systems in the relevant area during the ramp-up phase. Notified bodies operating under those legislative acts should apply for designation under the AI Act within 18 months. Finally, the proposal clarifies that the applicability of the grandfathering provisions for high-risk systems depends on the model and type of the AI system rather than on individual units.

46%

of German companies call for reforms to the AI Act (According to a Bitkom Research survey)

[3] Bitkom Study, »KI in der deutschen Wirtschaft«, 2025.

Missing and insufficient regulatory implification measures

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

The Commission proposes to postpone the entry into application of the high-risk requirements. Specifically, for high-risk systems under Annex III (e.g. many applications in HR or critical infrastructure), the Commission suggests delaying its applicability by six months after all necessary standards or other compliant tools have been approved, with a maximum postponement of 16 months until December 2027. For high-risk systems under Annex I A (e.g. many AI systems in the medical device or machinery sectors), the proposal foresees a postponement of 12 months after approval of the relevant standards or tools, capped at a maximum delay until August 2028.

While this proposal represents an improvement in principle, the ordinary legislative procedure takes far too long to enable a timely decision on postponements, thereby significantly reducing the intended relief effect on planning security.

During the 2019-2024 European Parliament mandate, the average duration of the negotiations was 20 months.[4] In the case of the AI Act, the Commission presented its legislative proposal in April 2021, and the final adopted text was published in the official journal in July 2024 – a total of 39 months. AI providers and deployers only have about 7 months until key requirements start applying on 2 August 2026.

To ensure that the so-called »stop-the-clock« can be adopted before the deadline, it is **essential to fast-track the timeline changes by splitting them from the rest of the AI Act Omnibus**. This would much reduce the complexity of the text to analyse in priority, and allow to use faster adoption processes, such as the Parliament's »urgent procedure« rule 170.[5] In practice, this separate proposal would cover points 30 and 31 of the current AI Omnibus proposal, as well as corresponding recitals. The rest of the omnibus could then be discussed at a normal pace, as the timeline shift, once enacted, would allow for time to finalise the negotiations on other provisions.

Furthermore, the proposal is likewise not sufficient in substance. To implement the high-risk requirements organisations will need standards which act as practical recipes for compliance. With standards, AI providers and deployers would only need to follow set blueprints and checklists to help them operationalise the AI Act's provisions into their own processes, reducing uncertainty and compliance costs. Though voluntary, EU harmonised standards are preferred by most companies as they provide »presumption of conformity« to show compliance with corresponding legal requirements. These standards thus offer the safest and easiest compliance option for businesses and public

[4] European Parliament, »Handbook on the Ordinary Legislative Procedure«, March 2025, p. 11.
[5] European Parliament, »Rules of procedure«, Rule 170 : Urgent procedure, July 2025
↗ https://www.europarl.europa.eu/doceo/document/lastrules/RULE-170_EN.html.

bodies, especially smaller organisations which have limited legal and regulatory oversight resources (like startups or SMEs).

Organisations with experience in implementing digital regulations note that achieving compliance with a *single* standard often requires at least 12 months.[6] As the AI Act's high-risk requirements are expected to involve up to 35 (partially cross-referenced) standards, a significantly longer transition period will be necessary to guarantee effective and compliant adoption.

Having at most six months between the finalisation of standards or other compliance tools and the start of the requirements for Annex III systems will likely slow down product releases and reduce investment in these areas, ultimately hindering innovation and value creation. In addition, the complex dual timeline introduced that can now unilaterally be triggered by the EU Commission reduces planning certainty for companies, likewise reducing investments in the high-risk areas.

To ensure the development of high-quality standards and allow sufficient time for their implementation, **the AI Act Omnibus should extend the implementation timeline for the high-risk requirements under Annexes I and III by 24 months (fixed timeline instead of dual mechanism) and correspondingly delay the applicability of fines for non-compliance by 24 months.**

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

Early AI Act preparatory work is already showing the limits of applying horizontal AI rules to established sectoral frameworks, particularly those in Annex I, Section A. Drafting of harmonised AI standards is taking longer and proving more complex than expected, leaving manufacturers uncertain about how AI standards will align with existing sector-specific product standards. This uncertainty risks creating bottlenecks and disrupting established compliance pathways, especially for conformity assessments. The AI Act introduces obligations – some of which may conflict with sector-specific requirements – that many conformity assessment bodies are not authorised or prepared to handle under current sectoral regimes. In highly regulated sectors such as the machinery or radio equipment sector, where notified bodies are already under pressure, layering AI requirements without a clear integration pathway risk further delays and market disruption. Single applications and extra time will not fix structural problems.

The European Commission appears to acknowledge this issue, at least for the medical device and in vitro diagnostic sectors. In December, the Commission proposed moving regulations on medical devices (MDR) and in vitro diagnostic medical devices (IVDR) from Section A to Section B of Annex I in their simplification proposal for the MDR and IVDR.[7] We very much welcome this proposal. However, the inconsistencies, duplications, and dysfunctional interactions between sectoral regulations of Annex I A

[6] Kilian R, Jäck L, Ebel D. European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act. European Journal of Risk Regulation. 2025;16(3):1038-1062. doi:10.1017/err.2025.10032.

[7] ↗ European Commission, Proposal on the Revision of the MDR and IVDR (cf. Recital 23 on p. 26 and Art. 4 on p. 127).

and the AI Act are not limited to the MDR and IVDR. They affect all Annex I A regulations.

For these reasons, Annex I should be streamlined by merging its two sections and extending the more flexible Section B approach to the entire Annex. This would allow AI requirements to be integrated into sectoral frameworks, rather than applied directly and in parallel to sectoral rules. It would also enable harmonised AI standards to be translated into sector-specific contexts without undermining existing conformity procedures. Integration should follow a sequenced approach grounded in existing legislation: the goal is not to reopen well-functioning systems, but to align them with the AI Act while avoiding legal uncertainty.

To support this approach, the AI Omnibus should clearly state that Annex I legislation is lex specialis. But it should also confirm the AI Act as a maximum harmonisation instrument, ensuring that sector-specific measures (secondary legislation or technical specifications) do not add to, or expand beyond, AI Act requirements. This would prevent fragmentation and preserve a consistent, cross-sector understanding of the »state of the art« when integrating AI Act provisions into sectoral frameworks.

56%

of German companies see the AI Act as creating more disadvantages than advantages (According to a Bitkom survey)

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

No standards will be available for transparency rules set in the AI Act's Article 50. The Commission launched in the autumn 2025 a process to draft guidance for Article 50 and a code of practice to address obligations covering AI-generated content. Code and guidelines are not expected before May or June 2026, about a month before the entry into application date. To remedy this, the omnibus proposes an enforcement delay of 6 months (until 2 Feb. 2027), specifically for certain transparency obligations for legacy generative AI systems (paragraph 30 (a)), which would be placed on market before 2 August 2026. This concerns the AI Act's Article 50(2), requiring AI providers to mark AI-generated outputs so that their AI origin can be detected.

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

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

Certain provisions of Article 50 will not be addressed by the code, but only via guidelines, including provider and deployer information obligations to natural persons either interacting with the AI or exposed to it. As these guidelines are also only

expected just before the summer 2026, **the grace period should also cover AI providers and deployers in scope of Article 50(1)-(3), so that they have enough time to adapt their AI systems**.

Enshrine the legacy clause clarifications into the operative provisions

Recital 21 of the omnibus provides essential details regarding how the legacy clause set in Article 111(2) will apply in practice; for AI systems used by public authorities, it is a grace period until 2030. The recital clarifies that once placement on the market (or into service) has occurred for an individual AI system unit before the entry into application of high-risk requirements, other AI system units of the same type and model also benefit from the legacy clause, even if placed on the market after entry into application. If substantial modifications are carried out on the AI system, all future units, as well as the ones in operation, would have to be made compliant.

This clarification is essential as it recognises that the notion of »individual product unit« is not well suited to AI systems, i.e. standalone or embedded software distributed through complex supply and update channels. Additionally, certain categories of products with long development, certification and production cycles needed to have market placement considered at product-model or -type level, rather than for each individual unit.

For improved legal certainty, the clarifications brought by Recital 21 should be integrated into the operative provisions of the Act, meaning Article 111. There will be also a need to address potential frictions, for instance regarding NLF legislation of Annex I, which follows the Blue Guide logic of individual unit placement on the market.[8]

Moreover, the concept »substantial change«, which triggers recertification requirements under the AI Act, should be harmonized with the definition of »substantial modification« used elsewhere in the AI Act. This is necessary to prevent differing legal interpretations and to ensure that the concept of »substantial change / substantial modification« is used consistently throughout the AI Act.

Remove the Fundamental Rights Impact Assessment from the AI Act

Article 27 requires providers of high-risk AI systems to conduct fundamental rights impact assessments (FRIAs). These assessments evaluate how the AI system itself may impact individuals' fundamental rights, including human dignity, non-discrimination, and freedoms protected under the EU Charter. At the same time, Article 35 GDPR requires data protection impact assessments (DPIAs) to assess how the processing of personal data may affect individuals' rights and freedoms.

[8] European Commission, The Blue Guide on the implementation of EU product rules, June 2022, ↗ https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2022:247:FULL .

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

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

Align legal bases with the GDPR

The AI Omnibus proposes to insert a new Article 4a into the AI Act, to provide a legal basis for providers and deployers of AI systems and AI models to exceptionally process special categories of personal data for the purpose of ensuring bias detection and correction. While we support the intention, the resulting new article does not bring much more clarity than the original provisions set in Article 10(5), except from extending the scope beyond only high-risk AI providers, covering also high-risk deployers and both providers and deployers of other AI systems and models.

With the proposed targeted amendments to the GDPR brought by the Commission's proposal for a Digital Omnibus on data, privacy and cyber, adjustments are also being made to facilitate the processing of personal data for the development and operation of AI systems and models, under a new Article 88c. The resulting provisions differ compared to the AI Act: they are notably less restrictive, relying on the »legitimate interest« legal basis. In that context, alignment is needed between the proposed changes across AI Act and GDPR. **Ideally, a streamlined and unambiguous version of the new GDPR Article 88c proposal should be the baseline for improving and aligning the new AI Act Article 4a (for more details see page 41)**. Otherwise, companies and public bodies will refrain from using personal data to test and improve the function of their AI, with the risk of reducing the efficiency of bias detection and mitigation measures.

