Digital Omnibus: supporting innovation and consumer protection in the insurance sector

Insurance Europe expresses its support for the overarching aim of the European Commission's Digital Omnibus initiative. European insurers are challenged by a growing patchwork of complex and sometimes inconsistent digital regulations. This regulatory landscape – spanning artificial intelligence (AI), cloud, data protection and cybersecurity – has become particularly complex and burdensome for insurers, thereby diverting valuable resources from innovation and customer services.

Therefore, Insurance Europe welcomes the intention to lessen the administrative and compliance burdens faced by European businesses arising from the implementation of multiple regulations within the EU's digital framework and appreciates the efforts to simplify and streamline existing rules to boost competitiveness. To enable AI and data-driven innovation, the EU must focus on enhancing the usability, coherence and effectiveness of its legislative framework.

Please find below a number of suggested areas where a targeted clarification would help to alleviate some of the burden and costs faced by the insurance sector.

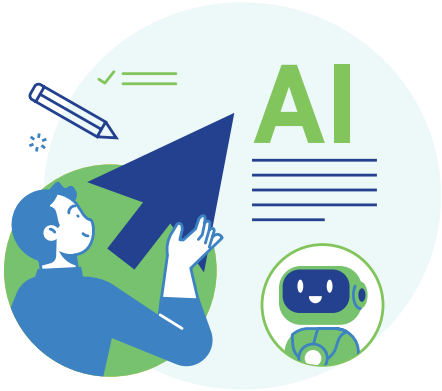
The proposals cover:

- AI
- Data Policy
- Cybersecurity
- European Business Wallet

1. Artificial Intelligence

1.1 Postponement of the date of application of high-risk requirements under the AI Act

The AI Act sets out fixed dates for when the obligations for high-risk AI systems would start to apply. The European Commission has acknowledged the challenges that companies face by not having all of the relevant supporting measures ready on time and it has therefore proposed under its Digital Omnibus proposals to link the start date for these obligations to the availability of harmonised standards, common specifications and Commission guidelines.



The postponement of the application date is a very welcome proposal that could potentially be of huge benefit to European companies. However, there are two clear problems with the current approach:

1. It seems unlikely that the Digital or AI Omnibus proposals will be adopted in sufficient time ahead of the 2 August 2026 deadline under the AI Act, which creates significant uncertainty for industry.
2. The approach that has been adopted in the proposal – with the Commission intending to issue a formal decision confirming when the supporting measures are ready and then announcing that the respective obligations apply from 6 or 12 months later – creates further uncertainty for companies.

Given the pressing need to have clarification of the starting date of the high-risk obligations, Insurance Europe would call on the co-legislators **to carve out these provisions from the rest of the omnibus proposals and to follow a fast-track procedure that provides certainty to the market regarding the application date as soon as possible**. Failure to do so runs the risk that the postponement itself is delayed due to a lengthy legislative process and not secured on time, meaning that European companies will be left with no choice but to try and comply with the obligations despite the absence of the relevant supporting measures. The benefits of any postponement for European companies would therefore be effectively lost.

To create more certainty for companies regarding the future date of application of the high-risk provisions, Insurance Europe also advocates for **setting a fixed date in the future on which the obligations will apply and clarifying that the obligations would apply no sooner than this date**. This has the benefit of ensuring that companies will have sufficient time to prepare with a known starting date, without the constant, day-to-day risk that the obligations will start to apply in 6 months' time. **In the event that the supporting measures are still not finalised by this date, to ensure sufficient legal certainty the date of application should then be 6 months following the Commission decision confirming that the measures are ready, ensuring that there will always be a minimum period of 6 months' notice for companies from when all the supporting measures are finalised.**

1.2 Existing legislative provisions relevant for AI use in insurance

The AI Act is complemented by a wide body of existing EU legislation that addresses many of the potential risks and challenges associated with the development and use of AI in the insurance sector, which is further complemented by national regulatory frameworks. Financial supervisory authorities, such as EIOPA and the European Banking Authority, have recognised that existing financial services legislation already provides robust safeguards in relation to AI use. The Solvency II framework, for example, contains provisions addressing the governance mechanisms put in place by insurers, while principles such as transparency, fairness and ethics are also addressed by rules on conduct of business and disclosure, such as the Insurance Distribution Directive (IDD). The Digital Operational Resilience Act (DORA) will also ensure that AI systems and the platforms that support them are resilient and meet relevant standards of cybersecurity, while many of the provisions of the General Data Protection Regulation (GDPR) already – and will continue to – address the use of AI applications. Examples illustrating the overlap between provisions of the AI Act and sectoral legislation include:

