GDV German Insurance Association

Empower. Innovate. Scale.

A coherent digital framework for Europe



Table of Contents

Introduction 03

1 Europe's digital and consumer protection framework: enabling trust, resilience and innovation 04

A regulated sector committed to a responsible digital economy 05
A regulatory framework that is fit for purpose 05
Towards smart, fair and strong EU legislation 06

2 Our recommendations on key digital legislative frameworks 07

Digital Omnibus: an opportunity to modernise Europe's Digital Rulebook 08
AI Act: clear guidance and risk-based approach are essential 09
Digital Fairness Act (DFA): the need to avoid duplication 09
European Business Wallet (EUBW): a tool for secure and efficient digital business interactions 10
Cloud and AI Development Act (CADA): a framework for European digital autonomy 10

3 Our proposals to secure, empower, innovate 11

Conclusion – One coherent digital rulebook 14

GDV

German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft e. V.)
Wilhelmstraße 43 / 43 G, 10117 Berlin
Visitor entrance: Leipziger Straße 121
P.O.Box 08 02 64, 10002 Berlin
berlin@gdv.de

Rue du Champ de Mars 23
B-1050 Brussels
Phone: +32 2 282 47–30
Fax: +49 30 2020–6140
bruessel@gdv.de

Contact
Florian Wimber
Head of European and International Affairs
Phone: +32 2 282 47–36
f.wimber@gdv.de

Photo credits
Cover, S. 4, S. 10 – Unsplash
S. 7 – Getty Images · 2257248656 · © tichr

Disclaimer
The content was created with the necessary care. Nevertheless, there is no guarantee that the information or assessments contained therein are complete, correct, up-to-date or appropriate.

© GDV 2026

Introduction

Digital regulation shapes everyday life across Europe. It affects how people access essential services, how their data is used, how quickly they receive support when something goes wrong, and whether innovative products and services reach them at an affordable price. Getting these rules right therefore matters not only for businesses, but for millions of consumers and citizens across Europe.

Insurance shows how directly these rules affect people's everyday lives. German insurers alone manage nearly half a billion contracts and handle more than 25 million claims every year, more than 69,000 every day. Digital rules therefore influence millions of interactions between consumers and insurers, from taking out a policy and sharing information to receiving support after an accident or loss. In 2024, German insurers paid €66 billion in claims and €101.8 billion in life insurance benefits, underlining how important efficient and reliable processes are for consumers when they need them most.

