VDA German Association of the Automotive Industry

Position

For a strong data and industrial base

Feedback on the European Commissions Digital Omnibus of 19 November 2025

10.03.2026

Introduction

The German Association of the Automotive Industry (VDA) welcomes the European Commission‘s initiative to simplify the digital legal framework through the Digital Omnibus. Consolidating existing regulations is an important step toward strengthening European industry’s competitiveness and enhancing legal clarity for companies. As a key sector for innovation and employment in Europe, the automotive industry is particularly reliant on a coherent and reliable legal framework.

From the VDA‘s point of view, the following points are particularly positive:

- **More precise definitions:** clearer definition of the term “personal data“ in Article 4(1) of the GDPR and introduction of a legal definition for “scientific research“.
- **Extended grounds for permission:** allowing the use of special categories of personal data under Article 9 GDPR for AI model development.
- **Creation of a compatibility basis for research in Article 5(1)(b) GDPR:** the removal of the “purpose limitation“ strengthens data access for research.
- **Prevention of rights abuse:** sanctions and refusal rights strengthen controllers’ position against abusive assertions of data subjects’ rights.
- **Bundled reporting obligations:** Bundling reporting obligations and reporting deadlines reduces bureaucracy.

These changes are suitable for creating legal clarity in specific areas. However, they do not address the structural problems identified by the VDA – as already highlighted in its statement on the European Data Union Strategy – and, without further adjustments, do not actually provide any noticeable relief for companies. The VDA therefore sees a need for further adjustments in order to consistently implement the goals of simplifying digital legislation and to ensure a balance between data and data protection law and innovation capacity.

Data protection

1. Inclusion of the characteristic of “directness“ in Article 9 GDPR and use of special categories of personal data for innovation

The EU Commission‘s proposal restricts the use of special categories of personal data to AI training purposes. This is insufficient and jeopardises safety-related innovations in the automotive industry.

The use of special categories of personal data for safety-enhancing technologies such as automated driving must be expressly permitted in order to promote innovation and thereby improve road safety. Driver condition data, gaze behaviour, reaction patterns, physiological indicators and behavioural signals are of central relevance for the further development of safety-critical technologies such as automated driving, collision avoidance and fatigue detection, and the corresponding data processing is necessary to enable vehicle manufacturers to contribute to reducing traffic accidents.

The Commission‘s proposal leaves open the question of how far the prohibition on processing special categories of personal data extends.

Proposal:

- In order to create legal certainty, it must be clarified that the prohibition on processing special categories of personal data only applies to information that directly reveals sensitive characteristics. Processing that allows indirect derivation must not be prohibited across the board. The inclusion of the characteristic of “directness“ in the wording of the law prevents an excessive extension of the scope of application of the standard.

- In addition, the implications of Article 9(5) GDPR must be clarified. It should be specified what measures are required to ensure that the data is not used to generate output. Furthermore, the restriction on disclosure to third parties may lead to significant practical challenges, particularly where data needs to be shared within a corporate group or with cooperation partners. Clear guidance is necessary to avoid legal uncertainty and ensure that legitimate data flows for safety and innovation purposes remain possible.

2. Practical adaptation of the transparency and consent rules in Articles 88a to 88c GDPR

The EU Commission‘s proposal includes a reform of the ePrivacy rules in the GDPR, which is generally welcomed as it creates a uniform legal basis and harmonises transparency obligations. The inclusion of an exception for aggregated usage information for reach measurement and for measures to maintain or restore the security of a service or terminal device is a step in the right direction. However, despite partial relaxations in Article 88a GDPR, the EU Commission is sticking to the basic consent requirement, which means disregarding all other equivalent legal bases of the GDPR and, as a consequence, excluding all downstream data processing based on Article 6(1)(f) GDPR.

Article 88a GDPR replaces the term “user or subscriber“ (as used in Article 5 of the ePrivacy framework) with “data subject,“ which creates significant challenges for B2B and multi-user

scenarios such as connected vehicle fleets. Under this approach, consent or the request of a service from the owner or authorised representative of the end device would no longer be sufficient[1], instead, individual consent from each user may be required. This would substantially complicate operational processes, particularly in fleet management, and restrict the decision-making authority of fleet operators.