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

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

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

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

The competencies of the AI Office should be extended to include the resolution of inconsistencies between national supervisory authorities. Since AI deployment can

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

Avoid unnecessarily burdensome notification processes

We generally welcome the amendments to the notification procedure for conformity assessment bodies proposed in the draft, as they aim to avoid duplicate assessments and simplify procedures. However, they fall short of this objective and do not provide legal certainty for bodies already notified in specific sectors.

In particular, a clear regulation on scope extension is missing. While the draft formally provides for the possibility of a uniform application and assessment procedure (»single application« / »single assessment procedure«), it does not clearly establish that existing sector-specific notifications can merely be supplemented with an AI-related assessment (gap application with gap assessment). Rather, the wording suggests that even already notified bodies would have to submit a completely new notification application. This would counteract the intended simplification effect and jeopardise the timely deployment of notified bodies for high-risk AI systems.

We therefore recommend:

- Explicitly providing for the possibility of a clear scope extension in the form of a gap application with gap assessment for bodies already notified in specific sectors,
- deleting the provision regarding the availability of single application and single procedure in sectoral regulation, and
- abandoning technology-related partial notifications within the framework of the code system, i.e., deleting subsection 3 of Annex XIV Section 2 entirely.

Clarification and removal of specific application areas from Annex III

Review, clarification and removal of specific application areas from Annex III by actively using the procedures and under the conditions foreseen in Article 6(6) and (7) and Article 7 (3) AI Act. As a first step and prior to this, clarification in the respective COM guidelines that risk assessments in life and health insurance under Annex III(5)(c) without relevance to pricing or selection of policyholders are generally not considered high-risk.

Furthermore, we likewise see a need for clarification of Annex III 5(a). According to our interpretation, we see the risk that AI systems of a purely organizational nature in the healthcare sector may also fall under the high-risk definitions – for example, organising bed access for potential patients. The provision of Annex III No. 5(a) of the AI Act should clarify that organisational measures do not fall under this provision, since the potential hazard and the associated fundamental rights interference factually do not exist. Essentially, the word »grant« should be removed, and an addition should be

incorporated: »...excluding organizational services such as billing, inventory management, ...«. The change for Annex III 5 (a) should look as follows: »AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services, excluding the granting and organisational services such as billing and inventory management«.

2 Cybersecurity

289 billion euro in damages caused by cyberattacks on German companies within the past twelve months illustrate the magnitude of the challenge Europe must address. This development shows that a balanced and coherent regulatory environment is essential for strengthening resilience across the continent. Bitkom therefore welcomes the intention of the European Commission to optimise the existing framework. At the same time, the newly published proposal for the Digital Omnibus falls short of expectations with regard to cybersecurity.

A key feature of the Digital Omnibus proposal is the introduction of a Single-Entry Point (SEP) for incident reporting, to be developed and managed by ENISA. The SEP is designed as a unified access point for reporting obligations under NIS2, GDPR, DORA, eIDAS, and potentially the CER Directive. Bitkom views the SEP as a promising step toward streamlining reporting obligations across key EU cybersecurity and digital regulations. By allowing organizations to submit a single incident report that is automatically distributed to all relevant national authorities, the SEP can significantly streamline reporting processes. This approach minimizes confusion over which channels to use, ensures that vital information reaches the appropriate parties more quickly, and strengthens early warning capabilities. As a result, it enables timely corrective actions and enhances public confidence in the EU's cybersecurity framework. Importantly, we support Member States retaining full legal authority over incident response and enforcement and for the SEP to function solely as a technical intermediary, designed to simplify administrative processes and ensure that information reaches the relevant authorities efficiently.

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. The Digital Omnibus provides an opportunity to correct the current inconsistencies and to establish a coherent foundation for future work. Since the proposal does not resolve the challenges identified by industry, the positions and requests previously submitted by Bitkom in the Call for Evidence remain fully valid.

Missing and insufficient regulatory simplification measures

Common registration, reporting and uniform application

The fragmented nature of reporting obligations remains a central challenge in the European cybersecurity landscape. For companies it is often not clear, which regulations are in scope when reporting a particular security incident. Furthermore, the CRA, NIS2, DORA, AI Act and GDPR each impose separate incident notification procedures involving different authorities, reporting channels and requirements. A decision tree to classify the incident and decide on reporting requirements could be helpful during this stressful period. Currently, individual legal entities must register separately rather than being able to register centrally. For companies operating across several Member States and regulatory domains, this creates significant complexity and an additional operational burden. Under existing legislation entities are required to notify incidents separately to the competent authorities foreseen in each act. This includes notifications under NIS2 to national authorities or national CSIRTs, vulnerability reporting and incident reporting obligations under the CRA, reporting obligations for high-risk AI systems to national market surveillance authorities, breach notifications under the GDPR and additional obligations under DORA for the financial sector. These obligations often coincide in practice yet remain procedurally distinct.

Short deadlines continue to pose a particular strain. Both NIS2 and the CRA require initial notification within twenty-four hours of becoming aware of an incident. While rapid information flow is important in critical cases such deadlines can be impractical when information is still incomplete. Companies frequently need to prepare multiple preliminary reports which diverts resources from containment and analysis. When an incident affects several domains such as data protection, financial systems and product security, organisations must navigate parallel processes which increases duplication and the risk of inconsistent submissions without corresponding security benefits. This burden is further amplified in cross-border or federal contexts, where companies may face follow-up questions from more than twenty different national or regional competent authorities, often issued independently and sometimes in different languages. Responding to these uncoordinated, authority-specific inquiries under tight time pressure significantly increases administrative overhead and the likelihood of misunderstandings, again without a clear added value for incident response or overall security.

As outlined above, the Digital Omnibus proposes a SEP to enable entities to meet reporting obligations under NIS2, GDPR, DORA, eIDAS and CER through a single submission. ENISA should develop the SEP with due regard to the CRA platform for actively exploited vulnerabilities and severe incidents. This structural improvement responds to a longstanding request from industry and can reduce administrative burden.

However, the proposal does not help companies determine which regulations are in scope when reporting a particular type of security incident, to whom, what level of detail and leaves the underlying reporting obligations unchanged. Definitions,

thresholds, timelines, formats, competent authorities and enforcement practices remain the responsibility of the respective legal acts. For example, both NIS2 and the CRA require initial notification within 24 hours of becoming aware of an incident, under the AI Act, very severe or widespread incidents must be reported within 48 hours, and the GDPR requires notification within 72 hours. Divergent requirements across acts and Member States therefore persist and continue to complicate operational compliance. Without further alignment the SEP cannot resolve these inconsistencies and companies will still need to map different criteria and timelines within one tool. Hence, for the SEP to effectively fulfil its goal of reducing administrative burden and legal uncertainty, it must be accompanied by uniform standards across EU frameworks and aligned with international best practices.

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 centralized EU-level platform will accelerate information sharing and support a coherent understanding of emerging cybersecurity risks. Moreover, to ensure a unified EU-level reporting architecture, the SEP should also cover incidents notified under the CRA. The Digital Omnibus proposal allows ENISA to align the CRA Single Reporting Platform (SRP) with the SEP, but risks remain if both platforms evolve separately. Bitkom recommends ensuring that the CRA SRP fully serves the SEP's functions, enabling secure and interoperable, incident reporting across frameworks. For this purpose, reporting in English should always be possible across the EU alongside national languages. This would significantly simplify communication, enable international forwarding, and reduce the risk of misunderstandings, especially in high-stress situations during severe incidents. Additionally, a mechanism for coordinated follow-up communications should be established to support information sharing and regulatory consistency, easing compliance for stakeholders. Against this background further harmonisation remains essential. Alignment of definitions, thresholds, timelines, reportable items and templates across the relevant legal acts would considerably improve legal certainty and reduce operational complexity. Clarification on cross border cases and safeguards that ensure a single report suffices for incidents that affect several Member States would also help avoid duplicate sanctions. Authentication solutions such as the European Digital Identity Wallet could support secure access to the single-entry point, provided interoperability and usability are ensured. On a more general note, in addition to the harmonization of reporting obligations, it would be beneficial for the purpose of the (proposed) regulations, if companies could obtain government support in the security incident analysing and triaging process – to better understand the root cause of the incident and the potential impact to nation states. Upon these results, security subject matters experts could be provisioned to help further investigate the cause of the incident, minimize the impact and support (digital) recovery.

Cybersecurity Act

The CSA adopted in 2019, was designed as a central instrument to strengthen the security of information and communication technologies. At the time, no other EU-wide product-related cybersecurity requirements existed. Since then, however,

the regulatory environment has grown more complex. With NIS-2, DORA, the CRA, the delegated Radio Equipment Directive (RED), and the AI Act multiple overlapping regulations have emerged. National regulations, schemes and gold-plating create further complexity. Instead of providing clarity, the CSA risks becoming another element of fragmentation. To remain effective, the CSA must evolve into an umbrella regulation that brings coherence to this patchwork. It should provide a framework for enforcement and certification, aligning sectoral and horizontal initiatives. Existing risk management systems like ISO/IEC 31000 should be considered as a general base and for the integration of several risk management systems. ENISA, as the EU's cybersecurity agency, should be given a stronger mandate to promote coherence and support implementation through practical tools.

Consequently, to ensure ENISA can effectively manage the SEP and its expanded responsibilities, any new tasks should be matched by increased budget and staffing. Without additional resources, ENISA's ability to deliver on its mandate – including certification, operational cooperation and oversight of new instruments – will remain constrained. This should be addressed in the upcoming CSA revision, which will consider ENISA's remit and resources within the EU cybersecurity framework. To ensure practical utility and regulatory coherence, ENISA should also regularly consult private-sector stakeholders when developing and maintaining the SEP. A structured mechanism – such as a stakeholder forum or expert group – with public consultations and technical workshops will help design secure, interoperable and user-friendly reporting systems and anticipate compliance challenges. To limit regulatory complexity, the CSA should establish a clear delineation between vertical and horizontal requirements. Systems and components whose suppliers can demonstrate compliance with robust sector specific regulation and certification schemes should not be subject to additional horizontal obligations. Horizontal rules should apply only where no equivalent vertical framework exists. This approach would prevent duplicate requirements, reduce administrative burdens and ensure that regulatory efforts focus on areas where gaps remain.