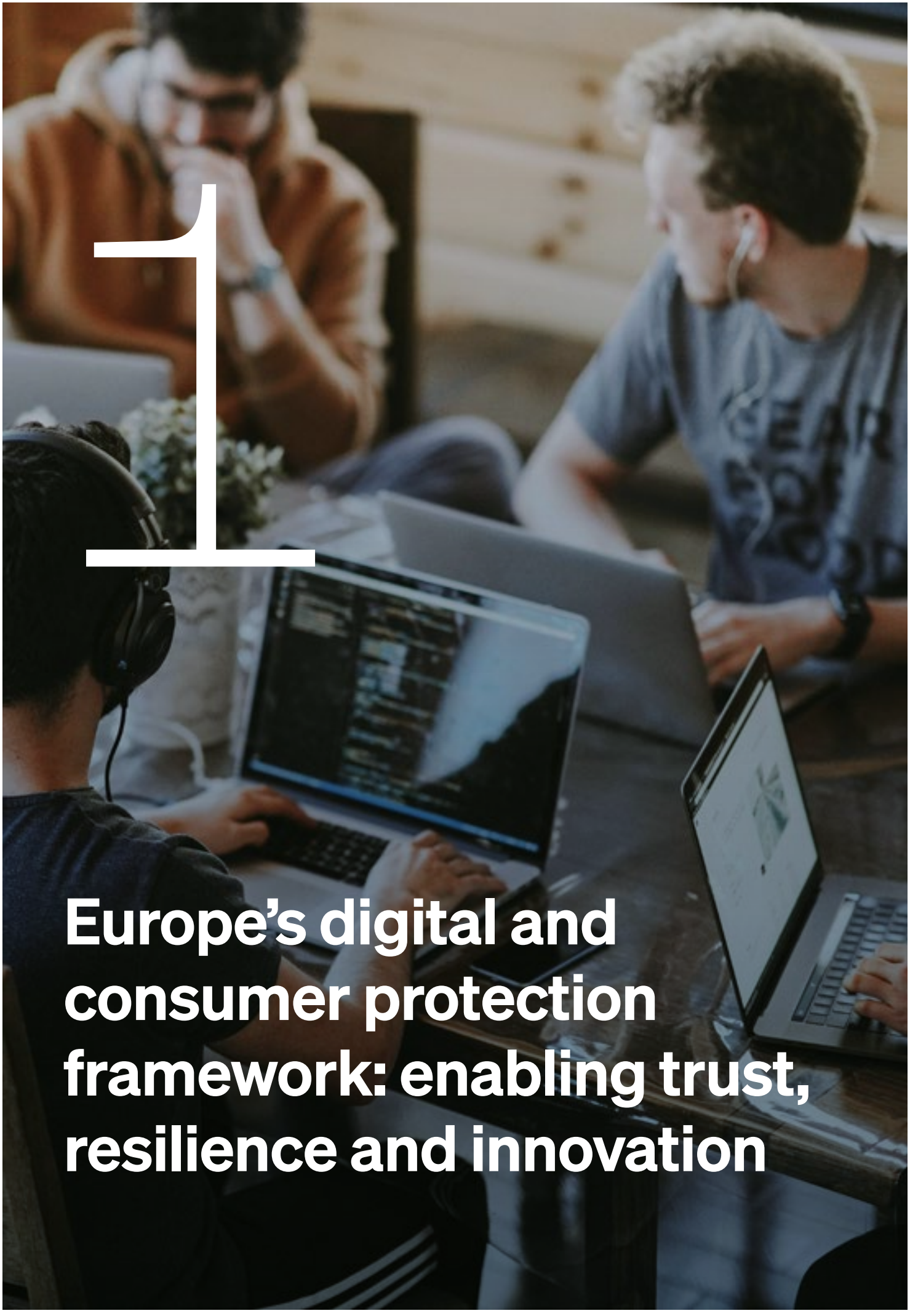
Digitalisation can make these interactions simpler, faster and more responsive. AI can accelerate claims handling and improve fraud detection. Better use of data can support more personalised services and reduce administrative friction. Secure digital identities and business wallets can simplify interactions for consumers and businesses alike. But these benefits will only materialise if Europe's regulatory framework combines effective consumer protection with sufficient room for innovation.

This is what **Empower. Innovate. Scale.** means in practice. **Empower** consumers by protecting their rights, preserving meaningful choice and giving them access to simple and secure digital services. **Innovate** by giving businesses the legal certainty and proportionality they need to develop new and better products, services and solutions. **Scale** by ensuring that successful digital solutions can be deployed across the Single Market rather than being held back by overlapping, fragmented or inconsistent rules.

From our perspective, the choice is not between consumer protection and innovation. Europe needs both. Well-designed digital regulation should protect people from genuine risks while allowing technologies that make their lives easier, safer and more affordable to develop and spread.

The insurance sector also has a wider stake in getting this framework right. With €1.9 trillion in assets and €200–300 billion in new investments each year, German insurers are major long-term investors in Europe. A regulatory environment that allows digital solutions to scale supports not only better services for consumers, but also Europe's broader capacity to invest, grow and innovate.