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

Finally, the proposed cybersecurity exemption is too narrow, as even the remediation of recognised vulnerabilities would still require consent – even though the measures are essential for road safety. These challenges arise fundamentally because the device-access rules of Article 5(3) ePrivacy are being embedded into the GDPR through Articles 88a–88c, thereby transferring a consent-only mechanism into contexts where connected-vehicle data access must support continuous and legally required safety- and cybersecurity operations.

Overall, the focus on cookies falls short and ignores the challenges of connected products such as vehicles and IoT devices, which require continuous, security-relevant data communication. As a result, the proposed amendments could lead to the automotive industry losing a significant proportion – in some cases up to 80% – of the data relevant for the development of innovative systems. To ensure that the reform does not lead to a de facto blockade of vehicle data, further adjustments to the standards are needed.

Proposal:

- The VDA rejects embedding the device-access rules of Article 5(3) ePrivacy into the GDPR and calls instead for a modernised Article 5(3) ePD that allows the use of all GDPR legal bases, including legitimate interests, and explicitly enables device access required for legally mandated safety- and cybersecurity operations (e.g. UNECE R155/R156, type-approval obligations, CRA and NIS2) without dependence on individual consent.

- B2B practice must be observed in such a way that consent given or service requested by the authorised representative is effective, so that device-access under Article 5(3) ePrivacy/ Articles 88a–88c GDPR does not require individual consent from every driver. This has been taken into account in the TDDDG, for example, as the “user“ according to § 25 (2) No. 2 TDDDG can be both natural and legal persons. Overall, the use of digital services ordered by a business must not depend on the consent of individual natural persons.

3. Technology-friendly, harmonised and internationally compatible design

The EU Commission‘s draft continues to classify intra-group data transfers as external transfers. This leads to considerable bureaucratic effort and unnecessary costs, particularly in global corporate structures.

---

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

Proposal:

- The VDA maintains its demand that a group privilege be enshrined in the GDPR.

In addition, the lack of harmonisation between the GDPR and the Data Act creates a parallel regulatory regime with conflicting requirements. A particular problem is that the two sets of rules impose different technical and organisational requirements, which leads to additional complexity and legal uncertainty. Clear guidelines confirming that proven GDPR mechanisms, such as standard contractual clauses, are sufficient, are missing.

Supplementary proposal:

The VDA sees an urgent need for the international transfer rules in the Data Act to be either deleted or at least harmonised with the GDPR.

4. Anchoring proportionality as a core principle of the GDPR in Article 5 GDPR

The GDPR does not enshrine proportionality as a core principle. All processing operations are treated equally, regardless of whether they pose a high or negligible risk to the rights of data subjects. Even short-term, technically necessary processing without any intended personal reference is subject to the same strict requirements as complex big data projects. This causes disproportionate costs and inhibits innovation in the development of automated driving functions, connected vehicles and mobility services.

Proposal:

- A risk-based approach should be enshrined in Article 5 of the GDPR, exempting non-data-intensive processing operations from comprehensive obligations. This creates legal certainty, reduces bureaucracy and promotes investment in future technologies.

5. Strengthening the role of the European Commission

The EU Commission‘s proposal strengthens the Commission‘s role in important areas. It should have the authority to set binding standards for data protection impact assessments, data breach notifications and machine-readable consent signals.

In addition, the Commission is to be supported by a “European Data Innovation Board“ as part of its strategic coordination and harmonisation of the legal framework.

The VDA welcomes the Commission’s intention to strengthen EU level governance, including through the introduction of Article 41a GDPR. Due to the limited availability of harmonised EU level criteria, essential GDPR concepts are interpreted differently by supervisory authorities, which hampers cross border innovation and creates inconsistent compliance obligations. The Commission’s current mandate, which is largely limited to implementing acts related to specification of pseudonymised data, does not sufficiently address these structural uncertainties or provide the legal clarity needed for emerging technologies.

Proposal:

- The mandate in Article 41a GDPR should be expanded to a more general level by empowering the Commission to adopt implementing acts to specify GDPR via binding, harmonised sector specific criteria and standards in areas where legal uncertainty hampers innovation.