Bitkom recommends that ENISA conduct a comprehensive mapping of overlaps and inconsistencies across EU cybersecurity regulations. This analysis should rely on internationally recognised standards and propose concrete measures for simplification. Mapping EU requirements against established standards would help both authorities and businesses, following a risk-based approach, highlighting gaps and clarifying the relationship between EU rules and international frameworks. Well-established standards such as ISO/IEC 27001 should serve as the foundation for demonstrating compliance wherever possible.

Ultimately, ENISA should lead the development of a harmonised cross-sectoral reporting framework under the CSA. Today, reporting obligations are dispersed across NIS2, CRA, DORA, GDPR, DA, and AI Act each with its own thresholds, timelines and channels. A centralised reporting portal, grounded in harmonised standards and coordinated by ENISA, would substantially enhance legal clarity and strengthen Europe's collective ability to respond to threats. To succeed, such a framework must ensure interoperability, align definitions and standardised procedures, while avoiding redundant obligations and duplicate sanctions. For instance, there is considerable potential for harmonization when it comes to CE marking requirements. These should be aligned across regulatory frameworks, with a single technical file format recognized

across frameworks and clear Commission guidance to ensure uniformity across Member States. By assuming a coordinating role, ENISA can ensure that the CSA becomes the foundation for coherence and effectiveness rather than an additional layer of complexity.

Network and Information Security Directive 2

The transposition and application of NIS-2 across EU member states lacks uniformity in timelines, scope and requirements, creating legal uncertainty and additional burdens for companies. Thirteen member states have not yet implemented the regulation. Inconsistent approaches are evident in several areas:

- Some member states, such as Hungary, have applied NIS-2 early, while many others have delayed or not yet transposed it.
- The treatment of minor activities, such as small-scale solar energy production, employee charging points or non-hazardous chemicals, varies significantly.
- Authorities like NUKIB in the Czech Republic consider recitals non-binding if not explicitly included, disregarding Recital 114 and thereby risking double registration for groups of undertakings.
- NIS-2 does not clarify which evidence or certification must be provided by Important and Essential Entities, while some member states introduce additional schemes, such as Germany's C5, complicating EU-wide compliance.

As Member States may also add further national requirements, companies operating cross-border face substantial monitoring and compliance overheads. This situation can only be addressed through the full harmonisation and uniform application of scope, timelines, obligations and requirements across the EU, alongside uniform guidelines that recognise overlap with other regulations.

Requirements for affiliated companies under NIS-2 should be simplified. If a company provides services listed in Annex I, point 8, Digital Infrastructure, in accordance with EU Implementing Regulation 2024/2690 exclusively within the group, these internal services should be assessed differently. Such intra-group services should be exempt from the requirements of the Regulation as they do not generate external risk exposure.

NIS-2 also tightens requirements for incident reporting. Article 23 obliges all essential and important entities to notify incidents with significant implications for their services. The intent is clear: to provide national authorities with the data needed to build a comprehensive and timely cybersecurity situation picture. Yet this only works if the reported information is analysed, shared and systematically integrated by authorities.

At present, NIS-2 imposes a five-step reporting regime. Companies must submit an initial notification within 24 hours, followed by a second report within 72 hours. Upon request, interim updates may be required during incident handling. A final report is due one month after the first notification. If the incident remains unresolved, a progress report must be filed, with a final report submitted one month after resolution. This system creates heavy administrative burdens. Meeting the 24-hour

deadline is difficult when reliable information is scarce. Divergences between Member States exacerbate the challenge, with some requiring broader reporting than others or applying varying cross-border criteria. Companies must therefore implement country-specific procedures, increasing compliance risks and pulling resources away from incident management.

A streamlined approach is needed. Instead of five steps, reporting should be limited to three. First, companies should issue an early warning within 48 hours of detecting a significant incident, limited to basic information such as company name and visible effects. Second, upon request, an intermediary report may be provided. Third, a final report should be delivered no later than one month after resolution.

This simplified model would maintain timely situational awareness for authorities while reducing burdens on companies, ensuring resources remain focused on mitigation and recovery rather than excessive reporting.

Cyber Resilience Act

Although the CRA may not be a central focus of the Commission's omnibus package, it cannot be treated as secondary. Its provisions are closely linked to CSA, NIS-2, GDPR, the AI Act and DORA, and its full enforcement in December 2027 will significantly reshape compliance requirements across Europe. While the CRA has the potential to strengthen cybersecurity in digital products, it also creates uncertainty and imposes considerable administrative burdens on manufacturers.

With horizontal regulations such as CSA, CRA and NIS-2, the cybersecurity regulatory landscape has expanded considerably. In addition, vertical, sector-specific regulations – such as RED (EU) 2014/53, (EU) 2018/1139 and (EU) 2019/2144 – already regulate cybersecurity and certification of specific systems and components. To avoid unnecessary duplication, the complexity of cybersecurity-related regulation and certification should be kept to a minimum. Where suppliers can demonstrate compliance with applicable vertical requirements, including technical specifications, cybersecurity measures and relevant standards, their products should not be subject to overlapping horizontal regulations. Small enterprises and start-ups require particular consideration, as the CRA does not differentiate obligations based on company size, unlike the NIS-2 Directive. Given limited personnel and financial resources, regulatory requirements should therefore be proportionate and streamlined to reduce administrative burden. Where such simplifications are introduced, they should be designed in a way that can also be leveraged by larger companies, without undermining the overall level of cybersecurity.

The downstream measures and harmonised standards required to operationalise the CRA remain delayed, leaving manufacturers with insufficient time for preparation. Current schedules are highly problematic:

- The type B standards for handling vulnerabilities are expected to be available to manufacturers by 30 August 2026, only days before the reporting obligations for actively exploited vulnerabilities and severe incidents take effect on 11 September 2026. Combined with obligations for legacy products dating back to the earliest digital elements, this creates disproportionate burdens for manufacturers.

A pragmatic solution would be to align the start of reporting obligations with the general applicability date of the CRA on 11 December 2027.

- Many other product-specific standards are to be published on 30 October 2026. This would leave approximately one year to implement the product-specific standards according to the corresponding deadlines, which is very tight.
- Further horizontal standards of type B regarding the CRA essential requirements have been announced for 30 October 2027, around 1.5 months before the CRA comes into general effect. This leaves manufacturers with little to no time to adapt their processes to the harmonised standards, which puts them at risk of high penalties.

The Commission should therefore consider reducing the number of harmonized European standards (hENs) and use existing standards from vertical, industry-related regulation. Realistic and technically feasible timelines for developing and delivering harmonised standards must be defined.

Article 14 of the CRA requires manufacturers to report actively exploited vulnerabilities through a designated platform in three stages: an early warning within 24 hours to both the CSIRT and ENISA, a detailed notification within 72 hours, and a final report within 14 days after corrective measures. This system duplicates existing frameworks and diverts resources from actual remediation. To improve efficiency, the reporting procedure should be streamlined to two steps: an initial notification within 72 hours with essential information and a comprehensive report within 14 days of corrective action. All notifications should be submitted only once through ENISA's platform, to eliminate parallel processes. Manufacturers are additionally confronted with overlapping and uncoordinated supervisory demands. Multiple Market Surveillance Authorities create a fragmented supervisory environment with uncoordinated requests. To streamline oversight, a lead authority should be designated based on the location of a manufacturer's main EU establishment, or another suitable basis if required, to act as a single point of coordination for regulatory inquiries. The EU should ensure a level playing field between the various national market surveillance authorities, which should be equally strict regardless of the manufacturer's main EU location.

The CRA introduces indefinite obligations for monitoring products and reporting vulnerabilities and incidents. Unlike vulnerability management obligations, which end at the close of the support period, monitoring and reporting requirements currently apply without limitation. Such perpetual obligations are disproportionate. Instead, monitoring and reporting should be limited to a defined period, for example three to five years after the end of the support period.

Another critical challenge for manufacturers is the CRA's treatment of »substantial modification«. Originating from the NLF, this concept is difficult to apply to digital products. Many software products, especially in the cybersecurity sector, must be updated several times a day or per week for cybersecurity reasons and, in case of doubt, each update may contain significant changes. According to CRA requirements, each update might require a new conformity assessment. Such an effort required for conformity assessments and declarations is unrealistic. This also goes for any technical documentation because this cannot be fully automated. We are aware that views exist in the Commission that the CRA will lead to a competitive edge. But current

implementation will weaken the EU software industry and may lead to an exodus of software development into other countries. European products will not be competitive any more in this case, due to cost advantages. Instead, the Commission should provide practical guidance, including thresholds and examples, to ensure legal certainty in determining substantial modifications. Furthermore, a shift away from the product concept and toward documentation of development processes instead is necessary. For example, it can be required that product documentation can be created at relatively short notice but does not have to be available immediately. For this purpose, an added module for the conformity assessment procedure for software is required. Module H is not usable for this purpose as of now, since »FAQs on the Cyber Resilience Act« would require continuous recertification due to constant significant changes, and it also does not consider the problems with documentation requirements. The module could take the form of an initial »baseline« conformity assessment confirming that the software currently meets the requirements, combined with an assessment of the development processes to ensure continued compliance throughout subsequent updates.

The scope of the CRA also extends to trivial products such as A/D converters or devices whose only »digital interface« is a USB charging port, for example electric toothbrushes. Although these products present virtually no cybersecurity risk, they are nevertheless subject to the full New Legislative Framework conformity assessment. As established in the Machinery Directive (»trivial machines«) and the EMC Directive (»inherently benign products«), a specific exemption for »inherently benign products« should be introduced in the CRA. This category would apply to products with digital elements that, due to their technical simplicity, cannot pose cybersecurity risks.

To further reduce complexity, it is necessary to align conformity assessments under the CRA and AI Act. Joint procedures and mutual recognition of assessments would help avoid duplication and foster consistency in implementation. This could be achieved by establishing a Joint Conformity Assessment Framework that integrates the requirements of CRA Modules B, C, and H (as outlined in Decision 768/2008/EC) with the AI Act's internal (Annex VI) and third-party assessments (Annex VII). Additionally, Conformity Assessment Bodies (CABs) with cross-competence should be authorized to assess compliance under both Acts, and mutual recognition agreements should codify that compliance with one framework (such as AI Act Annex VII) satisfies equivalent CRA obligations. Ideally instead of an ad hoc 3rd party assessment per regulation, companies would define compliance gaps and residual risks in their respective security controls framework. The regulatory required additional controls would then be added to the scope of their (mostly already existing) 3rd party independent/ objective assurance review. This would save considerable costs and efforts. We would welcome the possibility for ENISA to accredit 3rd party assurance providers.