GDV advocates for a digital regulatory framework that builds on existing safeguards, avoids unnecessary duplication, provides legal certainty and follows a proportionate, risk-based approach. The following chapters show where the initiatives currently under discussion can contribute to that objective — and where changes are needed to ensure that Europe's digital rulebook **empowers consumers, supports innovation and allows successful solutions to scale.**



1

Europe’s digital and consumer protection framework: enabling trust, resilience and innovation

© GDV 2026

The digital transformation of the insurance sector is not a future scenario; it is already underway. Insurers are leveraging digital tools to improve risk assessment, streamline claims processing, and enhance customer experiences.

A REGULATED SECTOR COMMITTED TO A RESPONSIBLE DIGITAL ECONOMY

Insurers play a central role in risk management and innovation. In the digital age, they continue to demonstrate leadership by adopting new technologies responsibly. The sector operates within a comprehensive regulatory framework that ensures robust consumer protection, data security, operational resilience, and ethical use of emerging technologies.

The **Insurance Distribution Directive (IDD)** requires insurers to act honestly, fairly, and professionally in the best interests of their customers. It mandates that products align with customer needs and that distribution strategies remain transparent and appropriate. These measures ensure fair treatment for all consumers, including vulnerable groups.

The **General Data Protection Regulation (GDPR)** establishes a robust framework for processing personal data, including sensitive information. Its safeguards for automated decision-making and profiling protect consumers from unfair or opaque practices. Insurers have made substantial investments in compliance and data security, often exceeding minimum requirements to protect customer information.

The **Digital Operational Resilience Act (DORA)** imposes comprehensive ICT risk management, incident reporting, and third-party risk requirements on financial entities, including insurers. These obligations ensure that insurers maintain high levels of cybersecurity and can withstand and recover from cyber incidents.

The **Artificial Intelligence (AI) Act** introduces a risk-based framework for artificial intelligence systems. Insurers rely on a broad spectrum of analytical tools, including established statistical and actuarial models that differ fundamentally from autonomous or adaptive AI systems and should therefore be treated accordingly under the regulatory framework. In parallel, they constantly adapt to new technologies to offer the most suitable products to their customers. For instance, AI-driven tools help identify and prevent fraudulent claims, saving costs while protecting policyholders. Advanced data analytics enable the development of products tailored to individual needs, improving accessibility and affordability. Automation and digitalisation have significantly reduced claims processing times, enhancing customer satisfaction and operational efficiency.

A REGULATORY FRAMEWORK THAT IS FIT FOR PURPOSE

Europe does not lack digital regulation. On the contrary, insurers already operate under one of the most comprehensive regulatory frameworks in the world, encompassing consumer protection, data governance, operational resilience, cybersecurity, and artificial intelligence. The central challenge is therefore not the absence of rules but ensuring that existing frameworks work together coherently. Future legislative initiatives should focus on improving consistency, reducing unnecessary overlap, and providing the predictability needed to support both innovation and consumer trust.

A streamlined regulatory environment is particularly important as Europe seeks to strengthen its competitiveness. Resources devoted to navigating overlapping obligations are resources that cannot be invested in innovation, cybersecurity, customer service, or the development of new products. Regulatory effectiveness should therefore be measured not by the quantity of legislation adopted, but by the ability of existing rules to work together effectively, deliver policy outcomes, and support European competitiveness.

While insurers are fully committed to digital transformation, they also recognise the importance of balancing innovation with consumer protection and financial stability. The current regulatory landscape is complex and multi-layered, with overlapping requirements that can sometimes create unintended challenges.

As the regulatory framework continues to evolve, overlapping or conflicting requirements across different pieces of legislation can create ambiguity and risk, making it difficult for insurers to plan and invest with confidence. Smaller insurers may struggle to keep up with the administrative demands of multiple regulatory frameworks, potentially reducing their ability to compete effectively.

The objective is not less regulation, but better regulation: clear, coherent and proportionate rules that deliver strong consumer protection while enabling innovation, investment and competitiveness. A smart, fair, and strong regulatory framework can help ensure that insurers can continue to innovate, protect consumers, and contribute to Europe's digital economy.

