European Commission Public Consultation on the Digital Fitness Check
Insurance Europe Response

Question
Identify the 3 pieces of EU regulation holding a digital angle that have had the largest impact on your organisation. This will inform the European Commission's scoping and prioritisation of the legal framework to be analysed more in-depth in the Digital Fitness Check. If you are not familiar with the names of specific legislative acts, you may refer instead to policy areas or domains.

- AI Act
- GDPR
- DORA

What are, in your opinion and experience, areas of digital law where there is scope for making key improvements? Be as precise as you can. Please highlight, where possible, the aspects specifically relevant to SMEs.

The EU insurance and reinsurance sector relies on digital technologies to improve efficiency, develop new products and respond to evolving customer and societal needs. A regulatory environment that keeps pace with this transformation is essential. Digital rules should be designed to facilitate innovation and growth, rather than adding layers of complexity that slow progress. The Digital Fitness Check offers an important opportunity to take stock of the cumulative impact of EU digital legislation and to identify areas where rules are overlapping, inconsistent or difficult to implement in practice. In the contribution below, Insurance Europe outlines the key regulatory challenges currently faced by insurers and reinsurers and sets out recommendations to ensure that the EU's digital framework better supports innovation, competitiveness and consumer value.

GDPR: Continued legal uncertainty around special categories of data in insurance
In order to lawfully process special category data, an insurer needs to identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9. The processing of health data is essential for insurers, both for underwriting and claims handling, as well as for reinsurance. In practice, however, there is no uniform legal basis across the EU.

In Member States where no specific national provisions were adopted to regulate the processing of health data in the insurance context, this situation has resulted in significant legal uncertainty for insurance bodies. In the absence of a specific national provision or intervention at national level, insurers are often left with the option of processing health data based on consent. However, using consent as a legal ground for the processing of health-related data has many disadvantages:

- Gathering explicit consent for insureds, policyholders and beneficiaries can be burdensome.
- Gathering consent for beneficiaries or injured parties, who are not formal contracting parties, can be extremely difficult
- Reinsurers do not always have a direct contractual relationship with the data subjects whose health-related data is being processed, making it difficult to obtain their consent.
- Once obtained, consent can be withdrawn at any time; consent is hence not a sufficiently reliable and efficient legal ground for the performance of an insurance contract.

A structural tension can be observed 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. Within the framework of (re)insurance contracts, (re)insurance undertakings acting as data controllers must therefore

reconcile the reliance on consent for the processing of health data — particularly in the context of claims handling — with their overarching contractual duty to assess and settle claims. This interplay may give rise to significant operational difficulties and compliance risks. The absence of consent may constitute an impediment to the proper performance of contractual obligations (such as the claims handling process), while, conversely, the need to proceed with the settlement of a claim despite the lack of consent may expose the data controller to the risk of unlawfully processing health data.

Furthermore, the validity of the consent could be challenged as the conclusion and performance of certain insurance contracts as well as the execution of the contracts (i.e. insurance claims) is simply not possible without the processing of health-related data. Given that the processing of health data relating to policyholders — or to other natural persons involved in the performance and fulfilment of insurance obligations — is essential, in certain (re)insurance contracts and/or at specific stages of the contractual relationship, for the provision of insurance related services, the requirement for consent to be "freely given" risks to be considered invalid.

Without voluntary consent, it may therefore occur that the insurer, in the absence of an appropriate legal basis, finds itself unable, for example, to process a private health insurance claim statement. Paradoxically, at the very moment when the insured brings a legal action against the insurer for payment of those private health insurance benefits, the insurer is permitted to process the health data for the establishment, exercise or defence of legal claims pursuant to Article 9(2)(f) GDPR and to pay out the benefits.