3 Data Acquis

European data regulation has grown significantly in recent years, for example, through the Data Act (DA) and the Data Governance Act (DGA). In the context of the EU initiatives for a Data Omnibus legislative package, an EU digital package, and the roadmap for the Data Union Strategy, the question is not whether, but how and when the Data Act will need to be amended or at least clarified in key areas as a result of these initiatives.

Bitkom is open to this and is committed to ensuring that targeted harmonisations and clarifications are made to the substance of the Data Act in the first half of 2026 in order to limit implementation risks, legal uncertainties, and unintended market effects.

Bitkom welcomes the European Commission's approach to better align and consolidate existing EU data legislation within the framework of the Digital Omnibus. The integration of the Data Governance Act, the Open Data Directive (ODD), and the Free Flow of Non-Personal Data Regulation into the Data Act can make a significant contribution to the coherence of European data law.

Particularly, Bitkom welcomes the restriction of government access to data to genuine public emergencies, the intention to strengthen the protection of trade secrets (especially with regard to third countries), exceptions to cloud switching, and the deletion of the smart contract regulations.

At the same time, Bitkom identifies further regulatory, review, and clarification needs. These relate in particular to the required level of protection for trade secrets and confidential business information, the scope and design of exemptions in cloud switching, transitional and application rules of the Data Act (Article 50 DA), the question of applicability of Chapter VI/VIII on B2B SaaS providers, the question of applicability of Chapter VI/VIII on B2B SaaS providers, the question of retroactive effect of Chapters VI–VIII on existing contracts, the practical definition of the new public emergency situation, as well as the voluntary nature of data intermediation.
Bitkom therefore advocates using the omnibus initiative not only for formal consolidation, but also for the targeted clarification of key open implementation issues relating to the Data Act.

90%

of German companies affected by the Data Act report feeling overwhelmed by the volume of new legislation and regulatory requirements (According to a Bitkom survey)

Evaluation of key omnibus changes

Integration of DGA, ODD and Free-Flow-Regulation

The consolidation of these legislations in the Data Act is systematically comprehensible. It will be crucial that this integration is not only formal, but also leads to uniform terminology, coherent obligations, and consistent governance.

Bitkom sees particular implementation and interpretation issues here that should be addressed in the further process.

Extended protection of trade secrets (Article 4(8), Article 5(11) DA)

Bitkom welcomes the extension of rejection rights in cases where there is a high risk of trade secrets being disclosed to third countries with weaker levels of protection. This is a step in the right direction, as it enhances the safeguarding of sensitive business data and reflects current geopolitical realities.

However, Bitkom emphasises that the measures introduced so far do not go far enough to ensure legal certainty and prevent unintended distortions of competition. The new wording of Article 4(8) DA, which enables data access to be denied based on a »high risk« of disclosure, remains overly vague and may lead to misinterpretation or even strategic misuse.

In particular, there is a risk that companies will refuse access to data rooms on the basis of corporate ownership structures or the mere origin of shareholders, without having to prove specific technical or organisational security risks. This could lead to the de facto commercial exclusion of individual market players, even though they are legally established in the European Union and subject to European law.

Bitkom therefore considers it necessary to clarify that companies that are based and operate in the EU and fully comply with the European legal framework should not be classified as high-risk players solely on the basis of their ownership structure. Verifiable, objective security criteria should be decisive, not geopolitical attributions.

While the omnibus proposal strengthens the protection of trade secrets in substance, it fails to adequately address the reporting obligations that accompany the exercise of refusal rights.

In particular, Article 4(8) DA-E requires that, where a data holder refuses to share data on the basis of a high risk of trade secret disclosure, it must notify the competent authority designated pursuant to Article 37.

Bitkom reiterates its long-standing concern that such blanket reporting obligations are disproportionate and unnecessary. Even in the absence of a complaint, dispute or any indication of non-compliance, data holders would be required to report prima facie justified refusals to authorities. This creates a significant administrative burden for companies and risks overwhelming competent authorities with information that is neither actionable nor required for effective enforcement.

Existing enforcement mechanisms are already sufficient. In particular, Articles 37(5)(b) and 37(14) DA empower competent authorities to request comprehensive information from data holders in the context of substantiated complaints. Data recipients also retain access to all relevant legal remedies to assert their rights where appropriate.

Against this background, Bitkom maintains that the reporting obligations provided for in the following provisions of the Data Act should be deleted:

- Article 4(2), last sentence;
- Article 4(7), last sentence;
- Article 4(8), last sentence;
- Article 5(10), last sentence;
- Article 5(11), last sentence;
- Article 8(3), last sentence;
- Article 8(4), last sentence (new);
- Article 20(2), last sentence.9

Removing these obligations would not weaken enforcement, but rather ensure proportionality, legal certainty and an efficient use of supervisory resources.

In addition, Bitkom notes that several provisions of Article 4 DA combine substantive restrictions with far-reaching reporting obligations. As outlined above in relation to Article 4(8), such obligations should be limited to cases of substantiated complaints and not apply automatically to lawful and justified data uses or refusals.

Government data sharing only on cases of »Public Emergency«

The replacement of the broad concept of »exceptional need« with a restriction to public emergencies is welcomed in principle. At the same time, Bitkom believes that further clarification is 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 Article 22a.

Cloud Switching: Small-Mid-Caps and Custom-Made-Services

Bitkom welcomes the extension of privileges to small and mid-cap companies.
The targeted exemption for certain customer-specific individual developments is also understandable.

At the same time further clarification is needed, in particular:

- The proposed distinction between »custom-built« and the newly introduced category of »custom made services« (new Article 31(1a)),

[9] Bitkom Position Paper, »Call for Evidence: Digital Omnibus«, 2025, p. 33

- the interaction with existing contracts,
- and the practical scope of the remaining obligations (e. g., interoperability).

On the new Article 31(1a) DA-E, we appreciate the underlying intent. However, the provision is fundamentally flawed and should be removed.

While it is positive that the legislator recognizes the absence of clear rules on retroactivity for Chapter VI, the current drafting aggravates rather than resolves the issue:

i) It does not address retroactivity in Chapter VI in a general and proportionate manner, for example through adequate transitional periods comparable to existing approaches in the Data Act.

ii) It introduces a new category that conflicts with the definition of »data processing services« in Article 2(8). As formulated, »custom-made services« would effectively nullify the requirement of »minimal service provider interaction«, undermining the conceptual coherence of the »DPS« definition.

If the genuine intention is to deal with retroactivity, a more coherent approach would be either to exempt Chapter VI and Chapter VIII from retroactive application (preferred), or to introduce a proportionate transitional regime analogous to the Data Act's existing entry-into-application mechanisms (Article 50 (5) and (6) DA). Either route would align with the European Court of Justice´s doctrine on retroactivity and preserve the integrity of the »data processing services« concept.

More fundamentally, the new Article 31(1a) does not mitigate detrimental impact of Chapter VI and VIII on European enterprise SaaS providers and carries a real risk of disruption for European industry. Therefore, corrections are needed to address cloud switching requirements that are not technically achievable for complex B2B SaaS.

To ensure legal certainty and maintain the Data Act's pro-competitive objectives while avoiding unintended harm to EU innovation, we recommend that the co-legislators:

- Remove Article 31(1a) and, if retroactivity is to be tackled, adopt either a full non-retroactivity carve-out for Chapters VI and VIII or a targeted transitional regime with reasonable timelines.
- Clarify in the recitals that Chapter VI primarily targets switching barriers at the resource layer (IaaS/PaaS), and that pure application software—complex enterprise SaaS such as ERP, HCM or payroll—falls outside the core »DPS« concept.
- Provide interpretation guidance on key terms, including a resourcelayer definition of »computing resources« (for example, compute, storage, networking, container/VM orchestration, database instances) and a precise understanding of »ondemand« (requiring userinitiated or APIdriven provisioning, configuration or release of resources in near real time).
- Draw a clear line between resource-layer portability/interoperability and application-layer business logic.
- Focus interoperability and switching obligations on feasible, resource-layer outcomes (for example, export, portability, orchestration, interfaces) with

proportionate timelines, and avoid obligations that would require bespoke re-engineering of application-layer processes.

We welcome the exemption for »customer-specific« services from the Cloud Switching Rules for contracts that were concluded before or on 12 September 2025 (»existing contracts«). It is essentially in line with the EU Commission's confirmation (FAQ 58a) that Chapter VI only applies to data processing services where the digital service itself, including SaaS, can be provided or released quickly with minimal administrative effort and minimal interaction from the service provider.

Customised services, on the other hand, require time-consuming preparatory work by customers, lengthy negotiations and interactions between customers and service providers, and subsequent technical adjustments, which makes rapid provision impossible. However, the same principle also applies to digital services based on contracts concluded after 12 September 2025.

To avoid uncertainty, we propose the following overall approach:

Definition »data processing service«

We call for clear wording in the Data Act stating that a digital service itself must fulfil all the characteristics of the definition in order to be considered a data processing service. The clarification provided by the European Commission (FAQ 58a) should be included in the definition, but at the very least, the recitals should be amended accordingly to close this crucial loophole for the industry.

Specific wording:

Article 2(8) (Definitions) shall be replaced by the following wording:

»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~~ <u>if and insofar the digital service itself is elastic,</u>** 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.

Exemptions in Article 31(1)

a) *<u>Without prejudice to Article 2(8) specifying all other characteristics of a data processing service</u>, 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), 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.*~~

b) *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 service is a small and medium-sized enterprise or a small mid-cap,*~~ *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 a data processing service 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.~~*

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.

Removal of smart contract obligations

Bitkom expressly welcomes the complete removal of smart contract obligations, as the original regulation was associated with considerable practical implementation problems.

Voluntary data intermediation instead of mandatory notification

The switch to a voluntary registration and labelling system represents a fundamental change to the system. Bitkom sees a need for further discussion and clarification here, particularly with regard to:

- The future reliability of the trust framework for data intermediation,
- the reduction of organisational protection obligations,
- and the effects on competition and market structure.

Open data integration & higher fees for very large companies

The proposed changes to the reuse of public sector data and documents, in particular the possibility of setting higher fees and special conditions for very large companies, represent a further development of the previous system.

Bitkom sees a need for clarification here, particularly with regard to:

- Uniform application in the member states,
- the formulation of objective and transparent criteria,
- and the distinction from existing competition law instruments.

Bitkom also points out that differentiated fee models for the reuse of data by very large companies can also have an impact on location and innovation policy.