- Article 9 AI Act ↔ Articles 41 and 44 Solvency II, Articles 5–15 DORA, Article 25 IDD
- Article 13 AI Act ↔ Article 18 IDD, Articles 5 and 13–15 GDPR

The Digital Omnibus on AI provides an opportunity for **appropriate clarification, including through the forthcoming EU Commission guidelines, on how existing legislative provisions under the financial services regulatory framework apply to the use of AI and meet the obligations under the AI Act to avoid unnecessary additional burden and duplicative requirements and contribute to further enabling the uptake and deployment of AI in the sector.**

Insurance Europe **calls on the Commission to ensure the prompt publication of this guidance**, with a focus on showing where existing Solvency II/IDD requirements already meet AI Act obligations for insurers, and where additional measures are required, to provide implementation clarity for insurers as early as possible.

In addition, to guarantee clear, consistent, and effective oversight of AI, financial supervisory authorities should be formally designated as AI market supervisors without delay. Furthermore, the AI Office should actively involve financial and insurance supervisors when coordinating the development of secondary legislation and regulatory guidelines. This approach will help avoid fragmented supervision and prevent conflicting interpretations across the financial sector.

1.3 GDPR and AI Act: Removal or simplification of the Fundamental Rights Impact Assessment

The AI Act introduces for a narrow array of AI use cases the obligation to draw up a Fundamental Rights Impact Assessment (FRIA). This document overlaps in many ways with a Data Protection Impact Assessment (DPIA) under the GDPR, thus risking duplicate requirements and unnecessary burdens for companies and public authorities.

Focusing solely on reducing regulatory burdens, **the FRIA requirement could be removed from the AI Act**, thereby creating a level playing field for all AI users and eliminating overlap-risks with existing GDPR obligations. The rule in fact also impacts the **level playing field within the private sector**. Only certain private actors – notably credit institutions and insurers – are subject to this additional compliance burden, while other private deployers of high-risk AI systems are not. Imposing this obligation solely on certain private entities and not others also falling under Annex III is difficult to justify.

[1] See: Supervision of AI: Finding the right balance - European Insurance and Occupational Pensions Authority and AI Act implications for the EU banking sector updated 20/11/2025.

Insurers are already subject to a robust EU financial services regulatory framework (prudential, conduct rules), complemented by national frameworks and by EU legal requirements in a wide range of different areas (fundamental rights, data protection), as well as strict supervision by supervisory authorities. This comprehensive regulatory framework already addresses the potential risks stemming from the use of AI in insurance.

If removal is not possible, it could be specified that a FRIA is only required if no DPIA has been conducted. The key distinction between a FRIA and a DPIA is that a DPIA arises from the GDPR and therefore applies only to scenarios involving the processing of personal data. In contrast, a FRIA is not limited to personal data processing and thus covers broader fundamental rights considerations.

A more flexible approach could be to closely align the FRIA-requirements with the existing DPIA requirements, thus avoiding overlap, duplication and removing unnecessary obligations. It should be possible to integrate the two assessments into a single process and document. Since the AI Office has been mandated to develop a template for an online FRIA questionnaire, if removal is not possible, this form should be designed in a way that minimises duplication with DPIA requirements as far as possible, and should refer to the DPIA for any matter related to the protection of personal data. This should allow an already comprehensive DPIA to also fulfil FRIA obligations, and provide clear guidance on which additional elements, if any, should be incorporated into an existing DPIA to ensure full compliance with FRIA requirements.

1.4 New legal basis for AI bias training

The insurance sector **welcomes the introduction of the new Article 4(a)** by the European Commission allowing providers and deployers of AI systems to process special categories of personal data, when it is necessary to detect and correct bias in AI systems. The current legal provision, Article 10(5) of the AI Act, is too limited in scope, as it applies solely to situations where data is used to detect bias in high-risk AI systems. Extending this legal basis to non high risk AI systems is step towards the right direction and will support the development of more robust and safe AI systems, while remaining subject to appropriate safeguards.

1.5 Registration requirements

The insurance sector **welcomes the Commission's proposed removal of the registration requirement for high-risk AI systems that fall under the exemption in Article 6**, ie where the AI system is used in a high-risk area but does not itself constitute a high risk. The Commission's accompanying Staff Working Document estimates that approximately 222,750 companies might have to register AI systems and suggests total savings of up to EUR 148,500 per year on the assumption that 20% of companies registering high-risk AI systems could be exempted under Article 6(3) of the AI Act. The rate of exemption could be proportionately even higher in the insurance sector, however, as most AI systems that could fall under the high-risk categorisation are used only for preparatory tasks, such as data extraction, document summarisation and triaging. The removal of the registration requirement for such AI systems would therefore help to reduce the operational and cost burden faced by insurers.