- The Commission's role should be strengthened so that it can independently approve codes of conduct and certification mechanisms under Articles 40 and 42 GDPR.

6. Clarifying Information Obligations and Research Exemptions under the GDPR

Transparency and effective data subject rights are crucial for strengthening data sovereignty. However, the practical implementation of data subject rights under Articles 13, 14 and 15 GDPR poses considerable challenges in practice. The Digital Omnibus provides for simplifications, for example in the rejection of abusive requests for information, exemptions from information obligations and indirect information in research projects. However, these approaches are not sufficient. These limitations become particularly evident in sectors where continuous data processing is inherent to product functionality and safety.

The development of ADAS and automated driving functions relies fundamentally on real world data, including recordings of public road traffic. For technological progress, data from series production vehicles is increasingly essential.

However, for such continuous data collection in public traffic environments, Article 13 GDPR requires that information obligations be fulfilled at the moment of data collection. In series production vehicles, this is practically impossible. In these scenarios, the controller has no direct interaction with the data subjects in the traffic environment, making individual notice obligations operationally impossible. Furthermore, it remains unclear how the requirement to make information publicly available under the new Article 13(5) GDPR is to be implemented in large-scale, decentralised real-world data collection scenarios.

The Digital Omnibus proposes amendments to Article 89 GDPR, including potential exemptions from Article 13 for research and innovation. It remains unclear to what extent the amended Article 89 GDPR, including the new Article 13(5), provides effective relief for innovation driven technological development in the automotive sector. The Commission's proposal to recognise scientific research as a legitimate interest under Article 6(1)(f) GDPR is an important step. Clarification is required on whether industrial research and innovation activities fall within this scope, as such forms of development often lie outside the narrow academic research definition.

Proposal:

- The VDA calls for binding rules against abusive requests with clear deadlines and an exception for direct data collection analogous to Article 14(5)(b) GDPR. Without these additions, implementation of data subject rights would remain disproportionately complex and costly for companies, without significantly improving data protection for the data subject concerned.

In addition to these general requirements, clarification is required to ensure that the amended Article 89 GDPR effectively covers data-intensive automotive innovation. To this end:

- The Commission should clarify that Article 89 GDPR, as amended, applies to innovation related development of ADAS and automated driving, including exemptions from Article 13 GDPR.

- Guidance should explicitly confirm whether the revised definition of “scientific research“ covers automotive innovation activities.

- The Commission should explain whether the proposed amendments lead to a practical change for series vehicle data use or whether further adjustments are required.

7. Practical adjustment of the documentation obligation under Article 30 GDPR

The Commission‘s proposals do not yet include risk-based relief from documentation requirements. Companies must continue to document all processing operations, even if they pose a low risk to the rights of data subjects. This results in considerable administrative effort without providing any tangible added value for data subjects.

Proposal:

- The VDA calls for a risk-based exemption in Article 30(5) GDPR to exclude non-data-intensive processing operations from the record.

Data economy

The automotive industry relies on reliable, internationally compatible and innovation-friendly data access rules, particularly in connection with connected vehicles, sensor data, OTA updates, assistance systems and AI-based automation. Only a coherently structured data ecosystem enables research, product development and series production to be scaled efficiently. The EU Commission‘s Digital Omnibus can be a decisive lever for this, as it provides for the first time for the harmonisation of regulations such as the GDPR, Data Act and Data Governance Act and reduces redundant parallel interpretations. This is urgently needed in view of the increasing overlap between personal, non-personal and industrial machine data.

At present, the Data Act in particular is creating uncertainty regarding the reuse of vehicle and sensor data and role relationships. While this already creates practical challenges, the underlying issues extend beyond isolated misalignments and point to structural conflicts between the GDPR and the Data Act, which create systemic inconsistencies that go beyond isolated implementation issues. Mixed datasets in the automotive sector - comprising inseparable personal and non-personal information – are simultaneously subject to both regimes, yet neither the GDPR nor the Data Act provides a clear mechanism for resolving normative conflicts. This causes legal uncertainty for downstream data use, particularly in fleet, rental and corporate vehicle contexts, where OEMs cannot realistically identify drivers and therefore face ambiguity as to whether the processed information constitutes personal data at all. Furthermore, the Data Act requires compliance with the GDPR but does not itself establish a suitable legal basis for the processing of personal data. As a result, companies frequently find themselves in a compliance dilemma: sharing data risks GDPR non-compliance, while refusing to share data risks violating the Data Act. Additional uncertainty arises from diverging definitions – such as “data holder“, “user“ and “controller“ - which complicate technical implementation and contractual governance. Finally, overlapping transfer restrictions under the GDPR and the Data Act create redundant obligations and obstruct international data flows within global