Research- and AI-intensive companies in particular are highly dependent on access to public data sets. Increased fees can effectively have the effect of placing an additional burden on innovation and influencing investment decisions to the detriment of Europe as a business location.

Against this background, Bitkom suggests that the impact on international R&D investments and the global competitiveness of Europe as a digital location be carefully considered in the further development of these regulations.

Missing and insufficient regulatory simplification measures

Transitional periods & retrospectivity (Article 50 DA)

There is an urgent need for clarification and adjustment on the entry into application and legacy contracts, in particular:

- Regarding the transition periods pursuant to Article 50 DA, clarify when each obligation in Chapters VI–VIII applies, and provide proportionate, phased transition periods for existing deployments.
- Regarding existing contracts: confirm whether obligations apply only to contracts first concluded after 12 September 2025 or set out a clear transitional regime for pre-existing contracts (including renewals, extensions and material amendments).
- Regarding the short termination notice and switching periods in Chapter VI: define how the notice period and the switching window interact; ensure technically feasible timelines; and allow contractual freedom, e.g. for justified extensions for complex migrations.
- Regarding the question of retroactivity confirm that Chapters VI–VIII do not apply retroactively to legacy, or, failing that, adopt a transitional mechanism that preserves legitimate expectations and avoids forced re-engineering of complex

SaaS. As described above, it should be clarified that the regulations do not apply to contracts concluded before or on September 12, 2025.

- Regarding standards and common specifications under Article VI and VIII:
  Confirm that harmonised standards and common specifications remain voluntary instruments, conferring a presumption of conformity where used.

The interpretation of Article 29(2) in relation to Article 50 DA also requires clarification.

Temporal scope of Chapters II-III (IoT data access)

The current regulation creates high implementation risks, significant retrofitting costs, and considerable investment uncertainty for manufacturers and data holders.

In particular, Bitkom sees a strong need 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.

Bitkom therefore recommends aligning the applicability of the direct access obligation under Article 3(1) DA with the availability of relevant interoperability standards and providing for a sufficient implementation period thereafter. A clearer sequencing of regulatory obligations and standardisation processes is essential to ensure legal certainty, proportionality, and effective implementation of the Data Act.

Clarification of the term »data holder« (Article 2 No. 13 DA)

There is still a considerable need for clarification regarding the definition of the term »data holder« in accordance with Article 2 No. 13 of the Data Act. The Commission's current omnibus proposal does not resolve the existing demarcation problems either but rather shifts them in part by creating a circular link between the terms »access« and »data holder«.

From Bitkom's point of view, the definition should be consistently linked to the actual technical possibility of accessing the data and to the legal responsibility for this data. Circular references within the legal definitions should be avoided.

Use of non-personal data (Article 4 (13) and (14) DA)

Bitkom sees a need to revise the provisions on the use of non-personal data in Article 4(13) and (14) DA. In their current form, these provisions create significant legal uncertainty, impose disproportionate operational burdens on data holders, and unnecessarily restrict data-driven innovation within the European Union.

From a systematic perspective, the current framework for non-personal data is conceptually inconsistent with the GDPR. While both regimes follow a comparable regulatory logic, the Data Act provides for only a single legal basis for the use of non-personal data, namely contractual permission by the user. As a result, non-personal data is subject to stricter limitations than personal data, despite its inherently lower sensitivity. This paradoxical outcome creates strong factual incentives for organisations to rely more heavily on personal data rather than on non-personal data, which runs counter to the objectives of data minimisation, innovation, and responsible data use.

In practice, the requirement to conclude a contract with the user as the sole legal basis for the use of non-personal data is in many cases commercially and technically unfeasible. This is particularly true in complex data ecosystems, data spaces, and IoT environments, where direct contractual relationships with all users cannot realistically be established. The current approach therefore risks significantly limiting the usability of non-personal data and undermining the economic potential of the European data economy. This applies in particular to large-scale industrial or machine-generated environments, complex value chains involving intermediaries, and products already placed on the market, where individual contractual relationships with users are diffuse, absent, or cannot realistically be renegotiated ex post.

In addition, Articles 4(13) and 4 (14) DA suffer from internal inconsistencies and ambiguities that further exacerbate legal uncertainty. In particular:

- The distinction between »use« and »making available« of data is not sufficiently explained or justified.
- The material scope of the two provisions is inconsistent, with Article 4(13) referring to »readily available data that is non-personal data«, while Article 4(14) is limited to »non-personal product data« without an apparent rationale.

- While Article 4(13) largely respects party autonomy and contractual freedom, Article 4(14) appears to restrict this freedom by limiting data sharing to what is strictly necessary for the performance of the respective contract.
- It remains unclear whether lawfully anonymised data falls within the scope of Articles 4(13) and (14); if anonymised data were covered, this would create a disincentive for anonymisation, as data that would otherwise benefit from the more flexible legal bases under the GDPR would become subject to stricter limitations under the Data Act.

Against this background, Bitkom reiterates its view that Articles 4(13) and (14) should be consolidated into a single, clearly structured provision. The revised provision should allow the use of non-personal data based on multiple legal grounds, aligned with the GDPR, and should respect contractual freedom without imposing unnecessary purpose limitations. Such legitimate interests may include, for example, research and development, product improvement, quality control, safety and security measures, diagnostics, maintenance, and the provision of updates or repair services, in particular where such uses also serve the interests of the user.

Clarifying that lawfully anonymised data falls outside the scope of Article 4(13) would further strengthen incentives to prioritise non-personal data and align the Data Act with broader data protection and data minimisation objectives.

At the same time, it should provide appropriate safeguards to prevent the misuse of data in a manner that could undermine the commercial position of users.

Bitkom therefore advocates for a reform of Articles 4(13) and (14) that ensures legal certainty, reduces compliance complexity, and better reflects the practical realities of digital business models, while maintaining a high level of protection for users and fair competition in the internal market.

Proposal for Article 4(13), (14) of the Data Act:

(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 use is necessary for the purposes of the legitimate interests pursued by the data holder or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the user.

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

paragraph, the data holder shall, where relevant, contractually bind the third party not to further share data received.

(14) (deleted)

Suggested amendments to the recitals:

Corresponding Recitals (25) and (26) should also be amended to clarify these broader legal bases and explicitly confirm that lawfully anonymised data falls outside the scope of Article 4(13), thereby creating a clear incentive for anonymisation. In addition, the recitals should include exemplary legitimate interests (e.g., research and development, product improvement, ensuring safety and quality control).

They should further clarify that where the use of non-personal data also serves the interests of the user, such as ensuring product safety, providing security updates, enabling repair, performing diagnostics or improving functionality, this must carry substantial weight in the balancing of interests under Article 4(13)(d). This would make clear that the data holder's interests will generally not be considered overriding, as they are consistent with and supportive of the user's interests.

Pre-contractual information requirements (Articles 3 (2) and (3) DA)

Bitkom also advocates a significant simplification of the pre-contractual information requirements under Articles 3 (2) and (3) DA. The current highly extensive information catalogues often overwhelm users and at the same time create substantial compliance costs for companies. In particular for data-poor devices and emerging data spaces, many of the mandated disclosures offer little practical value for the actual use context.

Bitkom therefore recommends limiting mandatory information to content that is actually relevant to users and making the regulations more practical overall.

4 Data Protection and ePrivacy Directive

Bitkom strongly welcomes the proposed targeted adjustments to the GDPR. The digital economy supports the Commission's approach of addressing concrete implementation problems and clearly innovation-inhibiting areas without reopening the entire Regulation. The proposal tackles many points identified by business and research as in need of reform, for example clarifying the concepts of »personal data« and »special categories of personal data«, easing certain transparency duties, adjusting breach notification requirements, and clarifying aspects of data processing in the context of AI. At the same time, many structural issues persist (see section 3). The Omnibus should be strengthened further to deliver additional, meaningful simplifications.

GDPR reality check: broad reform pressure from business

- 79% of German companies call for GDPR reform at EU level
- 77% say data protection hinders digitalisation in Germany
- 72% believe data protection is overdone in Germany
- 97% rate the data protection compliance burden as »high« or »very high«
- For 69%, the burden increased further over the last year

(According to a **Bitkom Research** survey)

These figures underline that GDPR reform is not a narrow sectoral interest, but a broadly supported concern across German business.

Across the proposal, three positive points stand out:

First, it strengthens legal certainty and innovation-friendly processing. A clearer, context-based understanding of personal data reduces interpretative discretion and aligns with the CJEU case on relative anonymity. The proposal also explicitly addresses the development and operation of AI systems through, for example, the new legal ground for processing special categories of data in an AI context (Article 9(2)(k) GDPR) and Article 88c GDPR, which frames AI training under legitimate interests. The clarification of solely automated decision-making under Article 22 also provides much-needed certainty.

Second, it reinforces risk-based and proportionate solutions. This includes raising the breach notification threshold to »high risk« cases (Article 33 GDPR), clarifying the ability to manage abusive or excessive access requests (Article 12(5) GDPR), adapting transparency obligations to clear, low-risk relationships (Article 13(4) GDPR), and introducing graduated safeguards for sensitive data in AI contexts. The exception

for user-controlled biometric authentication (Article 9(2)(l) GDPR) is also a welcome element.

Third, it contributes to harmonisation and simplification. Centralising DPIA lists and methodology (Articles 35 and 70 GDPR), creating a single reporting template and an EU-wide shared understanding of typical »high-risk« breaches, using the ENISA single entry point for notifications, and shifting key device-access and security issues from the ePrivacy Directive into the GDPR framework (Articles 88a et seq. GDPR and amendments to the ePrivacy Directive) all move the system towards a more coherent internal-market framework.

EU-wide consistent interpretative standards are essential for legal certainty. Any additional guidance can be helpful, but it should be concise, practice-oriented and example-based, and it must not introduce new substantive obligations or additional documentation burdens. Legal clarity should primarily be achieved in the Regulation itself and its recitals. Delegated and implementing acts should be used only in clearly delimited, technically necessary areas and must not add regulatory complexity.

Evaluation of key omnibus measures

Article 4 GDPR: personal data, health data and new technical definitions

The proposal clarifies that whether data is »personal« must be assessed from the perspective of the specific controller, data are not personal merely because someone else could identify the person. It also recognises that data may change status (personal vs. anonymous) when transferred between actors, and it introduces additional technical definitions aligned with other EU digital legislation.