Diverging interpretations among Member States also create significant problems in cross-border collaboration, especially for reinsurers, who need access to health data from other countries without direct contact with the data subject. There is therefore a need for a clarification of the **right legal basis at EU level for the processing of health data for the conclusion and performance of (re)insurance contracts.**

GDPR: Lawfulness of processing

The requirements for the lawfulness of processing form an essential part of data protection. However, there are clearly challenges in certain sectors. For example, In insurance, personal data is processed not only for policyholders but also for insured persons, beneficiaries, or injured third parties, who are not formal contracting parties. Although insurers have contractual obligations toward these individuals, processing often needs to rely on legitimate interest - which leads to a certain degree of uncertainty and compliance burden - rather than contract performance, since only the policyholder is party to the contract. It is therefore proposed the matter to be further assessed, or at least explained in a guideline, so it also covers persons who "derive rights from" a contract.

GDPR: Codes of conducts

Insurance Europe supports the intention behind the proposed amendments under Omnibus IV that promote the development of codes of conduct and certification mechanisms. However, experience has shown that these tools have seen limited adoption across the EU due to high requirements imposed by the EDPB guidelines and long and complex approval processes by the national authorities. To date, very few codes of conduct have been approved, demonstrating that the process is both underutilised and unworkable in its current form.

A key barrier lies in the requirement to establish an independent monitoring body with both functional and legal independence. In many cases, such bodies are not yet in place and must be created from the ground up. Furthermore, the requirements for codes of conduct and their monitoring set out in the EDPB guidelines exceed the provisions of Articles 40 and 41 GDPR and can only be implemented with considerable effort. This process introduces significant delays, uncertainty and discourages industry initiatives.

To promote further developments of codes of conduct, the establishment of monitoring bodies should be made optional as supervision of EU data protection rules ultimately should remain a responsibility of the relevant

national data protection authorities. It should also be ensured that no requirements are imposed beyond those set out in Articles 40 and 41 GDPR.

Finally, the use of approved codes should offer tangible incentives for adherence, such as reduced exposure to sanctions or the possibility of mitigating penalties for participating entities. In this context, data controllers that comply with established codes should benefit from more favourable treatment, reflecting their proactive efforts to ensure compliance with data protection obligations.

GDPR: Data Processing Agreements

It is recommended that Article 28 GDPR, which regulates data processor agreements, be significantly streamlined. The current provision imposes extensive formal requirements on the contractual relationship between data controllers and data processors, which may be considered excessive and not strictly necessary given the overall regulatory framework.

The accountability of the data controller is already well established throughout the GDPR and cannot be delegated through the use of data processors. The manner in which controllers ensure compliance when engaging processors should be left more to their discretion, provided the overarching obligations of the GDPR are met.

Article 28(3) mandates the use of a contract or legal act to govern the controller–processor relationship. While it is appropriate to require measures that prevent processors from using personal data for their own purposes or in ways inconsistent with the controller's instructions or applicable law, such requirements could be addressed more efficiently. In particular, the specification of instructions for data processing, as outlined in Article 29, may be sufficient in practice. These instructions can be incorporated into existing contractual arrangements with suppliers, which often already include relevant compliance, audit, and enforcement provisions.

In practice, the current requirements of Article 28 result in a disproportionate use of resources in drafting and negotiating data processing agreements, many of which add limited substantive value. These agreements frequently replicate standard templates without enhancing legal clarity or enforcement capability. Moreover, in certain sectors, particularly those involving large technology providers, it is often the processor who dictates the terms of the agreement, leaving the controller with minimal negotiating power. This dynamic further reduces the practical utility of the detailed formalities imposed by Article 28. A more flexible, principles-based approach could achieve the same regulatory objectives without imposing unnecessary administrative burdens. This also challenges the demand for control of processors, including sub processors, throughout the supply chain, which is reflected also in other parts of the digital legislation. Hence, it should be addressed broadly in relation to the digital fitness check and feed into a general discussion on 3rd part liability, including certifications.