TOWARDS SMART, FAIR AND STRONG EU LEGISLATION

For GDV, smart regulation builds on existing legislation and avoids unnecessary duplication. Fair regulation maintains a level playing field while ensuring proportionate obligations. Strong regulation protects consumers and strengthens resilience without unduly constraining innovation and investment.

To address these challenges, GDV advocates for a consistent approach to digital and consumer protection regulation. For insurers, the digital agenda is not about technology for its own sake. It is about ensuring that Europe's frameworks enable secure data use for risk assessment, efficient claims handling, and seamless customer interactions across borders. It is about maintaining access to global cloud capacity and digital tools without sacrificing resilience. And it is about leveraging digital identity solutions to reduce fraud, streamline compliance, and improve operational efficiency.

© GDV 2026



2

Our recommendations on key digital legislative frameworks

GDV's recommendations are guided by a simple principle: where robust protections already exist, new legislation should reinforce and simplify the framework rather than duplicate it. This approach underpins our vision of smart, fair and strong regulation.

DIGITAL OMNIBUS: AN OPPORTUNITY TO MODERNISE EUROPE'S DIGITAL RULEBOOK

Deliver targeted GDPR simplification while preserving trust

The proposed clarification of when pseudonymised data constitute personal data is particularly important for insurers. Insurance relies on data to understand risks, develop products, prevent fraud and improve services. A clear and balanced approach to pseudonymisation can facilitate responsible data use while preserving the protection provided by the GDPR.

GDV also supports clearer rules for the use of data in the development and operation of AI systems. A predictable legal basis for responsible AI development is essential if European insurers are to develop trustworthy applications within Europe.

GDV also strongly supports the proposed clarification of Article 22: decisions necessary for entering or performing a contract should be eligible for automation even where a human could also take them. This would provide legal clarity for automated underwriting and claims handling while preserving individuals' rights to human intervention and to contest decisions.

The simplification of automated decision-making and the modernisation of cookie rules can further support efficient digital services and improve the customer experience. Longer breach reporting timelines would also allow firms to focus resources on understanding and containing incidents before providing complete information to authorities.

GDV nevertheless considers further clarification necessary to ensure that new requirements do not create additional uncertainty. In particular, the framework should remain proportionate when regulating sensitive data and should avoid creating rights or obligations that are difficult to reconcile with existing GDPR principles.

Provide legal clarity for insurance-specific data use

The Digital Omnibus should address areas where insurers continue to face uncertainty despite having legitimate and well-established business needs.

GDV calls for a clear legal basis for the processing of health data where this is necessary for the conclusion and performance of insurance contracts, including reinsurance. Clear rules for intra-group data processing would also support group-wide risk management, compliance and supervisory reporting.

Greater clarity is equally needed concerning the processing of data relating to criminal convictions where this is necessary for fraud prevention, supervisory compliance or the establishment, exercise or defence of legal claims.

A specific legal basis within the GDPR should also be established for intra-group processing, particularly where this involves special categories of personal data under Article 9 GDPR.

Make cyber regulation coherent

Insurance is already subject to the Digital Operational Resilience Act, which establishes a comprehensive and sector specific framework for ICT risk management, incident management, resilience testing and third-party ICT risk.

The Digital Omnibus should therefore ensure that cyber legislation works as one coherent framework. Requirements under DORA should not be duplicated by the Cyber Resilience Act, Cyber Security Act or other horizontal cyber rules.

GDV supports the proposed single-entry point for cyber incident reporting. One incident should generate a

© GDV 2026

single reporting process rather than requiring insurers to provide substantially the same information under several regulatory regimes. At the same time, the information contained in the report and the stored data should only be accessed by the respective competent authorities.

The same principle should guide the wider implementation of DORA, the Cyber Resilience Act and NIS2. Strong cyber resilience is essential for insurers and their customers, but resilience is not strengthened by duplicative reporting and compliance requirements.