value chains. Taken together, these inconsistencies undermine legal certainty, create disproportionate compliance burdens, and ultimately hinder the scalability of data-driven innovation across the automotive value chain.

Proposal:

- Establish a clear conflict-resolution mechanism between the GDPR and the Data Act to provide legal certainty for mixed datasets and to prevent contradictory obligations for downstream processing.

- Clarification of the term “data holder“ (Article 2 (13) Data Act) remains necessary. The EU COMs first proposal In the Digital Omnibus does not amend the wording of Article 2(13), but the practical ambiguity of the definition persists. The focus should be on the actual ability to access the data and the legal responsibility regarding the data. Therefore, a clearer delineation of the criteria that determine who qualifies as a data holder remains essential.

- Improvements regarding the use of non-personal data (Article 4 paras. 13 and 14 Data Act). No application to anonymized data; full possibility for user consent without purpose limitation; consolidate Article . 4 paras. 13 and 14 Data Act into a single provision.

- Simplification of the provision of pre-contractual information (Article 3 paras. 2 and 3 Data Act) and reduction of catalog information to relevant content for the user.

- **Repeal of RED III, Article 20a:** With the Data Act (and existing competition law regulations), there is already a harmonized and binding legal framework within the EU for sharing IoT data. In this respect, some aspects may be redundant without providing significant added value. Therefore, consideration should be given to (fully) repeal of Article 20a RED III.

Only through this systemic consolidation can the Digital Omnibus actually achieve the desired simplification and strengthen European industry in global data competition.

Cybersecurity and reporting obligations

With the implementation of NIS 2, the Cyber Resilience Act (CRA), the AI Act and sectorspecific type approval legislation (UNECE R155 / R156), cybersecurity-related obligations in the European Union are increasingly fragmented. Parallel requirements regarding risk management, certification, documentation and incident reporting are currently accumulating, forcing companies to notify identical incidents multiple times under different legal frameworks. The Digital Services Act (DSA) further contributes to a fragmented set of obligations.

While each regulatory instrument pursues legitimate objectives, their cumulative effect leads to growing complexity without a proportional increase in cybersecurity. The Digital Omnibus represents the first opportunity to structurally consolidate these requirements. However, the current draft does not yet specify how uniform reporting thresholds, harmonised timelines and effective “one-stop submission“ mechanisms will be implemented in practice.

This issue is particularly relevant for the automotive industry. Connected and OTA-updateable systems continuously generate security-relevant software versions throughout the entire product lifecycle. At the same time, manufacturers and suppliers are required to report incidents

to multiple authorities, including data protection authorities, market surveillance bodies, type approval authorities and cybersecurity centres. This fragmentation consumes resources that are urgently needed for prevention, mitigation and rapid incident response. An EU-wide harmonised reporting framework would significantly reduce regulatory friction and improve response times in crisis situations.

In addition, the VDA notes that the embedding of the ePrivacy device-access regime (Article 5(3) ePD) into Articles 88a–88c GDPR would further aggravate this fragmentation, as it risks making legally mandated safety- and cybersecurity operations under UNECE R155/R156, type-approval legislation, the CRA and NIS2 dependent on individual consent.

Beyond reporting obligations, cybersecurity requirements increasingly affect organisational governance, supply chain structures, certification practices and global operating models. Without clear coordination and proportionality, horizontal cybersecurity regulation risks overlapping with established sectoral frameworks, leading to uncertainty, duplicated controls and inefficient allocation of security resources.