2. Data Protection

Insurance Europe welcomes the changes proposed by the European Commission to the EU's data protection framework. As the insurance sector continues to evolve, driven by rapid digital transformation and the growing integration of AI, it is essential that the regulatory environment supports innovation while ensuring robust protection for individuals.

The implementation of the GDPR should avoid creating unintentional barriers to the development and use of such technologies. While strong data protection remains essential, overly restrictive or narrow interpretations of GDPR provisions, particularly when reflected in guidelines from the European Data Protection Board (EDPB), risk undermining innovation in the insurance sector. Legal uncertainty or excessive compliance burdens may discourage the uptake of promising digital tools that could ultimately improve consumer outcomes.

In this context, the Commission's proposals are a step in the right direction. By clarifying certain aspects of the GDPR and seeking to streamline elements of the current framework, the proposals can help provide greater legal certainty for companies while maintaining high standards of data protection.

In particular, the insurance sector welcomes the proposed amendments that:

2.1 Clarify the definition of personal data

The insurance sector supports the proposed revised definition of personal data, as it brings much needed legal certainty to a core concept of the GDPR. The proposal codifies recent CJEU case law, notably *EDPS v SRB*, by confirming that information is not personal data for an entity that does not have the means **reasonably likely** to identify the individual, and that such processing therefore falls outside the GDPR for that entity.

By moving away from an "absolute" interpretation of personal data, this clarification resolves long standing uncertainty and brings the legal framework into line with judicial interpretation. At the same time, it will also strengthen predictability for data controllers, including insurers, when applying pseudonymisation techniques, and will encourage wider use of privacy enhancing measures while maintaining a high level of data protection.

2.2 Introduce a specific legal basis for AI training with sensitive data

The insurance sector supports the European Commission's proposed new Article 88c and Art. 9(2)(k) under the GDPR. Together, these provisions clarify that the training and operation of AI models may be carried out on the basis of legitimate interest, including, where appropriate, by processing sensitive data, provided that robust and proportionate safeguards are in place. The change will guarantee more legal certainty while continuing to ensure a high level of protection for individuals. Legitimate interest in fact remains subject to strict safeguards including purpose limitation, necessity and balancing tests and transparency obligations. This clarification can enable insurers to deliver faster and higher-quality services. For example, AI has the potential to streamline the processing of simple insurance claims, enabling insured individuals to receive their benefits more rapidly. This increased efficiency can allow experts to dedicate their attention to more complex cases, thereby improving overall service quality.

Recommendation for clarification:

The proposed new Article 88c(2) requires the implementation of technical and organisational measures during AI training and operation to ensure appropriate safeguards. We support measures aimed at preventing data misuse, enhancing transparency, and safeguarding personal data throughout the AI lifecycle. However, we have serious concerns regarding the reference to an **"unconditional" right to object**. This goes beyond Article 21 GDPR and would in practice be unworkable. An unconditional objection 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.

Additionally, the restrictions under the proposed new Article 9(5) must also be workable in practice. As currently drafted, the provision appears to require the unconditional avoidance of processing sensitive data during AI training and operation. To ensure a proportionate and operationally feasible framework, we recommend clarifying that sensitive data processing should be avoided **as far as reasonably possible** or, alternatively, linking the obligation to the **principle of data minimisation**, as reflected in Article 89(1) GDPR. This would preserve high standards of protection while still allowing essential and justified processing in clearly defined circumstances.

2.3 Clarify the appropriate legal basis for solely automated decision making

The proposed clarification concerning the "necessity test" in Article 22 is also a positive development. The application of this Article is frequently interpreted restrictively. Some data protection authorities assert that solely automated decisions cannot be deemed "necessary" if similar tasks have previously been carried out by humans. As a result, they conclude that automated decision-making is not permissible under this provision. Furthermore, they maintain that valid consent under Article 22(2)(c) and Article 7(4) GDPR can only be obtained if the data subject is offered the option to have their data processed by a human from the beginning. This restrictive interpretation of necessity inhibits insurers and consumers from fully realising the advantages brought by technological progress.

2.4 Ensure that data breach reporting is more effective

The proposed extension of the deadline for data breach reporting to 96 hours is also to be welcomed. Short deadlines often lead businesses to submit rushed notifications. By giving companies more time, businesses will be able to conduct proper assessments, verify affected systems, and provide more useful information to the competent authorities.

