GDV German Insurance Association

Position Paper

of the German Insurance Association (GDV)
ID-number 6437280268-55

on the EU Commission Digital Package

A strategic step forward in reinforcing our competitiveness

German insurers welcome the EU Commission's proposal on a Digital Omnibus. It already includes important approaches to simplify digital regulation without weakening protection standards. The proposal is a step in the right direction and paves way for a more innovation-friendly and efficient regulatory landscape. We encourage European legislators to continue boldly on this path and restore the necessary balance between regulatory requirements, innovation and strong citizens protection. Regarding the current proposal, we would like to outline our analysis and suggestions.

Table of Contents

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
German Insurance Association
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Phone: +49 30 2020-5000 · Fax: +49 30 2020-6000

Rue du Champ de Mars 23, B-1050 Brussels
Phone: +32 2 28247-30 · Fax: +49 30 2020-6140
ID-number 6437280268-55
www.gdv.de

Contact
European office

E-Mail
bruessel@gdv.de

1. GDPR

If we want the European Union to remain competitive and deliver real benefits to citizens, we need a GDPR framework that protects privacy **while enabling innovation**. For consumers, this means faster claims processing, fairer pricing, and stronger fraud prevention. For society, it means trust in digital services and responsible AI use. For EU businesses, it means legal certainty and reduced compliance costs, so companies can invest in innovation instead of bureaucracy.

We welcome:

- **Clearer rules on pseudonymisation: Art. 4(1), Art. 41a** – which confirms the relative approach and empowers the EU Commission to define when pseudonymized data is considered non-personal. This allows data to be used in a privacy-preserving way, benefiting customers through innovative services while maintaining a high level of data protection.
- **Legal basis for AI: Art. 88c, 6(1)(f), Art. 9(2)(k)** – which allows AI model training and operation under legitimate interest – including sensitive data – with safeguards. This enables insurers to offer faster, more accurate, and personalised products and services to the direct benefit of customers, while ensuring European insurers remain competitive globally and develop trustworthy AI, within a clear predictable legal framework.
- **Automated decisions simplified: Art. 22** – The strict “necessity” test is removed which allows automated individual decision making even when a non-automated option hypothetically exists. This supports efficient, scalable digital processes that are essential for modern insurance services.
- **Less burden for breach reporting: Art. 33** – Deadlines are extended up to 96 hours and reporting is limited to high-risk breaches. This allows resources to focus on incidents that are genuinely relevant for data subjects and supervisory authorities.
- **Limits on abusive requests: Art. 12(5)** – which adds cases where rights are exploited for non-data-protection purposes. This helps ensure that customer rights remain meaningful and are not diluted by misuse or mass requests.
- **Data Protection Impact Assessments**: **Art. 35, 70** – The EU Commission will adopt a single EU-wide list of processing operations that do/do not require a Data Protection Impact Assessment, and a common template/methodology, in cooperation with the EDPB. This promotes harmonisation, legal certainty and a level playing field across Member States.
- **Modernised cookie rules: Art. 88a, Art 88b** – which reduces banner fatigue and enables central consent settings.

Our suggestions:

- **The provisions on AI training and operation must be practically feasible to achieve full effectiveness.** These two limitations should be reconsidered:
    - **No unconditional right to object: Art. 88c -** Serious concerns arise regarding the reference to an "unconditional" right to object in Art. 88c Sentence 2. This goes beyond Article 21 GDPR and would in practice be unworkable. An unconditional right to object would imply that organisations must remove an individual's data from trained AI models, an action that is generally technically infeasible. We therefore recommend deleting the word "unconditional" or aligning the provision directly with the right to object laid out in Article 21 GDPR.
    - **No unconditional avoidance of sensitive data: Art. 9(5) -** Sentence 1 formulates an unconditional avoidance of sensitive data. We would recommend introducing that processing sensitive data is to be "avoided to the greatest extent possible" instead. Alternatively, processing could be required to be avoided "in accordance with the principle of data minimisation" (cf. Article 89(1) sentence 2 GDPR).
- **The changes in Art. 12(5) on abusive requests are a step in the right direction. However, the burden of proof to demonstrate the abusive intent behind a request remains heavy: Art. 12(5)** – there is potential for meaningful relief. For example, an exemption could be introduced for cases in which providing the information would impair the establishment, exercise, or defence of legal claims, and the controller's interest in not providing the information outweighs the data subject's interests.

What's missing for insurers:

- **Legal basis for health data in insurance: Art. 9(2)** – Processing health data in the private insurance sector is legally complex, especially in Germany. Obtaining informed consent is rarely practicable. Therefore, a clear statutory legal basis under Article 9(2) GDPR for processing health data for the conclusion and performance of insurance contracts (including reinsurance) is needed. This ensures legal certainty and a level playing field across the EU – core objectives of the digital Omnibus.
- **Clarification on criminal conviction data: Art. 10** – the insurance industry urgently needs clarification that Article 10 GDPR does not prohibit the processing of personal data related to criminal convictions and offences when necessary to meet supervisory requirements, manage the insurance business, prevent fraud, or defend or enforce legal claims.