Proposal

To effectively reduce regulatory complexity and strengthen cybersecurity outcomes, the following measures are necessary:

- **Ensure coherent cybersecurity governance and avoid parallel oversight**

  Cybersecurity governance must be clearly structured and coordinated across horizontal and sector-specific frameworks. Where products, systems or services are already subject to harmonised sectoral security regimes, additional horizontal oversight must be avoided. Cybersecurity regulation should focus on coordination, information sharing and consistency rather than creating parallel audit or enforcement structures.

- **Avoid double regulation and reduce regulatory complexity**

  Cybersecurity-related regulation and certification approaches should be limited to the necessary minimum. Systems and components supplied by companies that can demonstrate compliance with established vertical, industry-specific regulation and certification schemes should not be subject to additional horizontal requirements. Only where systems, components or separate technical units are not covered by sectoral regulation should horizontal cybersecurity rules apply. Voluntary product-group-specific cybersecurity certification schemes should be withdrawn where products are already subject to binding product security requirements under EU law.

- **Withdraw overlapping cybersecurity requirements under the Radio Equipment Directive**

  The Commission should repeal the Radio Equipment Directive Delegated Regulation (EU) 2022/30 and its Supplement (EU) 2023/2444 with regard to cybersecurity requirements. Systems and components, including radio equipment, are already comprehensively regulated under Regulation (EU) 2024/2847 (Cyber Resilience Act). Maintaining parallel requirements leads to legal uncertainty and duplicate compliance without improving cybersecurity.

- **Strengthen recognition of existing standards and certifications**

  Existing sectoral, international and industry-proven cybersecurity standards and certifications should be systematically recognised as equivalent. This includes well-established automotive assessment and audit schemes such as such as ISO/SAE 21434, VDA-ISA/TISAX, EUCC or equivalent internationally recognised frameworks used across multi-tier automotive supply chains. Cybersecurity compliance must follow a “once-only“ principle, allowing companies to reuse existing evidence across regulatory frameworks. Multiple certifications for identical security objectives do not increase security but generate unnecessary costs and delays, particularly for SMEs in industrial supply chains.

- **Reduce the number of harmonised European standards**

  The number of harmonised European standards to be developed under horizontal cybersecurity legislation should be considerably reduced. Instead, established and existing standards from vertical, industry-specific regulation should be recognized. This ensures continuity, international compatibility and efficient implementation without lowering security levels.

- **Adopt a strictly risk-based approach to supply chain security**

  Cybersecurity measures affecting digital supply chains must be proportionate and based on real security risks. The classification of systems or components as security-relevant must be grounded in realistic attack paths, privileged access rights and actual exposure, rather than purely theoretical connectivity. Overly broad classifications risk capturing entire system architectures without improving security outcomes.

- **Ensure lifecycle-oriented implementation and transition arrangements**

  Cybersecurity requirements must reflect the long development, approval and operational lifecycles of industrial products. Clear differentiation between new developments and systems already placed on the market is essential. Binding transition periods and grandfathering provisions are necessary to preserve supply continuity, investment security and the long-term operability of deployed systems.

- **Ensure harmonised EU-wide implementation of NIS 2**

  Uniform and central guidance is required to ensure consistent interpretation of key concepts under NIS 2 and to avoid additional national requirements that fragment the internal market. Diverging national approaches undermine legal certainty and operational efficiency.

- **Simplify NIS 2 requirements for intra-group services**

  Where NIS-2-regulated services pursuant to Annex I No. 8 (Digital Infrastructure) are provided exclusively within a corporate group, in line with Commission Implementing Regulation (EU) 2024/2690, such services should be exempted from the full scope of NIS 2 obligations. Applying identical requirements to purely internal group services does not increase cybersecurity but creates disproportionate administrative burden for globally integrated automotive groups.

- **Recognise CE marking under the Cyber Resilience Act for critical ICT products**

  In accordance with Article 24(2) of Directive (EU) 2022/2555 (NIS 2), CE marking pursuant to Regulation (EU) 2024/2847 (Cyber Resilience Act) should be recognised as a sufficient cybersecurity requirement for critical ICT products. Additional cybersecurity assessments under NIS 2 for products already compliant with the Cyber Resilience Act should be avoided in order to prevent duplicate conformity procedures without added security value.