Additionally, ensuring that only high-risk incidents need to be reported eliminates the need to notify breaches that have a lower impact, reducing the number of filings and the burden on compliance teams. By eliminating notifications that are lower risk, authorities can focus resources on incidents that truly warrant intervention.

2.5 Introduce a legal basis for accessing data from a terminal equipment for providing a service requested by the data subject

The e-Privacy Directive entered into force 23 years ago, when many technological innovations (eg connected devices and the Internet of Things) and the services offered in relation to them were not prevalent. As such, its provision on the collection of information from terminal equipment does not stand the test of time. Innovative insurance offerings, such as telematics motor insurance policies, increasingly rely on the processing of data obtained directly from terminal equipment. These devices include telematics boxes installed in vehicles and other connected vehicle technologies, which enable insurers to gather and analyse data essential for providing personalised insurance services.

The collection and processing of such data are currently regulated under Article 5 of the e-Privacy Directive. Under the existing e-Privacy framework, consent serves as the primary lawful basis for accessing and utilising data from terminal equipment. This reliance on consent as the sole basis can present challenges for both insurers and policyholders. The proposed amendment would introduce a legal basis akin to the performance of a contract. This development represents a positive step, as it provides insurers with a more robust and reliable foundation for processing data in connection with telematics-based insurance policies.

2.6 Improves safeguards against abusive requests –

The insurance sector welcomes the proposed extension of safeguards against the abuse of data access rights under Article 12(5) GDPR. Allowing controllers to refuse or charge for access requests that are manifestly unfounded or excessive, including where data subject rights are exercised for purposes unrelated to data protection, is a step in the right direction.

However, important challenges remain. In particular, the burden of proof still rests with the controller to demonstrate that a request is abusive. In practice, this is difficult to meet, as data subjects are not required to justify their requests and controllers often lack the evidence needed to establish abusive intent.

Recommendation

In exceptional cases, disclosure in response to an access request may seriously prejudice the legitimate interests of the controller, for example by compromising fraud investigations or ongoing litigations. To address this, an exemption could be introduced for situations where providing access would clearly impair the establishment, exercise or defence of legal claims, and where the controller's legitimate interest in withholding the information outweighs the interests of the data subject. Such an amendment would further clarify and build on the "rights and freedoms of others" safeguard already set out in Recital 63 while preserving the core objectives of the GDPR.

Further areas that should be addressed:

2.7 Legal uncertainty around special categories of data in (re)insurance

In order to lawfully process special categories of data, (re)insurers must rely on both a lawful basis under Article 6 GDPR and a specific condition under Article 9. The processing of health data is essential for underwriting, claims handling and reinsurance. However, there is no clear legal basis across the EU. Article 9(4) GDPR allows Member States to introduce additional conditions for processing health data, leading to fragmented national approaches and legal uncertainty, particularly where no specific insurance related provisions exist.

In practice, insurers are often left to rely on consent, which is not a reliable or effective legal basis. Obtaining explicit consent can be burdensome, especially for beneficiaries, injured parties and in reinsurance, i.e. where no direct relationship with the data subject exists. Moreover, consent can be withdrawn at any time, undermining legal certainty where health data processing is indispensable to the performance of insurance and reinsurance contracts, thus generating a structural tension between, on the one hand, the requirement to obtain valid consent for the processing of health data and, on the other, fundamental principles of contract law, pursuant to which both parties are expected to perform their respective obligations in the form and within the timeframe agreed. In addition, the validity of consent in insurance contexts could be put into question because health data processing is indispensable for concluding, performing, and managing certain insurance contracts, including claims handling: since such processing is essential to provide insurance services, consent may be regarded as not "freely given". Diverging national interpretations further complicate cross border cooperation, notably for reinsurers. This situation highlights the need for a **clarification of an appropriate legal basis that could be relied upon at EU level for the conclusion and performance of (re)insurance contracts including claims handling**. It would be appropriate to clarify that such processing may be covered by one of the derogations under Article 9 GDPR, such as the establishment of legal claims (Article 9(2)(f)).

2.8 Definition of health data –

The current broad interpretation of health data, which extends protection to any personal data from which health information can be inferred, creates various legal and practical problems. In practice, almost any personal data could be treated as health data if someone could infer health-related information, even when the data itself contained no medical information. This is problematic as it can make the scope of Article 9 unpredictable and detached from the actual risk the data poses to the individual. Clarifying that health data covers only personal data that directly reveal information about a person's health status would make the framework more predictable and usable. A more precise definition would improve legal predictability for controllers and supervisory authorities, enable proportionate risk-based compliance, and support responsible data use in areas such as research and innovation without weakening protection for individuals' core health information.