Bitkom strongly supports this shift towards realistic identifiability and actual risk rather than hypothetical re-identification possibilities. It can significantly reduce unnecessary compliance burdens, particularly in research, AI development and data-driven product improvement. 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. More generally, data should not be treated as personal for a recipient simply because they were personal for the sender or might be personal for another potential recipient; the decisive factor must remain identifiability for the actor at hand.

This approach is consistent with the CJEU's case law of 4 September 2025, which confirms that anonymity must be assessed from the perspective of the respective controller and that pseudonymised data may be anonymous for a controller lacking the mapping information where re-identification is not realistically feasible.

To avoid divergent supervisory approaches, the criteria for »means reasonably likely to be used« should be applied in a consistent, risk-based manner, taking account of time and cost, technical availability, lawful access possibilities, and protective measures in place. Practical examples would also help users apply the concept consistently.

The additional technical definitions can increase coherence between the GDPR and other EU digital acts and support modern, user-friendly mechanisms (for example in consent management or device access). Clear delineation of competences is needed to avoid overlaps with the DMA, DSA or the EECC.

Finally, further practical clarification on pseudonymisation and anonymisation would increase legal certainty. 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.

63%

of German companies advocate for simplified use of pseudonymised data (According to a Bitkom survey)

Article 5 GDPR: purpose limitation and the research privilege

The proposal provides that further processing for archiving in the public interest, scientific or historical research, and statistical purposes is automatically compatible with the original purpose, provided the safeguards in Article 89(1) GDPR are met.

Bitkom welcomes this strengthening of research, statistics and archiving. Removing the need for a separate compatibility test under Article 6(4) GDPR will materially reduce administrative burden and facilitate data-intensive research and development, such as AI development, retrospective analyses and long-term archives, while maintaining safeguards under Article 89(1). For the change to be effective, »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. The same applies to product improvement and closely related iterations of digital products and services: continuous analysis and optimisation of functionality, security and user experience are integral to the lifecycle of digital services and align with users' legitimate expectations. This also corresponds to civil-law obligations such as the duty to provide updates for digital products (Section 327f German Civil Code). Such developments should therefore be considered compatible, provided appropriate safeguards, such as data minimisation, pseudonymisation or aggregation, are used.

Finally, it is worth reviewing whether existing consent and objection models meet the needs of modern, long-term and dynamic research and innovation projects. Rigid, purpose-specific consent can be difficult to operationalise over time; more flexible approaches may better balance research freedom and fundamental-rights protection.

Article 9(1) GDPR: the scope of protection for special categories

Compared to an earlier leaked version, the current draft no longer narrows the scope of Article 9(1) GDPR. From the perspective of the digital economy, a clarification remains necessary.

Current interpretations, under which even indirect or abstract links to health data can trigger the Article 9 consent threshold, have far-reaching practical consequences for companies without corresponding risk for individuals in many cases. The CJEU's case law on the sale of pharmacy-only products as processing of health data (CJEU, 4 October 2024, C-21/23), and the further expansion in Russmedia (CJEU, 2 December 2025, C-492/23, para. 51 et seq.), illustrate the problem: remote, reflexive or even inaccurate health inferences can be sufficient to bring processing within Article 9. This creates significant legal uncertainty, complicates consent and withdrawal mechanics, and can materially hinder innovation, particularly on digital platforms.

If the mere abstract possibility of a sensitive inference is enough, Article 9 risks becoming the default for almost all personal data processing. That would dilute the special protection for genuinely high-risk operations, consume resources with little added value for fundamental-rights protection, and undermine practical enforceability.

Article 9(2) GDPR and Article 9(5) GDPR: new permissions and safeguards (AI and biometrics)

The draft adds new legal grounds in Article 9(2) GDPR for processing special categories of data, including for developing and operating AI systems and for biometric identity verification under the individual's control, accompanied by specific safeguards in a new Article 9(5).

While the AI permission addresses an important use case, it is too narrow because it is tied exclusively to »AI systems« within the meaning of the AI Act, leaving other data-driven technologies outside its scope. The legality of processing should depend on the legitimate purpose and risk profile, not on a formal label. Less intensive use cases, such as analytics for product improvement, should certainly be included. In many data-intensive contexts, special categories may be inherent and functionally necessary; these situations should also be covered where appropriate technical and organisational safeguards are implemented.

To ensure coherence between Articles 6 and 9 GDPR, Article 9(2) should be supplemented with additional grounds where processing special categories is strictly necessary:

- To protect the legitimate interests of the controller or a third party; and
- to conclude, perform or enforce a contract whose nature requires such processing.

These grounds should be subject to strict safeguards and a risk-based assessment, rather than a blanket consent requirement. Article 9(2)(g) should also be clarified so that »public interest« does not necessarily depend on detailed sector-specific legislation.

The new Article 9(5) would in practice significantly restrict the new permission by requiring controllers to »avoid« collecting special categories and, upon identification, to remove or isolate them. Given the size and complexity of modern training, validation and testing datasets, it is unclear how organisations could demonstrate the absence of such data or fulfil associated checking obligations. In particular, »avoidance« is technically unrealistic and disproportionate when working with publicly available web data; it effectively assumes such data must never be collected, which would severely constrain, or make impossible, the development of capable AI systems.

Similarly, the obligation to remove special categories once »identified« creates major legal uncertainty. The wording implies proactive, continuous monitoring of datasets that is not operationally feasible. To remain proportionate, any duty to stop processing should apply only where the controller is specifically and verifiably notified of the presence of such data, without creating a duty to pre-emptively screen future inputs or data streams.

The additional requirement to implement output filters to prevent the display of special categories is overly restrictive and can fundamentally limit AI system utility. It would also unduly interfere with legitimate information interests, for example in relation to public figures.

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.

Finally, it should be clarified that the new exemption in Article 9(2)(k) applies not only to controllers but also to processors acting on the controller's behalf and in its interest. Given the complex AI value chain, legality must extend across the processing chain, including external AI providers, infrastructure providers and model developers. An explicit statutory clarification is needed to prevent interpretative risks and competitive distortions.

Article 12(5) GDPR: handling abusive data subject requests

The revision of Article 12(5) GDPR clarifies how controllers may deal with manifestly unfounded or excessive requests while maintaining the principle that data subject rights are generally exercised free of charge. Controllers may charge a reasonable fee or refuse requests that are manifestly unfounded or excessive, and specifically for Article 15 access requests, where it is apparent that the request is pursued for purposes other than personal data protection. The burden of proving abuse remains with the controller.

Bitkom welcomes the increased legal certainty in dealing with abusive, tactical or mass requests, which frequently arise in employment disputes, serial access requests or automated bulk submissions. Explicitly addressing purpose-misuse in Article 15 context reflects common practice where access rights are used as leverage in negotiations.

The ability to charge fees should be clarified as applying in particular where the underlying relationship is not primarily shaped by data protection and processing is merely an ancillary consequence. In such cases, controllers should be able to charge a reasonable fee reflecting the actual effort required, taking into account staffing and technical resources, scope and complexity of the data, the level of identity verification needed, and any third-party involvement, subject to any applicable sectoral rules.

However, the abuse provision risks becoming ineffective if individuals are never required, even upon request, to provide information about the purpose of their access request. Without that, it is often practically impossible to evidence misuse. It should therefore be clarified that, upon request, data subjects must explain the purpose of their request. This would allow a fair misuse assessment without changing the nature of the right of access. Controllers should be able to assess the stated purpose only on the basis of objective and verifiable criteria. A concise, practice-oriented clarification of what »other purposes« means, ideally through typical examples, would be helpful, provided it does not create additional proof or documentation burdens.

Overall, Bitkom considers the reform an important step in safeguarding workable GDPR processes and providing controllers with a practical instrument against misuse. To ensure consistent application, the terms »manifestly unfounded« and »excessive« should be further clarified. In repeated, mass or clearly non-data-protection-related requests, it should be sufficient for controllers to set out the misuse in a reasoned manner; in those situations, it should be for the data subject to make a plausible case for a further legitimate interest.

Article 13(4) and (5) GDPR: expanded exemptions from information duties

The draft introduces new exemptions from information duties for direct collection. Article 13(4) allows information duties to fall away where there is a clear relationship, processing is not data-intensive, and it is reasonable to assume the individual already knows the key information, except for particularly high-risk processing. Article 13(5) introduces an additional research exemption where providing information is impossible, would involve disproportionate effort, or would seriously impair research objectives, provided safeguards under Article 89(1) are in place.

These exemptions can materially reduce transparency burdens, particularly for SMEs, organisations with straightforward customer relationships and research institutions. Article 13(4) can prevent unnecessary repeat or boilerplate notices in situations where individuals already know the relevant facts, without weakening protection in complex or high-risk processing.

In modern, distributed digital processing structures, it should also be made clear that controllers may rely on high-quality privacy notices provided by engaged third-party providers, where those notices fully, clearly and up-to-date cover the relevant information. This would avoid duplication, improve consistency and increase legal certainty for both controllers and individuals.

From Bitkom's perspective, the carve-back in Article 13(4) is problematic because 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

85%

of German companies are calling for less bureaucracy in data protection incidents. (According to a Bitkom survey)

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 every day, 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.

Finally, the term »not data-intensive« remains too vague and creates legal uncertainty. It needs workable clarification, for example by illustrative categories or by reference to existing risk criteria such as those used in Article 35 GDPR, to support consistent EU-wide application.

60%

of German companies are calling for fewer information requirements (According to a Bitkom survey)

Article 22 GDPR: conditions for solely automated decisions

The proposal clarifies when decisions with legal effects or similarly significant impacts may be based solely on automated processing, including profiling. Such decisions should be permissible where they are necessary for entering into or performing a contract, are authorised by Union or Member State law with appropriate safeguards or are based on explicit consent.

This reform is highly relevant for data-driven business models and the use of AI-supported decision-making. It increases legal certainty and flexibility, notably by clarifying that a decision can be »necessary« even where a manual route is theoretically possible, resolving a long-standing dispute in current practice. It creates a workable framework for typical digital use cases such as scoring, fraud detection, automated risk assessments and AI-based decisions, without weakening individual protection.

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. In particular, inconsistencies may arise where a decision-maker relies decisively on an automated score or assessment generated by a third party: while the decision-maker may benefit from the exception under Article 22(2)(a) GDPR, the third party that created the automated assessment may itself fall within the scope of Article 22 GDPR under CJEU case law, yet have fewer possibilities to rely on the exception due to its narrow interpretation and the lack of legal clarification. Explanations in the recitals could support consistent and practice-oriented application.