GDPR: Records of Processing Activities

Insurance Europe welcomes the Commission’s intention, as reflected in the Omnibus IV proposal, to ease the obligations related to records of processing activities for small mid-cap companies. That said, the proposed approach remains too narrow. In Insurance Europe’s view, company size is not an appropriate proxy for determining record-keeping obligations. Instead, the focus should be on whether specific processing operations are likely to pose a material risk to data subjects. A more proportionate approach could include narrowing the scope of information to high-level elements—such as the main purposes of processing, the types of data and data subjects involved, and data recipients—or excluding routine, low-risk processing activities from record-keeping obligations altogether.

GDPR: Clarification on criminal conviction data (Art. 10)

The insurance industry highlights the need to clarify the application of Article 10 GDPR so as to allow, under appropriate safeguards, the processing of personal data relating to criminal convictions and offences where this is necessary for supervisory compliance, fraud prevention, claims handling, and the enforcement of legal claims in the course of insurance activities.

According to Article 10 GDPR, the processing of personal data relating to criminal convictions and offences based on Article 6(1) GDPR must be carried out only under the control of official authority, or when the processing is authorised by Union or Member State law.

The insurance industry is dependent on the processing of personal data relating to criminal convictions and offences.

Examples:

- In certain Member States, insurance undertakings are required to check the reputation of persons who have a management or other key function, as well as of insurance intermediaries. They have to request certificates of good conduct or comparable documents which show whether a person has a criminal conviction.

- Insurance companies may gain knowledge of data relating to criminal offences during the performance of an insurance contract. This is evident in criminal liability insurance. Other examples include traffic offences in motor third-party liability insurance and acts of arson in home insurance.

A legal basis pursuant to Article 6 GDPR exists in the cases mentioned above. There is legal uncertainty, however, as to whether the requirements of Article 10 GDPR are fulfilled.

Furthermore, undertakings must be able to discourage fraud against them. The GDPR explicitly recognises that the processing of personal data for the purpose of preventing fraud constitutes a legitimate interest of the data controller concerned. Finally, the processing of personal data relating to criminal convictions and offences must also be allowed in order to enforce claims under civil law that result from criminal activities.

GDPR: Intra-group data transfers

To facilitate intra-group transfers the establishment of a clear legal basis under the GDPR for intra-group data processing, in particular for special categories of personal data under Article 9 GDPR should be considered. In the insurance context, data sharing is essential for group-wide risk management, compliance, reinsurance and supervisory reporting.

To improve efficiency, tasks are delegated and centralized within insurance groups – as in other industries. Yet, the GDPR treats intra-group data transfers as if between separate entities. Beyond administrative purposes, only two legal frameworks apply depending on the roles of the entities involved: Article 28 GDPR if there is a controller–processor relationship, or Article 26 GDPR if the entities are joint controllers. Both require additional agreements between group entities and an additional legal basis for intra data transfers at least between joint controllers. This adds bureaucracy and delays customer services.

Article 6(1)(f) GDPR cannot justify processing sensitive data and therefore cannot serve as a legal basis in such cases. Obtaining consent from all customers is impractical and would also unnecessarily strain customer relations: frequent consent requests feel disruptive, and could rode trust- especially without clear benefit.

Cyber incident reporting under DORA

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).

There is a need to harmonise incident reporting requirements (under DORA, GDPR, NIS2). In particular introduce a unified classification model to better alignment incident classification criteria. For example, the criteria for

classifying critical incidents under DORA are not aligned with those under NIS2; moreover, a single event could fall under multiple regulations (e.g., DORA, GDPR, NIS2) but be assigned different severity levels, resulting in inconsistent reporting.

Avoid duplication of requirements under various legislative acts

DORA establishes a harmonised, directly applicable EU framework for ICT risk management and ICT third-party risk and should therefore operate as *lex specialis* for ICT-related outsourcing in the insurance sector. Applying Solvency II outsourcing rules in parallel to the same ICT arrangements creates duplicative—and potentially inconsistent—requirements, increasing compliance burden without a corresponding prudential benefit. To ensure a coherent single set of ICT standards and effective supervision, ICT outsourcing should be assessed under DORA, with Solvency II reserved for non-ICT outsourcing and broader governance considerations.