AI ACT: CLEAR GUIDANCE AND RISK-BASED APPROACH ARE ESSENTIAL

Ensure the AI Act captures genuine AI risk

GDV supports the risk-based approach of the AI Act. The framework should protect citizens and fundamental rights while allowing European businesses to develop and deploy trustworthy AI.

For insurance, two issues are particularly important: the definition of AI and the classification of insurance use cases as high-risk.

Keep established statistical models outside the AI definition

The AI Act should distinguish genuinely autonomous or adaptive AI systems from established statistical and actuarial techniques.

Insurance has used mathematical and statistical models for decades to assess risk and calculate premiums. Generalised linear models, linear regression and logistic regression operate according to predefined human designed parameters. They do not independently develop new decision logic after deployment.

These established models should not fall within the AI Act simply because they are computational or use large datasets. Bringing traditional actuarial techniques within the AI framework would create significant additional compliance requirements without addressing the risks that the AI Act is designed to regulate.

GDV therefore supports a clear interpretation of Article 3 that excludes established statistical and actuarial models as they do not meet the substantive characteristics of an AI system.

Apply high-risk classification proportionately

The AI Act currently identifies certain AI systems used for risk assessment and pricing in life and health insurance as high-risk under Annex III.

GDV recognises the importance of ensuring strong safeguards where AI can affect individuals. At the same time, insurance is already subject to extensive European and national requirements governing underwriting, product oversight, conduct, governance, data protection and risk management.

The implementation of the AI Act should therefore take full account of these existing safeguards. High-risk requirements should be applied in a proportionate manner and should not duplicate obligations that are already imposed by Solvency II, the Insurance Distribution Directive and the GDPR.

GDV also supports effective implementation guidance and close coordination between the AI Office, EIOPA and national authorities. Consistent interpretation is essential to prevent divergent supervisory expectations across Member States.

DIGITAL FAIRNESS ACT (DFA): THE NEED TO AVOID DUPLICATION

Strengthen digital fairness without creating a parallel consumer rulebook

GDV supports strong consumer protection in the digital environment. This trust is fundamental to insurance, particularly as more customers interact with insurers through digital channels.

The Digital Fairness Act should build on the comprehensive EU consumer protection framework already applicable to insurance undertakings. This includes cross-sectoral regulation such as the Unfair Commercial Practices Directive, Consumer Rights Directive and Unfair Contract Terms Directive, together with the AI Act and GDPR as well as insurance-specific provisions such as the Insurance Distribution Directive. These rules already provide extensive safeguards for consumers in the digital environment – covering, for example, fair commercial practices, transparency, personalised services, profiling and automated decision making.

In parallel, the EU Kids Act addresses issues regarding the protection of minors in the context of online services.

Avoid duplication, conflicting requirements and an excessive regulatory burden

For insurers, the priority is a coherent framework in which the Digital Fairness Act and other legislation complement each other rather than create overlapping or conflicting obligations. The Digital Fairness Act should address genuine regulatory gaps rather than create parallel requirements for practices already regulated under existing legislation.

Any new obligations introduced through the Digital Fairness Act should be carefully assessed against existing requirements and their cumulative impact. Regulatory change inevitably requires significant investment in implementation, governance and legal adaptation, including uncertainties regarding interpretation to be resolved by the courts. For this reason, legislative intervention should be targeted at demonstrable market failures or consumer harm, ensuring that additional obligations deliver tangible benefits for consumers while preserving legal clarity for businesses.

Protect consumers online while preserving useful digital services

Digital insurance can improve accessibility, customer communication, claims handling and personalised services. The regulatory framework should therefore distinguish between genuinely harmful practices and legitimate digital personalisation.

GDV supports a targeted, evidence-based approach focused on demonstrable consumer harm, with effective safeguards for vulnerable consumers and strong enforcement where needed.