- **Simplify and harmonise incident reporting obligations**

  Incident reporting obligations should be harmonised across EU cybersecurity and data legislation. A maximum of three reports per incident should apply:

  – an initial report within 48 hours containing basic information,
  – an interim report only upon explicit request by the authority,
  – a final report after resolution with full details.

- **Establish a central EU reporting gateway**

  A central EU reporting gateway should consolidate incident notifications under the GDPR, NIS 2, the Cyber Resilience Act and sector-specific legislation. Reports should be automatically routed to competent authorities, reducing administrative burden and accelerating response times.

- **Introduce risk-based reporting and documentation thresholds**

  Minor incidents should not trigger disproportionate reporting and documentation obligations. Risk-based thresholds for both reporting and documentation are essential to focus resources on genuinely security-relevant events while maintaining a high level of protection.

- **Recognise established automotive cybersecurity frameworks and audit schemes**

  Well-established and audited cybersecurity frameworks used across the automotive industry, such as recognised information security assessment and management schemes, should be explicitly acknowledged as compliant minimum standards. Where companies can demonstrate conformity with such frameworks, additional organisational or process-related cybersecurity audits must be avoided. This recognition is essential to prevent redundant assessments, reduce administrative burden and ensure efficient cybersecurity governance across complex, multi-tier supply chains.

- **Ensure voluntary and proportionate organisational cybersecurity certifications**

  Organisational cybersecurity certifications should remain voluntary and must not become a de facto prerequisite for market access, contractual eligibility or regulatory compliance. Where such certifications are used, they should be designed as reusable, cross-regulatory evidence following a “once-only“ principle. Mandatory or implicitly enforced organisational certifications would disproportionately affect small and medium-sized enterprises and divert resources away from effective technical and operational security measures.

- **Maintain international compatibility and mutual recognition of cybersecurity approaches**

  Cybersecurity frameworks, certifications and assessment schemes should be designed with international interoperability in mind. European-specific requirements that are not aligned with globally established standards risk creating new trade barriers and weakening global supply chain resilience. Mutual recognition of equivalent international cybersecurity approaches is essential to preserve Europe's competitiveness and to support globally integrated development, production and security operations.

- **Safeguard operational cybersecurity and incident response capabilities**

  Cybersecurity regulation should support effective operational security, including continuous monitoring, threat detection and coordinated incident response. Regulatory requirements must not delay or obstruct technical mitigation measures through excessive procedural obligations, particularly in crisis situations.

To ensure that the Digital Omnibus achieves its objective of genuinely reducing bureaucracy, regulatory fragmentation in the area of cybersecurity must not only be acknowledged but also resolved in a technically and procedurally coherent manner.

Contact persons

Dr. Marcus Bollig
Managing Director

marcus.bollig@vda.de

Jürgen Mindel
Managing Director

juergen.mindel@vda.de

Martin Lorenz
Head of department security, data & digitalization

martin.lorenz@vda.de

Susanne Jonetzko
In House Counsel, Legal and Compliance, DPO

susanne.jonetzko@vda.de

The German Association of the Automotive Industry (VDA) consolidates around 620 manufacturers and suppliers under one roof. The members develop and produce cars and trucks, software, trailers, superstructures, buses, parts and accessories as well as new mobility offers.

We represent the interests of the automotive industry and stand for modern, future-oriented multimodal mobility on the way to climate neutrality. The VDA represents the interests of its members in politics, the media, and social groups. We work for electric mobility, climate-neutral drives, the implementation of climate targets, securing raw materials, digitization and networking as well as German engineering.

We are committed to a competitive business and innovation location. Our industry ensures prosperity in Germany: More than 780,000 people are directly employed in the German automotive industry.

The VDA is the organizer of the largest international mobility platform IAA MOBILITY and of IAA TRANSPOR-TATION, the world's most important platform for the future of the commercial vehicle industry.

If you notice any errors, omissions or ambiguities in these recommendations, please contact VDA without delay so that these errors can be rectified.

Publisher	German Association of the Automotive Industry Behrenstraße 35,10117 Berlin www.vda.de/en
	German Bundestag Lobby Register No.: R001243 EU Transparency Register No.: 9557 4664 768-90

Version	March 2026