Insurance Europe Response to Data Union Strategy Consultation

Our reference:	COB-TECH-25-133	Date:	18/07/2025
Referring to:	European Commission Consultation for a European Data Union Strategy		
Contact person:	Danilo Gattullo Senior Policy advisor, Conduct of business	E-mail:	gattullo@insuranceeurope.eu
Pages:	4	Transparency Register ID	33213703459-54

Insurance Europe welcomes the opportunity to provide input to the European Commission on its new EU data union strategy. This position paper is intended to supplement the response provided via the online survey to add greater clarity and context to Insurance Europe's answers.

We believe that a new EU data strategy would provide a significant opportunity for the EU to adopt a future-proof, innovation-friendly framework that supports data-driven business and enables the digital transformation of society, while ensuring appropriate protection for consumers.

Potential consolidation of data legislation

To enable artificial intelligence (AI) and data-driven innovation, the EU must focus on enhancing the usability, coherence and effectiveness of its legislative framework. The proliferation of overlapping legal instruments – including the General Data Protection Regulation (GDPR), AI Act and the Data Act – creates uncertainty about their interplay. Comprehensive and accessible guidelines must be developed to help stakeholders understand how these instruments interact in practice. Such guidance should clarify obligations and rights while facilitating compliance and innovation.

The ongoing digital transformation and integration of AI present significant opportunities for insurers and their customers alike. Innovation and digitalisation are driving forces within the insurance sector. While the current regulatory framework is designed to safeguard consumers, it is equally important to evaluate whether existing rules inadvertently hinder innovation or impose unnecessary barriers for both insurers and policyholders.

- **Automated decision making under GDPR**

For example, the application of **Art. 22 GDPR** regarding automated decision-making is often interpreted narrowly. Some data protection authorities claim that automated decisions cannot be considered "necessary" simply because humans have historically performed such tasks. They draw the conclusion that automated decision-making is not permissible and that an effective consent according to Art. 22 (2) (c) and

Art. 7 (4) GDPR can only be given if the data subject has the opportunity to choose processing by a human being from the beginning. However, such a narrow interpretation of what can be considered *necessary* would prevent insurers and consumers from fully accessing the benefits of new technology.

For instance, an insurance company may offer online motor insurance through a mobile phone app where the consumer can obtain coverage simply by sending a picture of the car and providing the requested data via an app. In this case, the premium is automatically calculated and the contract is entered into when the payment is effective. This is an example of solely automated decision-making that falls under Art. 22 (2) (a). As a safeguard, the data subject has the right to obtain human intervention and ultimately to contest the decision pursuant to Art. 22 (3). To ensure that Art. 22 does not become an obstacle to digitalisation, it should therefore be made clear that it is a right of the data subject and not a prohibition.

- **Interaction between GDPR, the Artificial Intelligence Act and other legislation**

Another example is the interaction between the GDPR and the AI Act. Although Art. 2(7) of the AI Act states that the Act does not affect the application of the GDPR, the concurrent application of both frameworks has resulted in overlaps and inconsistencies – such as the duplication between the data protection impact assessment required under Art. 35 GDPR and the fundamental rights impact assessment mandated by Art. 27 of the AI Act.

There are also risks about fragmented approaches in guidance and supervision, particularly within the financial services sector. Insurers are already subject to a robust EU regulatory framework in terms of both prudential and conduct rules. Under current legislation, insurers deploying AI technologies could be subject to supervision by various authorities, including the relevant data protection authority, the insurance supervisory authority and a designated authority under the AI Act. This approach may result in duplication, inconsistencies and legal uncertainty.

- **Simplify cybersecurity reporting burdens**

Recent EU legislation has also focused on strengthening cybersecurity measures across the Union, focusing on tackling third-party ICT risk, mandating cyber reporting and a renewed focus on testing to increase cyber resilience. Insurers are primarily subjected to the Digital Operational Resilience Act (DORA) as a key sector-specific legislation for the financial sector; however, horizontal legislation also applies, such as the GDPR, the e-Privacy Directive, the AI act and in some instances, the Cyber Resilience Act. The DORA measures are complex and burdensome to implement, which companies have invested in heavily over the past few years ahead of the January 2025 application date. With new cyber reporting introduced, this has led to a duplication of reporting of cyber and data incidents under different pieces of legislation, according to different timelines, as well as reporting to multiple national agencies in some jurisdictions.

Measures to reduce and streamline the reporting burden to avoid unnecessary duplication would be welcomed. In particular, aligning cyber reporting mechanisms across different pieces of legislation and centralising the notifications would help companies avoid duplicating notification submissions. It should also be ensured that across various jurisdictions, the reporting formats are comparable to not complicate the process and to avoid creating differing interpretations of reporting requirements. For instance, clarifying the **interplay of the DORA and Solvency II texts** regarding the reporting of third-party risk would be welcome.

Data availability in the EU

To provide reliable insurance cover, insurers must carry out sophisticated risk assessments and calculations, using various types of information. In particular, insurers carry out statistical analysis of past events to estimate the probability of such events reoccurring. This data analysis is performed at the product design stage, allowing insurers to learn and manage the risks of offering a new insurance policy.