EUROPEAN BUSINESS WALLET (EUBW): A TOOL FOR SECURE AND EFFICIENT DIGITAL BUSINESS INTERACTIONS

GDV supports the European Business Wallet as an opportunity to make digital business interactions more secure and efficient. The proposed framework provides important building blocks, including interoperability with the EUDI Wallet, trusted corporate identity and attributes, electronic signatures and seals, as well as mandate and role-based authorisation.

For insurers, the EUBW should deliver tangible benefits in practical business processes. Verified corporate identity data, attributes and mandates should be usable for customer onboarding and relevant KYC/KYB checks without unnecessary re-verification. The framework should also enable insurers to reliably verify authorised representatives and support seamless end-to-end processes, from corporate identification to digital contract conclusion.

Clear liability and reliance rules should ensure that insurers and other relying parties know when they can rely on verified information, attributes and mandates provided through the EUBW and where responsibility lies if such information is inaccurate, outdated or invalid.

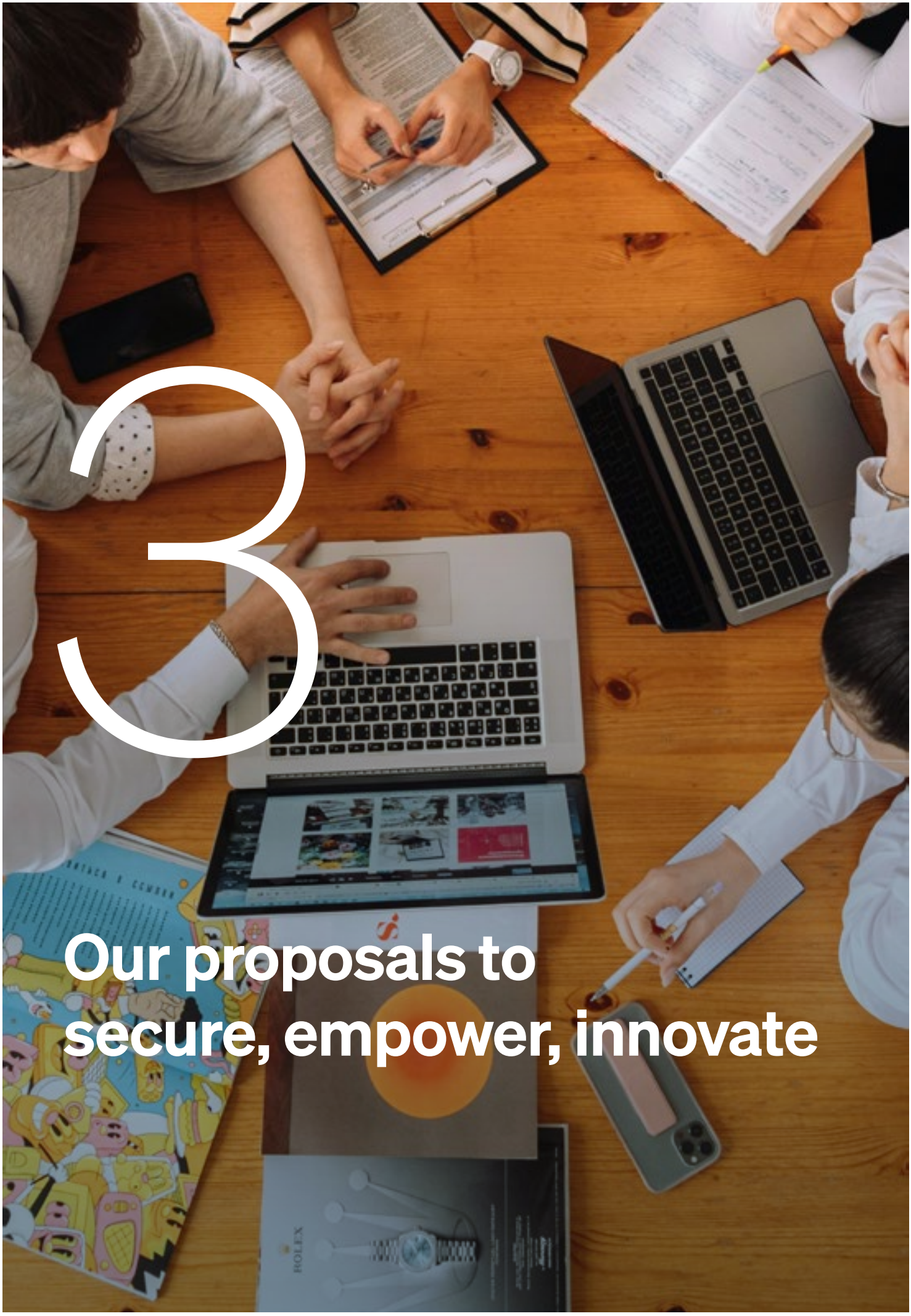
Finally, the EUBW should integrate seamlessly with insurers' existing identification, onboarding and contract management systems and remain interoperable with relevant European and global standards.