2.9 Data transfers

Another pressing concern is the continued instability surrounding international data transfers. The GDPR's current framework — particularly following Schrems II — places the burden of carrying out a transfer impact assessment on companies, many of which lack the resources or access to conduct comprehensive legal assessments of third-country legal regimes. In this regard, further simplification measures could be considered particularly for low-risk transfers. For example, the European Commission could develop a centralised, regularly updated European register of legal frameworks applicable in third countries with regard to data protection for international data transfers. Such tool could be helpful for businesses, including SMEs, when carrying out their transfer impact assessments.

3. Data Act

3.1 Business-to-Government data sharing

The insurance sector also welcomes the proposed modifications to the B2G data sharing provisions under the Data Act. The proposed changes introduce greater legal certainty, by better defining the scope of mandatory data sharing. By redefining B2G access from the broad and ambiguous concept of "exceptional need" to the much clearer and narrower threshold of "public emergencies," the proposal reduces the likelihood of broad or unpredictable data-access requests that could lead to compliance risk and operational uncertainty for companies.

3.2 Business-to-Business data sharing

The proposed revision to the Data Act, which would allow data holders to refuse disclosure of trade secrets where there is a high risk of unlawful acquisition, use, or disclosure to third country entities operating under weaker legal safeguards, raises significant concerns from an industry policy perspective. While the objective of strengthening trade secret protection is legitimate, the introduction of a broad concept such as "high-risk of unlawful acquisition, use, or disclosure to third country entities" creates substantial interpretative ambiguity.

The existing safeguards in Article 4 (6) and (8) already establish a clear, proportionate, and sufficiently stringent framework to protect trade secrets without undermining the Data Act's core objective of promoting fair access to data. Diluting this balance by expanding the grounds for refusal would disproportionately strengthen the position of certain, already dominant, market actors who may leverage the provision to deny access to in-vehicle data.

3.3 Public sector data reuse

The Digital Omnibus proposal consolidates the rules on the reuse of both open and protected public sector data by repealing the Data Governance Act and the Open Data Directive and integrating their substance into the Data Act. However, the distinction between the rules applicable to the reuse of open government data and those applicable to the reuse of certain categories of protected data held by public sector bodies (as referenced notably in Article 32w) remains insufficiently clear. While open data is governed by a harmonised re use regime, the provisions relating to protected data largely defer to Member State discretion, without adequately specifying the types of rules that Member States may or should adopt. This lack of clarity risks leading to diverging national approaches, legal uncertainty for data users, and fragmentation of the internal market. The legislation should therefore better define the types of rules Member States may implement, in order to ensure more predictability.

In addition, we recommend deleting Articles 32q(6) and 32y(5), which allow higher charges for data reuse by very large enterprises. Reuse costs should be based on objective criteria such as the volume or nature of data accessed and the costs incurred by public authorities, rather than the size of the company accessing the data.

4. Cybersecurity

Insurance Europe welcomes the European Commission's proposals in the Digital Omnibus to simplify and harmonise cybersecurity and operational resilience requirements across the EU. The insurance sector faces increasing complexity and administrative burden due to overlapping digital regulations, and the introduction of a Single-Entry Point (SEP) for incident reporting, managed by ENISA, is a significant step forward. This mechanism enables organisations to "report once, share many" across DORA, the Critical Entities Resilience Directive (CER) and GDPR, reducing duplication and streamlining compliance processes.

The intention to develop harmonised templates for incident reporting is also a positive development. Consistent templates will help companies operating across multiple frameworks and national jurisdictions to comply more efficiently and with greater legal certainty, minimising the risk of varying interpretations of authorities. The recognition of practical challenges encountered during DORA's first year of implementation, and the linkage of ongoing simplification efforts to the Omnibus workstreams, are further steps in the right direction.

The insurance sector welcomes in particular the following proposed improvements:

4.1 Establishing a Single-Entry Point for incident reporting

- The creation of a centralised reporting channel, managed by ENISA, will allow companies to submit incident notifications once, with the information shared across relevant regulatory frameworks. This approach will reduce administrative burden and avoid duplication, enabling compliance teams to focus on managing incidents rather than navigating multiple reporting systems.
- In terms of the specific design, it is essential that the single-entry point functions as a transmission platform and is not developed into a database. It is equally important that reporting in English is always made possible.
- However, without adjustments to this proposal, a single submission channel will not meaningfully simplify compliance given the persisting differences in reporting timelines and data fields. Where an AI system processing personal data is compromised, notifications would still be required to ENISA under GDPR and to the relevant national competent authority under the AI Act. Addressing these discrepancies is paramount to the success of the SEP.
- There is also a lack of details on how the SEP will impact businesses in practice. The future SEP should make reporting easier, faster, and less resource-intensive for companies. This is all the more crucial as the SEP will serve in times of operational crisis for cybersecurity teams of companies that will be experiencing cyberattacks.
- At present, the implementation timeline for the SEP is unclear, casting doubt on its expected benefits. It is also uncertain how the SEP will interact with existing national reporting frameworks; this should be clarified by the relevant authorities to avoid conflicting obligations.