Therefore, for insurers, greater availability of data could lead to improved risk monitoring and assessment, meaning insurance products can be better tailored to each consumer's risks and needs. Developing new or more sophisticated risk models can enable insurers to offer more competitive rates or cover previously uninsurable risks, thanks to increased data availability that could help close existing information gaps.

- **High-value datasets**

Insurance Europe welcomed the introduction of the High-Value Dataset (HVD) Implementing Regulation and its objective to ensure that a common EU-wide layer of public sector datasets is easily and freely available for reuse. Public institutions can provide invaluable sources of data due to the comprehensiveness and the quality of the datasets.

In addition to the relevant datasets described in the Annex to the Regulation, we invite the Commission to also consider making further mobility data available. In particular, data on road traffic analysis, modes of travel used, intermodality as well as safety and security of road traffic would be helpful to provide insurance products that can be better tailored to each consumer's risks and needs.

- **Data Act**

The Data Act is a step in the right direction but not enough to clarify uncertainty concerning access to in-vehicle data. The most fundamental uncertainty facing service providers concerns how vehicle manufacturers will interpret the scope of data subject to the sharing obligations of the Data Act.

Access to in-vehicle data, functions and resources for third-party service providers can support innovation and enable the aftermarket to develop new, competitive services that benefit consumers and drive progress in the sector. As such, sector-specific legislation on access to in-vehicle data, functions and resources could help promote a more dynamic and competitive ecosystem. From an insurance industry perspective, direct access in real-time to vehicle data, functions and resources would enable motor insurers to promote safer and more sustainable driving through tailored insurance solutions like "pay-how-you-drive" policies, which reward responsible driving and reduce accidents. It would also help advance sustainability goals by encouraging lower-emission driving behaviour. Furthermore, the rise of autonomous and connected vehicles presents new risks that insurers need to understand to develop effective coverage.

As a matter of clarity, access to in-vehicle data, functions and resources to support innovation and third-party services is distinct from the evidence disclosure requirements defined under the Product Liability Directive, which should remain limited to their existing scope.

- **Cyber-risks**

Cyber insurance has substantial potential to enhance Europe's cyber resilience. It is a critical tool that companies can use to better mitigate cyber risks. However, lack of available data on cyber risks is one of the primary barriers to the development of the cyber insurance market. Due to the rapid pace at which technology and its associated risks develop, there is very little historical and actuarial data. As cyber risk is not a linear peril, the data on past incidents and losses is crucial to be able to model and better understand the development of these risks in the EU. Data on cyber incidents is being collected as a requirement of various EU legislations, including the Network and Information Systems Directive 2 (NIS2) and DORA. This data could be leveraged to support the insurance industry in increasing its knowledge of cyber risks.

- **Legal basis for AI training**

  Insurance Europe welcomes the Commission’s intentions to focus efforts on creating more synthetic data for AI training. However, to deploy AI effectively, safely and without discrimination, testing and training with real personal data is also necessary.

  AI can help process simple cases more quickly. This means insured individuals receive their benefits faster, and experts can focus on more complex cases. A fundamental problem is the lack of a clear legal basis for processing personal data for AI training purposes. The legal basis provided in Art. 10(5) of the AI Act only applies when data is used to detect bias in high-risk AI systems; it does not apply to General Purpose AI models or non-high-risk AI applications, even though the risk of bias is not limited to high-risk systems.

  In the absence of a specific legal basis for the reuse of data for AI training, such processing must rely on existing GDPR provisions. In practice, this will often have to be based on legitimate interest under Art. 6(1)(f) GDPR, since obtaining further consent after the conclusion of contract is frequently impractical or disproportionately costly. However, this legal basis cannot be used for sensitive data under Art. 9 GDPR. This problem should be further considered since it is in the public interest that AI applications are well trained, unbiased and achieve correct results.

International dimensions of data and data sharing standards

In the context of this consultation, the Commission is seeking stakeholders’ views on the necessity of further safeguarding non-personal data flows, including the need for assessing third-country legal, supervisory, and enforcement frameworks for protecting non-personal data. We acknowledge the importance of ensuring free, safe and trusted international data flows. At the same time, ongoing files like the **Financial Data Access Regulation (FIDA)**, risk granting access to large non-EU platforms or digital gatekeepers, potentially exposing sensitive EU citizen data to third-country jurisdictions and undermining the EU’s ambitions over data sovereignty and strategic autonomy.

We believe that gatekeepers and third-country Financial Information Service Providers (FISPs) should be excluded from accessing customer data under FIDA to avoid risks of market dominance and undermining the development of a secure EU data economy. Allowing such entities to access the financial data of EU citizens would strengthen any dominant position and customer lock-in, contradicting the Commission’s strategic objective on competitiveness and sovereignty.

Finally, there are concerns about ensuring security and protection of that data, particularly if it is shared with third-country entities that may not be able to guarantee the same level of personal data protection as exists in the EU. Facilitating such access, combined with the significant costs to be faced by industry in setting up the framework, could severely impact the competitiveness of the European financial sector.