CLOUD AND AI DEVELOPMENT ACT (CADA): A FRAMEWORK FOR EUROPEAN DIGITAL AUTONOMY

The Cloud and AI Development Act represents an opportunity to strengthen Europe's digital autonomy by expanding cloud capacity and supporting AI development. As with other digital initiatives, the success of CADA will depend on its ability to complement existing sectoral frameworks rather than the creation of parallel requirements. For insurers, the Act should not impose additional ICT risk management or outsourcing obligations on financial entities already subject to comprehensive sectoral rules.

Instead, CADA recognised assurance levels should serve as optional evidence to support DORA compliance, while Article 31 must remain voluntary for private entities. Furthermore, forced migration to EU based cloud providers must be avoided where insurers can demonstrate full compliance with DORA. This will ensure that European digital autonomy does not come at the expense of global competitiveness and operational resilience.

© GDV 2026



3

Our proposals to secure, empower, innovate

The European Union has already established a comprehensive digital rulebook. The priority should now be to ensure that these frameworks operate coherently, proportionately, and effectively. To this end, GDV proposes the following measures to strengthen legal clarity, improve regulatory consistency, reduce unnecessary duplication and foster innovation while maintaining high standards of consumer protection and resilience.

Digital Omnibus and GDPR – Clarify the rules for responsible data use

- → Align the proposed right to object under Article 88c with the existing GDPR framework and avoid an unconditional right that goes beyond Article 21.
- → Confirm the relative approach to identifiability for pseudonymised data (Articles 4(1) and 41a) and empower the Commission to set technical criteria for assessing re-identification risk.
- → Preserve the simplified framework for automated individual decision-making under Article 22, allowing automated decisions for contract conclusion and performance even where non-automated alternatives exist.
- → Maintain the extended breach notification deadline of 96 hours and the "high-risk threshold" under Article 33 and clarify that the deadline is calculated in working days.
- → Sustain the limitations on manifestly unfounded or excessive access requests under Article 12(5) and lighten the burden of proof for controllers facing abusive requests.
- → Replace absolute restrictions on the processing of sensitive data with a risk-based and proportionate approach, in accordance with the principle of data minimisation. Narrow the scope of the definition of sensitive data.
- → Provide a clear legal basis for processing health data where necessary for the conclusion and performance of insurance contracts, including reinsurance.
- → Clarify the conditions for intra-group data processing to enable effective risk management, compliance and supervisory reporting.
- → Clarify the processing of data relating to criminal convictions where necessary for fraud prevention, regulatory compliance or legal claims.
- → Provide a clear and predictable framework for the use of data to develop and train AI systems.