- The SEP should not evolve into a data bank accessible to ENISA or other authorities. Its purpose should remain limited to streamlining reporting, not expanding supervisory access to operational data.
- The simplification introduced through a SEP must not lead to the creation of an additional interlocutor. ENISA's role should remain strictly that of a transmission channel. Extending its responsibilities risks adding operational burdens for insurers. While analytical or aggregation functions could be useful, they should only be implemented if they do not generate additional workload, complexity, or exchanges with ENISA, as such features could otherwise increase reporting obligations and strain incident-management resources.
- To substantially alleviate the operational burden, the format of ICT incidents reporting templates should be harmonised in order to answer several requirements that are currently requested in several legislative texts (namely DORA, GDPR, etc.).
- In addition, ENISA should be given a mandate to aggregate anonymised data to make it available to a broader range of stakeholders, including the insurance industry. The availability of this aggregated data would enhance cyber insurance coverage, which in turn help to address the cyber risk protection gap.

4.2 Developing harmonised templates for incident reporting –

- The Omnibus signals intent to develop common templates for incident reporting under DORA, CER, and GDPR, moving towards consistency and simplification. The move towards unified templates for incident notifications under DORA, CER, and GDPR will provide greater clarity and consistency for organisations. Standardised templates will help ensure that the information provided is relevant and sufficient for authorities, while reducing the risk of errors and omissions caused by varying requirements. Moreover, it should be possible for multiple parties to fill out reporting templates simultaneously given the difference in deadlines across regulation.

Further areas that should be addressed:

4.3 Risk-based thresholds, proportionality, and definitions –

- While the Digital Omnibus takes steps towards streamlining reporting obligations, further clarification is needed to ensure these requirements are proportionate to the size and risk profile of each organisation. Reporting should focus on incidents that materially affect essential functions, and registers of ICT providers ought to prioritise those supporting these functions. However, the Omnibus currently lacks a proportional approach for low-risk or small entities and does not introduce flexibility or risk-based thresholds for reporting.
- Additionally, there is no refinement or clarification of the definition of 'ICT services', nor does the Omnibus address the efficient use of certifications or audit results for ICT providers. These gaps mean that reporting and compliance obligations may remain unnecessarily burdensome for many organisations, particularly those with lower risk profiles or limited resources.

4.4 Content requirements for intermediate reports

- The current expectation for early estimates of damage or customer data affected in intermediate reports is overly demanding. The Digital Omnibus should reduce the content requirements for intermediate reports on major ICT related incidents, in particular initially remove requirements related to estimates of the amount of damage or customer data affected. In the short time frame of 72 hours, it is necessary to focus on actual ICT incident management rather than statistics. At the same time, this information is often not available at the outset and can be provided in some statistical form later (in an updated intermediate report).

4.5 Duplication and overlap of requirements – CRA-DORA

- The overlap between the CRA and DORA presents serious implementation challenges for the financial sector. The CRA introduces horizontal rules for digital products, whereas DORA establishes a comprehensive resilience framework tailored to the financial sector. The lack of coordination between these frameworks risks creating redundant obligations for financial institutions, leading to a misallocation of resources and, at the same time, contradicting the Commission's goal of regulatory coherence and competitiveness.
- The Digital Omnibus should propose a clear exemption from the CRA (via delegated act, conditions for which are foreseen under CRA Article 2(5)) for financial entities subject to DORA. Financial services offered through digital channels are already subject to DORA, which imposes stringent and comprehensive requirements on financial entities' ICT systems and services.