Such clarifications would codify CJEU case law (including SCHUFA, C-634/21), prevent over-extension, and ensure that preparatory, supporting or purely technical automation is not mistakenly captured by Article 22.

Article 33 GDPR: notification of personal data breaches

The proposal aligns breach notification with EU cybersecurity law, especially NIS2, including extending the deadline to 96 hours for breaches likely to result in a high risk to individuals' rights and freedoms, and moving reporting over time to the NIS2 single entry point. It also requires the EDPB to propose an EU-wide reporting template, to be adopted by the Commission via an implementing act and reviewed regularly.

Bitkom welcomes the extension to 96 hours and the move towards NIS2 alignment. In practice, however, the relief will remain limited as long as weekends and public holidays count towards the deadline. Many cases already run partly or entirely over a weekend under the current 72-hour rule, so the additional time often provides little extra room for assessment and response. The deadline should therefore be calculated in business days, or at least weekend and holiday hours should be excluded.
For meaningful alignment, the sector-specific Regulation (EU) No 611/2013 should also be repealed.

More broadly, notification duties across EU legislation should be harmonised. Beyond deadlines, thresholds for when an incident becomes notifiable should be aligned across the GDPR, NIS2, DORA and other sectoral frameworks. Different timelines, risk concepts and parallel thresholds create legal uncertainty, multiple reporting and inefficient processes. A consistent standard would improve report quality, reduce duplication and conserve resources for both companies and authorities.

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.

The extensive internal documentation obligations for breaches that do not meet the high-risk threshold should also be reviewed. These obligations often create significant organisational overhead with limited added value for individuals. Refocusing documentation duties on notifiable high-risk incidents would allocate resources more effectively and keep attention on genuinely relevant security events.

Over time, a central EU single entry point can reduce duplicate reporting and improve coordination between data protection and cybersecurity authorities. A harmonised reporting template can also simplify administration, provided it is designed with practical use in mind, accommodates different company sizes and structures, and is aligned with existing notification duties under NIS2, DORA and sectoral rules.

Overall, Bitkom considers the proposed changes a useful step towards modernising and harmonising breach notification. They reflect the technical and organisational effort involved in assessing complex incidents and can reduce pressure to submit premature or incomplete notifications. Success will depend on consistent harmonisation of deadlines and thresholds and on a tangible reduction of documentation burdens below the high-risk level.

Article 35 GDPR: harmonisation and centralisation of DPIAs

The proposal would largely centralise and harmonise the DPIA framework. The EDPB would develop EU-wide lists of processing requiring a DPIA and exempt processing, as well as a common template and methodology, which the Commission would make binding via an implementing act. National lists would remain in force until the new EU-wide regime applies.

Moving from national lists to a centrally developed, Union-wide binding framework would overcome today's fragmented DPIA practice and significantly increase legal certainty, especially for cross-border businesses facing divergent and sometimes contradictory national requirements. A common template and methodology can standardise DPIA practice, clarify supervisory expectations and make planning, documentation and internal compliance processes easier. Regular review can ensure technological developments are properly reflected.

Bitkom supports the direction of centralisation, but it should take account of the fact that many organisations have built robust, effective DPIA processes that already meet the protective purpose of Article 35 GDPR. Forcing an immediate and mandatory replacement of established procedures with a single EU template or prescribed methodology could create substantial transition costs without necessarily adding value in every case.

Harmonisation should therefore allow existing DPIA procedures to continue where they are substantively compatible with EU requirements. EU templates and methods should serve as a common reference point and best practice that existing systems can align with, rather than requiring a wholesale replacement. Generous transition periods would also be appropriate, enabling gradual adaptation and preventing well-functioning compliance structures from being displaced abruptly.

For SMEs in particular, common templates and methods can be helpful. At the same time, the new framework should not become a one-size-fits-all solution that ignores organisational and technical realities. Flexibility and proportionality are essential for success.

Article 41a GDPR: criteria for when pseudonymised data are no longer personal data

Article 41a would empower the Commission to define criteria and technical benchmarks via implementing acts to determine when pseudonymised data are no longer personal data for certain controllers or recipients, taking into account the state of the art and actor- and context-specific re-identification risks. Applying these criteria could serve as evidence that data fall outside the GDPR.

Bitkom welcomes a Union-wide framework that gives controllers and recipients practical criteria to assess when pseudonymised data are no longer personal for them, addressing one of the GDPR's core practical problems: persistent legal uncertainty at the boundary between personal and anonymous data. The approach aligns with the CJEU's 4 September 2025 case law confirming relative anonymity.

For Article 41a to work, »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. Clear regulatory recognition of these technologies as valid state-of-the-art measures would create investment incentives, support market maturity and help ensure accessibility for SMEs. The criteria should remain technology-neutral, flexible and future-proof, reflecting the evolving capabilities of re-identification techniques.

It should also be clear that applying Article 41a criteria is one possible way to demonstrate that data are no longer personal, but not a mandatory procedure. Organisations must retain the ability to use their own risk-based methods. At the same time, the framework should support reliable documentation of the loss of identifiability. Optional recognition or certification mechanisms could contribute here. Once data have been classified as non-personal under an accepted approach, controllers and recipients need legal certainty that the data can be used outside the GDPR's scope on an ongoing basis.

Article 70(1) GDPR: expanded tasks for the EDPB

The proposal expands the EDPB's tasks to strengthen harmonisation of core GDPR processes. In particular, the EDPB would develop proposals for EU-wide DPIA lists (required/exempt), a common template and methodology, and a single breach-notification template including an EU-wide agreed understanding of typical »high risk« situations.

Bitkom welcomes strengthening the EDPB's role in technical coordination and the preparation of harmonisation tools. In areas such as DPIA lists, methodologies and reporting templates, the EDPB can help ensure consistency and bring together supervisory expertise.

Clear governance between the EDPB and the Commission is essential. Technical coordination and drafting should remain with the EDPB, while political steering, final adoption of binding requirements and enforcement should be anchored with the Commission. This is important both for uniform application and to avoid the creation of informal or de facto binding »side standards«.

EDPB working processes should also be improved. Early, structured and transparent involvement of business and other relevant stakeholders can increase practical relevance, test feasibility early and reduce later interpretative disputes. Public consultations, structured stakeholder dialogues and topic-specific expert rounds can be useful formats. Such openness would improve both the quality and acceptance of harmonised outputs and help ensure they are understood as a shared reference framework rather than rules developed far from operational realities.

Overall, strengthening EU-level harmonisation is welcome, but it should be embedded in a clear governance model that ensures transparency, participation and effective decision-making, while reinforcing the Commission's role as the central steering actor in EU data protection law.

Article 88c GDPR: processing personal data for the development and operation of AI systems

Article 88c would provide an explicit legal basis for processing personal data to develop and operate AI systems within the meaning of the AI Act, allowing reliance on legitimate interests (Article 6(1)(f) GDPR) where processing is necessary and individuals' interests or fundamental rights do not override. The legal basis would not apply where sector-specific rules explicitly require consent.

Bitkom strongly supports the Commission's objective: strengthening legal certainty for data-driven innovation with substantial social and economic benefits. AI systems already deliver essential value in areas such as healthcare, mobility, energy efficiency, cybersecurity, accessibility, public administration and education. Their development and operation frequently require processing large datasets, often impossible without a reliable legal basis.

Bitkom therefore welcomes the clear signal that developing and operating such systems is, in principle, a legitimate activity that can be grounded in legitimate interests, provided it is done responsibly and with appropriate safeguards.

To achieve its purpose, Article 88c must function as a reliable and EU-wide uniform legal basis. Ambiguous drafting 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 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.

Without this, Article 88c risks restricting or crowding out established data-driven business models, such as digital services, automated analytics, personalised functionality or AI-enabled process optimization, not because of real risks, but because of legal uncertainty and divergent national interpretation.

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.

In applying Article 88c, it should also be recognised that uniquely identifying natural persons is often not feasible in data-intensive digital contexts. Users operate across multiple devices (e.g., smartphone, tablet, laptop), and reliable cross-device attribution to a specific individual is frequently not possible for controllers without additional information. Regulatory assumptions that implicitly rely on continuous or unambiguous identifiability overstate risks and do not reflect technical reality.

Application of Article 88c should therefore be anchored in realistic identification and risk scenarios.

Further clarification is needed to ensure practical applicability along complex AI value chains, especially to make explicit that processors are covered where they act on the controller's behalf under an Article 28 relationship. Legality must extend across the entire processing chain, including external AI service providers, infrastructure providers and model developers.

Finally, the legislator should avoid hard-coding contested technical assumptions, for example about personal data being stored in model weights. The framework should remain technology-neutral and allow for different technical approaches.

Cookies, device access and aligning the GDPR with ePrivacy

Article 88a GDPR

Article 88a would integrate access to information on end-user devices into the GDPR framework where personal data are concerned. This direction is welcome: it acknowledges that the GDPR pursues a different protective logic than the historically communications-secrecy-focused approach of the ePrivacy Directive. Done properly, Article 88a could replace the inconsistent cookie regime developed over years and differentiate device access based on actual risk to individuals, provided it is designed as a true lex specialis within the GDPR rather than a continuation of a blanket consent requirement.

69%

of German companies say data protection complicates AI training (According to a Bitkom survey)

In practice, an end-user device cannot be equated with a uniquely identifiable natural person. Individuals commonly use multiple devices in parallel, smartphones, tablets, laptops, or share devices in households or workplaces. Reliable device-to-person attribution is often impossible for controllers without additional data or may be legally impermissible. A blanket reliance on person-specific consent therefore ignores technical reality and produces repeated, redundant consent prompts without effectively increasing protection.

Cookie use must be possible on the basis of Article 6 GDPR legal grounds. It is crucial to clarify that cookies and similar technologies are not confined to consent but, like any other processing of personal data, can rely on the other legal bases in Article 6 GDPR, particularly legitimate interests under Article 6(1)(f). Article 88a should explicitly confirm that all Article 6 legal bases are available for device access. A general priority for consent is incompatible with the GDPR's risk-based logic.