AI Act – Ensure proportionate and risk-based AI regulation

- → Clarify the definition of AI so that established statistical and actuarial techniques, including GLMs, linear regression and logistic regression, are not captured as they do not exhibit the characteristics of an AI system.
- → Ensure that the classification of AI systems used in insurance reflects the actual risk of the use case and takes account of existing sectoral safeguards.
- → Extend implementation deadlines for high-risk AI requirements where the necessary standards, guidance and supporting infrastructure are not yet available.
- → Remove duplicative assessment requirements where equivalent safeguards already apply under the GDPR or financial services legislation.
- → Ensure effective coordination between the AI Office, EIOPA and national authorities to promote consistent implementation across the EU.

© GDV 2026

Cyber security and DORA – Eliminate overlapping obligations

- → Avoid duplicative requirements between DORA, the Cyber Resilience Act and other horizontal cyber legislation for financial entities already subject to comprehensive sectoral requirements.
- → Establish a single-entry point for ICT and cyber incident reporting, supported by harmonised reporting templates and timelines across relevant EU legislation which is only accessible to the competent authorities.
- → Ensure that new horizontal cyber requirements recognise existing financial sector resilience frameworks rather than imposing parallel compliance structures.

Digital Fairness Act – Build on existing consumer protection

- → Align the Digital Fairness Act with the GDPR, Insurance Distribution Directive, Unfair Commercial Practices Directive and Consumer Rights Directive.
- → Focus new legislation on genuine regulatory gaps and demonstrable consumer harm.
- → Avoid additional sector-specific requirements where equivalent protections already apply to insurers.
- → Ensure that rules on personalisation, profiling and digital interfaces distinguish harmful practices from legitimate digital services that can benefit consumers.
- → Ensure consistency between the Digital Fairness Act and the wider EU digital rulebook, particularly the GDPR and AI Act.

Cloud and AI Development Act (CADA) – Strengthen European digital autonomy

- → Ensure alignment with DORA to avoid additional ICT obligations for insurers.
- → Treat CADA assurance levels as optional evidence for DORA compliance.
- → Maintain the voluntary nature of Article 31 for financial entities.
- → Avoid forced migration to EU based cloud providers where DORA compliance is demonstrated.

European Business Wallets – Guarantee interoperability of frameworks

- → Ensure interoperability with the EUDI Wallet and existing insurer systems
- → Establish clear liability rules for identity accuracy and reliance protection
- → Focus on practical use cases such as digital corporate identity and KYC checks
- → Guarantee technical interoperability with global standards

Conclusion – One coherent digital rulebook

At the October 2025 European Council meeting, EU leaders unanimously mandated the Commission to swiftly propose an ambitious simplification package for financial services. This task should be approached with the same high level of ambition that shaped the Commission's first year in office. In this context, the outlined proposals would reinforce Europe's global leadership in insurance and reinsurance, without changing capital requirements or compromising on consumer protection or financial stability.

GDV calls for EU digital legislation to follow a simple principle: new requirements should complement existing safeguards, not duplicate them. Europe has already built a comprehensive framework for consumer protection, data governance, cybersecurity, operational resilience and artificial intelligence. The challenge now is to ensure that these frameworks remain coherent, proportionate and future-proof.

A regulatory environment that is secure, empowering and innovation-friendly will strengthen consumer trust, encourage investment and enhance Europe's competitiveness in the global digital economy. By focusing on better coordination of existing rules rather than creating overlapping requirements, policymakers can help ensure that innovation and protection reinforce one another.

German insurers remain committed to working with European institutions to build a digital framework that secures trust, empowers consumers and businesses, and enables innovation to thrive across Europe.

By prioritising coherence over complexity, Europe can demonstrate that strong consumer protection, digital innovation and global competitiveness are mutually reinforcing objectives rather than competing ambitions.

© GDV 2026

German Insurance Association
(Gesamtverband der Deutschen
Versicherungswirtschaft e. V.)
Wilhelmstraße 43 / 43 G, 10117 Berlin
Visitor entrance: Leipziger Straße 121
P.O.Box 08 02 64, 10002 Berlin
berlin@gdv.de

© GDV 2026