4.6 A single, harmonised rulebook for outsourcing and third-party risk

- The current fragmentation across technology-related regulations creates unnecessary complexity in risk management and reporting. A harmonised framework would reduce duplication, streamline processes, and ease compliance for companies. The same harmonisation principle should apply to incident reporting. Reporting requirements should be aligned through the Single-Entry Point (SEP) across DORA and other outsourcing/third-party regimes to ensure consistency and avoid parallel reporting channels.
- The Digital Omnibus should strive to harmonise outsourcing rules under Solvency II and third-party risk management under DORA to remove duplication of compliance structures for services that qualify as an ICT service under both measures. It would contribute to simplification and less bureaucracy if compliance with DORA requirements is deemed sufficient in these cases. In the insurance sector, this could also be achieved in a minimally invasive manner by making the existing outsourcing regulations in Article 274 of the Delegated Regulation on Solvency II more flexible. The applicable requirements under DORA are generally more comprehensive. Only the contractual rights to issue instructions and the commitment to comply with corporate policies in Article 274 (4) b) and f) of the Delegated Regulation have no direct equivalent in DORA. Due to the nature of ICT contracts, these are also not necessary. Adding a flexibility clause ('if appropriate') to Article 274 (4) b) and f) of the Delegated Regulation would enable consistent contract design in case services qualify as both – ICT-services under DORA and outsourcing under Solvency II.

4.7 Harmonisation of deadlines

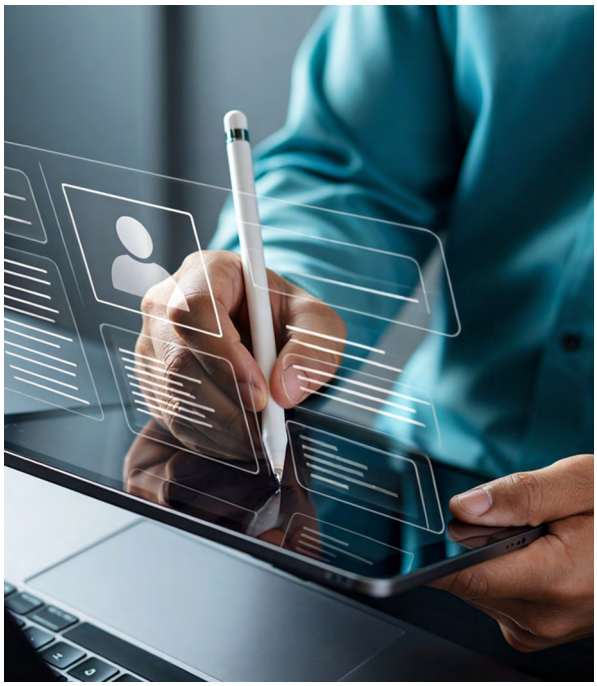
Different deadlines for incident reporting under various frameworks, such as DORA and NIS2, create confusion and increase administrative complexity. Uniform deadlines should be established to streamline compliance, especially considering the already-similar deadlines (NIS2: 24 hours after discovery / DORA: 4 hours after classification and no later than 24 hours after discovery).

4.8 Flexibility in testing requirements

- More flexibility in DORA's testing requirements is recommended, including a modular approach to testing, such as dividing penetration tests into smaller, manageable blocks. The provision of shared testing environments, particularly to support small entities, could be considered on a voluntary basis. These shared arrangements should be designed in a way that fully preserves confidentiality and ensures that testing results or conclusions from other entities are neither disclosed nor made accessible to participants of shared testing.

4.9 Reduce the complexity of the register of information

- The current requirements for the DORA register of information are overly complex and create a significant administrative burden for financial entities. Simplifying the register by reducing mandatory fields and limiting all mandatory fields to ICT services supporting a critical or important function would improve efficiency and enhance data quality. Even if significant simplifications are made, the European Supervisory Authorities should still be able to designate critical ICT third-party providers based on the register of information.
- Examples of simplifications include removing the annual-expense field linked to each contractual arrangement while keeping only the overall annual expense for the ICT provider. For criticality, the level-of-reliance field could be deleted while retaining the indicator on the impact of discontinuing the service. Location-related information could be streamlined by keeping only the location of data at rest and removing the fields on where data is processed and the country where the service is provided. Additional unnecessary elements that could be removed include the notice periods for both the financial entity and the ICT provider, the country of governing law, and the reason for contract termination.



→ Main simplification

Limiting all mandatory fields to ICT services supporting a critical or important function.