The current draft effectively reproduces the ePrivacy approach by making device access generally dependent on prior consent and allowing only a few narrowly drawn exceptions. This overlooks that device access is not inherently high-risk in every case and sits uneasily with the GDPR's structure. The EU legislator deliberately created multiple equivalent legal bases in Article 6 to legitimise processing in a risk-appropriate way. A general consent priority for device access cannot be derived from either the GDPR's wording or its purpose. Controllers should be able to rely on legitimate

interests for cookies and similar technologies where a careful balancing test is conducted and suitable safeguards are implemented. Otherwise, Article 88a would effectively create a new special category of processing that contradicts the GDPR's core design.

Low-risk processing, such as contextual advertising, audience measurement, frequency capping, traffic validation or fraud detection, serves legitimate economic purposes and is essential for an open, ad-supported internet. These uses must remain permissible under an Article 6 legitimate-interests assessment without mandatory consent. This approach would both reflect the GDPR's risk-based system and materially reduce consent fatigue by focusing consent on genuinely higher-risk situations.

The draft should also clarify that illustrative design examples, such as consent via a single-click button, are merely examples and do not establish mandatory technical standards. Different contexts, devices and user groups require flexible, equivalent mechanisms to ensure transparency and control. Similarly, rigid time-based lock-out periods for repeated prompts are not practical; they may even conflict with individuals' interests when contexts change, or a renewed situational choice is desired. A risk-based approach that allows flexibility is preferable.

Necessary clarifications and extensions

For Article 88a to deliver simplification in practice, further changes are needed:

- Expand the exceptions in paragraph 3 beyond purely internal audience measurement, including use by specialised processors and third parties, in particular for SMEs;
- expand paragraph 3 to allow manufacturers of connected products to use data for additional purposes such as load balancing and planning, pre-installed applications, devices and consumables, product improvement, security, and R&D, also supporting compliance with the EU Data Act;
- address the current limitation of audience measurement to »internal« use, which does not reflect market reality: SMEs and start-ups often cannot operate their own measurement infrastructure and rely on specialist providers under processing arrangements. Treating such providers as if they were independent controllers can lead to privacy-friendly aggregated measurement remaining consent-based in practice. A risk-based approach should focus on the nature of processing, not the number of actors involved;
- clarify »own use« to ensure purpose-bound processing by processors is included;
- ensure that security measures do not depend on whether they were »requested« by the user but reflect objective IT and platform security needs;
- extend the regime to non-personal device data, or adjust Article 5(3) of the ePrivacy Directive accordingly, to avoid the inconsistency whereby non-personal data are subject to stricter requirements than personal data.
- A particularly problematic inconsistency arises between personal and non-personal device data. While Article 88a provides exemptions from consent for personal data, technically anonymous or purely functional data remain subject to the stricter regime of Article 5(3) ePrivacy. This creates a paradox: less intrusive processing,

such as anonymous telemetry, diagnostics or security data from industrial or technical systems, faces stricter requirements than personal data. It also forces controllers to assess every device access for

- possible personal-data relevance, creating substantial overhead. This fragmentation is neither proportionate nor workable and should be avoided through a coherent, unified approach.

If properly designed, Article 88a can create a single, practical and innovation-friendly framework that protects privacy effectively without endangering functioning digital business models.

Article 88b GDPR

In light of the continued far-reaching consent requirements, the Commission presents machine-readable preference signals under Article 88b as an apparent remedy for consent fatigue. The concept is unconvincing both legally and practically and misses its stated objective.

At a conceptual level, Article 88b's scope is unclear: it is not evident whether preference signals relate only to device access or also to subsequent processing of read-out data. The draft also lacks a workable approach for mobile apps and app environments where browsers are not central. These uncertainties create substantial legal uncertainty and argue against adding another technically complex mechanism.

Under the GDPR, consent must be informed, specific and purpose-bound. Blanket browser settings such as »accept all« or »reject all«, intended to apply across all websites and purposes, cannot meet these requirements. This leads to two problematic outcomes: (1) legally robust consent remains necessary, so websites would still need their own prompts, cookie banners would not disappear; and (2) a global »reject all« signal would indiscriminately block cookies needed for low-risk, legitimate purposes such as audience measurement, fraud detection or contextual advertising.

The draft also fails to answer practical questions: how granular consent by purpose or provider would be represented; how to deal with dynamic websites where vendors change; and how to implement an effective, ongoing right to withdraw if the initial decision is made via a browser-level setting. These deficits conflict with the GDPR's requirements for informed and specific consent.

Rather than solving the problem, Article 88b risks worsening it and could function as a de facto ban on large parts of the ad-supported internet without data protection necessity. It would also shift power towards dominant browser providers, who would effectively decide how preference signals are interpreted and defaulted, raising competition concerns and undermining a fair, innovation-friendly internal market. In a highly concentrated market, it is doubtful that any intended SME privileges would work in practice.

The proposed sectoral »media exception« underscores the problem: it seeks to shield certain sectors from negative effects but does not reflect the reality of an interconnected digital ecosystem. Media companies depend on data flows from other sectors; if those flows dry up due to global rejection signals, the exception becomes ineffective.

Consent fatigue cannot be solved by adding technical complexity; it can only be addressed by reducing consent requirements where they are not warranted by risk. If Article 88a (i) exempts low-risk processing from consent, (ii) explicitly enables legitimate interests, and (iii) creates a coherent framework for all device data, then no additional mechanism under Article 88b is needed. Cookie banners would largely disappear in practice without outsourcing consent decisions to browser providers.

The proposed six-month binding effect for decisions taken under Articles 88a/88b also highlights practical incoherence: to enforce and respect a rejection, the rejection information itself must be stored locally, typically again via a cookie or similar storage mechanism. This creates a regulatory paradox: enforcing »no cookies« requires storing data on the device. Moreover, storage is device-based, while the draft assumes a person-based decision. Under these conditions, workable implementation is unlikely.

For these reasons, Bitkom strongly recommends deleting Article 88b and focusing legislative efforts on a clear, risk-based and GDPR-compliant Article 88a. This is the only way to reconcile effective privacy protection with digital value creation and a functioning European internet.

Missing and insufficient regulatory simplification measures

Despite the Digital Omnibus' positive direction, major structural deficits of the GDPR and the ePrivacy regime remain. This part builds on the logic supported in section 2 and highlights where the same approach should be taken further to strengthen harmonisation, legal certainty, risk orientation and innovation capability in a sustainable manner.

Persistent fragmentation

The reform reduces fragmentation only selectively. While DPIAs, reporting templates and some technical questions are harmonised, significant discretion remains across more than 40 national supervisory authorities in many other areas. Without further centralisation and more consistent enforcement and interpretation, divergent readings and supervisory practices will continue, at odds with the omnibus' goal of practical internal-market standards.

A key driver of fragmentation is also the continued existence of the ePrivacy Directive. The parallel application of the GDPR and ePrivacy perpetuates overlapping competences, duplication and avoidable compliance costs. To create a coherent framework, the outdated ePrivacy Directive should be repealed and the confidentiality of communications should be integrated into a future EU-wide instrument.

Missing risk-based principle 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.

Lack of risk-based differentiation for documentation and accountability duties

A core deficit remains the insufficiently risk-based design of extensive documentation and accountability obligations. Although a risk-based approach is referenced in several places, especially Recital 4, which recognises the need to balance data protection with other fundamental rights and societal interests, this principle has not been implemented consistently in practice. Documentation duties (e. g., Article 28 processing agreements, Article 35 DPIAs, Article 30 records of processing, internal accountability documentation) apply largely irrespective of the actual risk of a given processing operation. As a result, clearly low-risk processing is subject to the same formal requirements as high-risk processing.

Further relief should therefore be based on the actual risk of the processing, not primarily on company size. Large organisations also carry out many low-risk processing activities, and small companies can conduct high-risk processing. A rigid size-based approach is therefore inadequate.

What is needed is a deeper integration of a genuine risk-based approach across the GDPR, allowing the scope, depth and form of documentation duties to reflect the real protection needs of individuals. This would reduce administrative burden while allowing supervisory resources to focus on genuinely relevant risks. It would also give effect to the balancing logic in Recital 4, protecting data protection as a fundamental right without disproportionate interference with other rights and legitimate interests of business and society. SMEs would particularly benefit, without lowering the level of protection for individuals.

Limited use of legal openings for innovation

The omnibus strengthens legitimate interests in specific areas, especially for AI (Article 88c GDPR). This is welcome but remains limited to selected use cases. For other data-intensive processing with comparable social value, such as personalised medicine, mobility, energy optimisation or security, reliable legal openings are still missing. This unnecessarily constrains Europe's potential for data-driven innovation in key future-oriented domains.

Positive lists of data types

The GDPR could benefit from statutory positive examples that clarify which data types may be processed under which conditions and for which purposes within a legitimate interests balancing exercise. Such positive lists would concretise a risk-based approach, harmonise interpretation and reduce burdens by making lawful and robust room for manoeuvre visible, not only prohibitions.

Further sectoral specification and codes of conduct

Alongside horizontal tools such as Article 41a, a more differentiated, context-sensitive application of the GDPR is needed where general rules alone do not sufficiently reflect sectoral realities, processing contexts and risk profiles. Sector-specific codes of conduct under Article 40 GDPR are a key instrument for practice-oriented, flexible and innovation-friendly implementation developed with affected stakeholders and under supervisory oversight. Recognised codes can materially increase legal certainty by providing concrete sectoral guardrails for permissible processing, safeguards and risk assessments. A better combination of horizontal harmonisation and sectoral operationalisation would strengthen the GDPR's uniform application while preserving necessary flexibility.

Missing group privilege

The lack of a group privilege remains a major structural gap. Internal data sharing within a corporate group is still subject to the same requirements as transfers to external third parties, even where a uniform data protection management system and a consistently high group-wide level of protection are in place. An explicit group privilege for administrative and organisational purposes would significantly ease compliance practice and strengthen the competitiveness of European corporate groups without weakening individuals' protection. This is also a coherent adjustment given that administrative fines are calculated based on the group.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Jana Gaulke | Head of Brussels Office
P +49 30 27576-315 | j.gaulke@bitkom.org

Janis Hecker | Head of AI, Regulation & Strategy
P +49 30 27576-239 | j.hecker@bitkom.org

Lucy Czachowski | Head of AI & Cloud Policy, Resilience & Infrastructure
P +49 30 27576-320 | l.czachowski@bitkom.org

Isabelle Stroot | Head of Data Protection Law & Policy
P +49 30 27576-228 | i.stroot@bitkom.org

Felix Kuhlenkamp | Head of Security
P +49 30 27576-279 | f.kuhlenkamp@bitkom.org