A practical example is Article 28(3), which requires notifying the competent authority of any planned ICT arrangement supporting critical or important functions, or when a function becomes critical or important. The CAA in Luxembourg for example has not issued guidance on how this should be done, and today this information is assumed to be captured under Solvency II processes, but definitions and concepts are not fully aligned with DORA. Some harmonisation and clarification would therefore be helpful.

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.

Additionally, it would significantly ease the completion of the register if the European supervisory authorities (ESAs) maintain central reference data about companies based on the entered LEI codes. By linking registration to the LEI system, basic company data can be automatically retrieved and updated, minimising errors and ensuring that information is always current. This would not only reduce the administrative burden for companies but also improve data quality and traceability across the EU financial sector. It is also recommended to conduct an analysis of the potential savings that the EU financial sector could achieve through a common solution, compared with the costs for the European supervisory authorities (ESAs) to establish and operate such a system. Such a cost-benefit analysis would provide a solid basis for the decision to implement a common European ICT register

Clarity regarding expectations for financial institutions' risk assessments and due diligence

To ensure effective and consistent implementation of the new requirements for risk assessment and due diligence, more precise and operational guidelines should be developed for how financial institutions should approach these processes. It is crucial that expectations for risk assessments and due diligence are not described only in general terms, but are concretised so that institutions have a clear understanding of which elements must be included and how the principle of proportionality can be applied in practice. This will help reduce uncertainty and room for interpretation, ultimately lowering administrative burdens and ensuring that resources are used where they create the most value. One way to streamline risk assessment and due diligence processes could be through binding guidelines or by establishing a library of examples, which over time will lead to more coherent assessments and processes.

At the same time, differences in institution size, complexity, and risk profile should be taken into account, so that smaller and less complex institutions are not subject to disproportionately extensive requirements. Finally, a continuous dialogue between authorities and the industry should be established to ensure that the guidelines remain relevant and up to date in line with technological developments and evolving threat landscapes. Particularly, contracts with the appointed CTPP's should be based on standardised due diligence processes.

Simplified requirements for subcontractors of ICT services supporting critical or important functions
DORA requires that all security and risk-management obligations for ICT providers supporting critical or important functions also apply to their subcontractors. However, the additional detailed contractual clauses and extensive subcontractor-level due-diligence duties in Delegated Regulation 2025/532 create overlap and double regulation without necessarily improving actual security. We recommend clarifying that financial entities can meet their obligations by ensuring contractual flow-down of requirements to subcontractors and by overseeing that the main ICT provider has adequate processes and controls in place. Additional independent due diligence at subcontractor level should only be required where specific risks or transparency issues are identified. This approach aligns with the principle of proportionality and reduces unnecessary administrative burdens without weakening security.

Adjusted frequency of automated vulnerability scanning and assessments
The required frequency of automated vulnerability scanning and assessments as specified in article 10 of the delegated act specifying ICT risk management does not allow companies to act properly on the results of. The work involved in prioritising, testing, and implementing remediation measures – if needed - is far from completed within a week, where a new scan result already requires attention. The requirement risks undermining the purpose of vulnerability scanning. It may become scanning for the sake of scanning, rather than scanning to remediate vulnerabilities. We recommend that the frequency of vulnerability scanning on ICT assets supporting critical or important functions is adjusted, for companies to be able to focus on implementing the measures needed to effectively remediate identified vulnerabilities.

Voluntary certification of CTPPs
A harmonized EU-level certification regime for CTPPs should be introduced to confirm compliance with DORA's contractual and security requirements and ensure EU-based data-fencing. Such certification would allow financial entities to rely on a single assessment, significantly reduce administrative burdens, strengthen legal certainty, and create a "plug-and-play" model where certified providers can demonstrate compliance upfront. This would also incentivize ICT providers to opt into enhanced oversight and align with the Cybersecurity Act's certification framework.