→ Other simplifications

Overlapping data elements regarding costs

COLUMN CODE	COLUMN NAME	REMOVE
B_02.01.0050	Annual expense or estimated cost of the contractual arrangement for the past year	Yes
B_05.01.0100	Total annual expense or estimated cost of the ICT third-party service provider	No

Overlapping data elements regarding criticality

COLUMN CODE	COLUMN NAME	REMOVE
B_02.02.0180	Level of reliance on the ICT service supporting the critical or important function.	Yes
B_07.01.0100	Impact of discontinuing the ICT services	No

Disproportionate amount of data elements related to location

COLUMN CODE	COLUMN NAME	REMOVE
B_02.02.0150	Location of the data at rest (storage)	No
B_02.02.0160	Location of management of the data (processing)	Yes
B_02.02.0130	Country of provision of the ICT services	Yes

Disproportionate amount of data elements related to location

COLUMN CODE	COLUMN NAME	REMOVE
B_02.02.0100	Notice period for the financial entity making use of the ICT service(s)	Yes
B_02.02.0110	Notice period for the ICT third-party service provider	Yes
B_02.02.0120	Country of the governing law of the contractual arrangement	Yes
B_02.02.0090	Reason of the termination or ending of the contractual arrangement	Yes

4.10 Lack of practical guidance and harmonisation

- The Digital Omnibus should provide clear and consistent guidance to Member States. It should also address the risk of conflicting national frameworks and should strive to rather complement these frameworks, reporting or otherwise. The Digital Omnibus should harmonise outsourcing/third-party risk rules (e.g., between Solvency II and DORA) and include measures to prevent additional national requirements or duplication within corporate groups. Requirements should avoid duplication, rather than extending DORA requirements to all outsourcing, as well as a register of information for non-ICT third-party providers.

4.11 Insufficient detail on reporting, remediation, and feedback

- The Omnibus should clearly simplify the content of documentation or event qualification and should harmonise submission interfaces and IT tools. There should be clear guidance on remediation, risk assessments, and feedback mechanisms during the reporting process, as well as a template for annual risk framework evaluation.

4.12 Need to establish a centralised repository of subcontractor information at European level

- The Digital Omnibus should support financial entities by establishing a centralised mechanism for collecting relevant information from ICT providers. The introduction of a DORA compliance statement or standardised declaration from ICT service providers under DORA would reduce the administrative burdens of the financial entity.
- It should encourage the establishment of a standard agreement or contract addendum at EU level for DORA requirements to support the industry in delivering on the DORA measures through contract negotiations, without requiring the renegotiation of existing contracts.
- While there is value in centralising information of external subcontractors at EU level, intra group subcontracting arrangements should be excluded from this, as applying these requirements internally would create disproportionate administrative burden without added risk mitigation benefits.

Recommendation

To further reduce regulatory burdens and support innovation, the Digital Omnibus should contain clear risk-based thresholds for incident reporting, harmonise deadlines across frameworks, simplify content requirements for early reports, and ensure that compliance with DORA suffices for outsourcing and incident notification. Greater flexibility in testing requirements and the development of shared testing environments will also help organisations, especially SMEs, to meet regulatory expectations efficiently and effectively.

5. European Business Wallet (EUBW)

As a complementary initiative to the Digital Omnibus, the European Business Wallet (EUBW) can serve as a foundational instrument supporting secure digital identification, authentication, and exchange of company credentials across the EU.

We welcome the European Commission's proposal to introduce the European Business Wallet (EUBW) as a central instrument for secure digital identification, authentication, signature, and the exchange of tamper-proof company credentials. The EUBW can make a significant contribution to the digitalisation and acceleration of business processes, reduce administrative costs, and strengthen security, compliance, and fraud prevention.

For the EUBW to realise this potential, clear, practical, and EU-wide harmonised framework conditions are required. Key prerequisites include close integration with the EU Digital Identity Wallet to avoid parallel structures, a high level of security and trust, reliable governance, and clear liability rules as well as protection of trust for companies and authorities using the system.

For broad market adoption, it is crucial that the EUBW delivers substantial economic value for all stakeholders. From an insurer's perspective, potential benefits include the digital verification of company identity and representation/authorisation rights, efficient KYC and anti-money laundering checks, seamless digital contract execution in B2B and B2G contexts, standardised interactions with supervisory and administrative authorities, and more efficient claims and service processes in corporate client business. Attractive use cases and end-to-end digital processes are more effective than regulatory usage obligations in fostering acceptance and investment readiness.

Another critical success factor is the systematic involvement of public authorities as issuers of reliable digital credentials, particularly for registry information, permits, licenses, and supervisory status. Uniform role and authorisation models for company representations, as well as interoperable technical standards, are essential to enable legally compliant, automated business processes.

The EUBW should be developed as an integral part of a coherent European identity ecosystem, supported by clear governance structures, high security standards, technical interoperability, and sufficient transition.

Insurance Europe is the European insurance and reinsurance federation. Through its 39 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings active in Europe and advocates for policies and conditions that support the sector in delivering value to individuals, businesses, and the broader economy.

www.insuranceeurope.eu
Insurance Europe
Rue du Champ de Mars 23
B-1050 Brussels
Belgium