- **Intra-group data transfers –** the Digital Omnibus should establish a clear, explicit legal basis under the GDPR for intra-group data processing within insurance groups, in particular for special categories of personal data under Article 9 GDPR. This is essential for group-wide risk management, compliance, reinsurance and supervisory reporting, and to ensure legal certainty across Member States.

2. AI Act

By adopting proportionate, risk-based obligations and realistic timelines, legislators can ensure **responsible AI development without compromising Europe's leadership in technology**.

We welcome:

- **New legal basis for AI bias training: Article 4a** – the extension to non-high-risk AI applications and AI models is also welcome to reduce legal uncertainty and fragmentation while enabling insurers to develop and deploy AI in compliance.

Our suggestions:

- **Adequate use of the filtering mechanism: Article 6(3)** – we welcome the deletion of Article 49(2) AI Act, which removes the registration requirement for AI applications not classified as high-risk under Article 6 (3). However, it is crucial that the filtering mechanism of Article 6 (3) does not become ineffective due to the counter-exception in the second subparagraph.
- **Extension of exemptions for small mid-caps (SMC)** – We welcome the introduction of SMCs as a new companies' category and the plan to simplify the requirements for them in the AI Act. Exemptions currently applicable to small and medium-sized enterprises will be extended to this category. However, in the Omnibus IV legislative package debate, co-legislators called for higher thresholds for SMCs. The Parliament proposes threshold of 1,500 employees and annual turnover of €450 million or annual balance sheet total of €387 million. To meet European companies' demands and promote competitiveness, these thresholds should also be raised in the AI Act.
- **Reasonable deadlines for applying high-risk AI requirements** – although the insurance industry remains critical of classifying AI systems used for risk assessment and pricing in life and health insurance as high-risk, it is positive that legislators recognise the difficulty of implementing the requirements without standards and guidelines. However, it is questionable whether the proposed timeframe of six months is sufficient to implement

these requirements. To provide better planning security, deadlines should be extended, and specific dates would also be preferable.

What's missing for insurers:

- **Clarification on AI definition as traditional statistical methods are not AI** – In light of the re-emerging debate on the AI definition, linear models, supporting methods from the field of explainable AI and established statistical methods (e.g. logistic regression) as well as common statistical methods such as generalised linear models (GLMs) should not be classified as artificial intelligence under this definition. These existing statistical analysis and models, including GLMs, differ from AI tools because they generally lack autonomy or adaptiveness after deployment, and rely on rules entirely defined by natural persons to execute operations automatically.
- **Avoid overlapping of impact assessments** – the Fundamental Rights Impact Assessment under Article 27 AI Act substantially overlaps with existing obligations under Article 35 GDPR. It does not add meaningful additional protection but creates parallel procedures and unnecessary administrative burdens. The Digital Omnibus should therefore eliminate the separate requirement under Article 27 AI Act and avoid duplicative assessment obligations.

3. Data Act

The proposal allows data owners to refuse disclosure of trade secrets if there is a high risk of unlawful acquisition, use, or disclosure to third countries or entities controlled by them that are subject to a legal system with weaker safeguards than those in the Union. The vague terms 'high risk' and 'unlawful acquisition' leave excessive room for interpretation in practice. In our view, the existing provision in Article 4(8) is sufficiently specific and adequately protects data owners' interests regarding trade secrets.

4. Incident reporting & Cybersecurity

We welcome:

- **A single-entry point** for incident reporting – for its design, it needs to function as a transmission platform and is not developed into a database. In the long term, standardising both the reporting templates and deadlines would bring a noticeable reduction in effort.

What's missing for insurers:

- Digital regulation must remain coherent and avoid overlaps. **Insurers should not have to comply with the CRA** – DORA and the CRA offer similar protection but differ in implementation. In practice, this leads to additional interpretation issues and, in some cases, parallel internal capacity requirements – resources that could otherwise support innovation. At the same time, this allocation of resources does not measurably increase the system or consumer safety.
- The current **broad definition of ICT services** under DORA creates considerable effort for low-risk services. The bureaucratic effort, particularly in contract negotiations, is no longer proportionate to the expected added value. The definition should therefore be streamlined and clarified.

5. EU Business wallet

Insurers will rely on the Business Wallet for secure digital interactions with customers and partners, including identity verification, document signing, and data exchange. Clear rules are essential to ensure security, prevent profiling risks, and avoid unnecessary compliance burdens. **The Business Wallet should be designed alongside the citizen EUDI-Wallet from the outset.** Delaying it would lead to fragmented standards and duplicated development. A unified approach ensures a coherent, interoperable and scalable EU identity ecosystem for citizens, companies and public authorities.