Developing standard agreements for ICT contracts
Following DORA's entry into force, many financial institutions experience that ICT providers insist on delivering their services under their own standard terms, which are often not aligned with the regulatory requirements imposed by DORA. This creates significant challenges for institutions, as they must negotiate and adapt contracts to ensure DORA compliance, which is both resource-intensive and complex. To ease this burden, it is recommended that, similar to the standardized data processing agreements under the GDPR, a standard agreement or contract addendum be developed at the EU level that can be incorporated into ICT service contracts. Such a standard agreement should be designed to cover both general ICT services and ICT supporting critical or important activities, ensuring that providers' terms comply with DORA requirements. This would not only reduce the administrative and legal burden for financial institutions but also promote a more consistent and efficient implementation of DORA across the sector.

Simplification and proportionality in documentation requirements
The scope of DORA's documentation requirements is perceived as very broad and administratively heavy, particularly for smaller or non-critical ICT services. This can create unnecessary burdens without a corresponding gain in resilience. We recommend applying the principle of proportionality so that simple or non-critical ICT services are exempt from full contractual and DORA-specific documentation. Furthermore, the use of standard agreements or addenda, inspired by GDPR's standard contractual clauses, should be promoted for general ICT deliveries to reduce the negotiation burden.

Harmonization of deadlines: Set uniform deadlines for reporting incidents to avoid confusion between different legal acts (e.g., DORA vs. NIS2).

More flexibility in testing requirements under DORA:

- **Modular approach to testing**: Allow insurance companies to divide testing (e.g., penetration tests, recovery scenarios) into smaller, more manageable blocks.
- **Shared testing environment**: The regulator could offer or coordinate shared testing platforms for smaller entities. This proposal would therefore be specifically relevant to SMEs.
- **Proportionality of requirements**: Take into account the size and risk profile of the insurance company when determining the scope of testing. This proposal would therefore be specifically relevant to SMEs.

General improvement of digital rules

Conditional Entry into Force of Legislation

Rapid clarification of the specific scope and concrete implementation of new digital regulation would significantly reduce compliance-related costs for companies and help ensure that the intended implementation—and thus the necessary protection—is in place from the outset. A lack of clarification creates barriers to the use of digital technologies, as clearly illustrated by the AI Act, where experience from the financial sector in particular shows that AI projects have been put on hold while awaiting the necessary clarification to ensure that they can be implemented correctly from the start and are compliant with the regulation.

There is therefore a general need to introduce a conditional entry into force for new digital regulation. This should be understood to mean that the entry into force of the regulation is conditional upon the necessary supporting documents—such as delegated acts, guidelines, and standards—being ready and finally approved. The availability of the necessary guidelines, standards, RTSs, etc. is crucial for reducing the resources companies must spend on building the compliance required to meet the legislation, and for ensuring that the legislation is complied with at the appropriate level and thus provides the intended protection.

Functional Equivalence of overlapping legislation

Horizontal legislation should provide for a mechanism enabling sector-specific regulatory frameworks to operate as a form of procedural *lex specialis* where they pursue the same regulatory objectives and deliver safeguards equivalent to those required under the horizontal framework. Activation of such a mechanism should be subject to validation by the relevant EU-level competent authority and remain conditional on compliance with any horizontal obligations that are not fully covered by the sectoral regime.

A clear example is provided by the interaction between Solvency II and the AI Act. Solvency II already establishes comprehensive obligations for insurance undertakings in areas such as governance, risk management, and internal control systems. These requirements substantially mirror the obligations applicable to high-risk AI systems under the AI Act.

Where an insurance undertaking subject to Solvency II deploys a high-risk AI system, it should therefore be possible for Solvency II processes—addressing equivalent risks relating to model governance, risk controls, and oversight—to substitute for, or complement, corresponding AI Act requirements. While elements of this approach have been recognised in specific provisions of the AI Act, there is currently no overarching mechanism that would systematically address the remaining areas of overlap between the horizontal regulation and sector-specific regimes.

Introducing such a mechanism would help limit duplicative obligations, avoid unnecessary regulatory layering, and promote proportionality, while enhancing overall regulatory consistency. The proposed approach would be based on principles of functional equivalence and regulatory complementarity. EU-level competent authorities should be empowered to assess equivalence, acknowledge complementarities, and define the conditions under which sectoral rules may replace or supplement horizontal requirements in additional areas.

High-Quality Legislation and Sound Legislative Processes

The Commission should place strong emphasis on strengthening the quality of legislation in future digital regulation. The increasing volume and complexity of regulation have led to significant overlaps between sector-specific legislation, horizontal legislation, and product legislation, creating unnecessary burdens for the insurance and pensions sector. There is a need for a more principles-based approach, under which new regulation is introduced only where necessary and where systematic assessments are carried out to determine whether sector-specific and product legislation can replace requirements in horizontal regulation—or vice versa. Simplification is not about lowering standards, but about more effective regulation that supports innovation, competitiveness, and growth. At the same time, it is essential that the Commission consistently carries out thorough impact assessments that address costs, proportionality, unintended effects, and international competitive conditions, and that realistic implementation deadlines are set so that the rules can be complied with effectively without unnecessary administrative burdens.

Question

To what extent do you perceive overlaps, conflicts, or redundancies between the EU digital legislation and sector-specific EU regulations in your area of activity? Please provide examples and elaborate on aspects you find problematic.

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. Existing financial services legislation ensures a robust regulatory framework, with many provisions that already address identified risks in relation to the use of AI. 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). 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.

Particularly important is also 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.

As part of the Digital Fitness Check, the interaction between GDPR and e-Privacy should be further evaluated. While the Digital Omnibus proposal seeks to clarify the interaction between the GDPR and Article 5(3) of the ePrivacy Directive, de facto there are two parallel regimes depending on whether data accessed from terminal equipment is personal or non-personal. However, in practise it is not always easy to distinguish between personal data and other data in this context. Hence, the GDPR and the e-Privacy-directive probably need to be applied in parallel. As part of the Digital Fitness Check, the interaction between GDPR and e-Privacy should be further evaluated. One possible solution could be to align the use of all data from terminal equipment with Art. 6 GDPR legal bases therefore avoiding parallel regimes.

Considering the DORA regulation, there should be an improvement in all regulations related to proportionality, thus making the regulation more accurate to market reality and avoiding excessive charges to medium and small sized undertaking.

Some special fields where this proportionality could be developed would be:

2) Register of *all* ITC providers; could simply prioritize those providers supporting essential functions.
2) Incident notification: again, only incidents affecting essential functions should be prioritized.

Rules regarding outsourcing and different deadlines for reporting incidents (see answers to previous question for more detail).

The overlap between the Cyber Resilience Act and DORA presents serious implementation challenges for the financial sector. The CRA introduces horizontal rules for digital products, whereas DORA already 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. There should be 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.

Challenges and overlaps between AI Act and GDPR

Several key functions or foundational elements for AI implementation may create challenges in relation to the GDPR, which was introduced before the current wave of new AI tools and applications. The following areas have been identified as potential challenges:

- Data minimization: The GDPR requires that the collection and processing of personal data be minimised, whereas the AI Act emphasises that AI systems require large, diverse, representative, and as complete as possible datasets to function accurately, fairly, and to minimise bias. These objectives conflict: limiting data protects privacy but can at the same time reduce AI quality and precision. To ensure trustworthy AI, further clarifications or specific provisions are needed to explain how data minimisation interacts with the objective of building responsible AI. Data and data governance: In relation to Article 10(a) of the AI Act (Data and Data Governance), there is a need to clarify the relationship between the objectives of the AI Act and the GDPR principles of data minimisation and purpose limitation. Overlaps should be addressed, and measures should be defined to ensure complementarity between the two regulatory frameworks.
- Post-Market Monitoring, Article 17(1)(h) and Article 72: With regard to the AI Act's post-market monitoring requirements, it must be ensured that there is no risk of unlawful processing or disclosure of personal data under the GDPR. To avoid unnecessary burdens, post-market monitoring requirements should be reviewed to eliminate uncertainty regarding GDPR compliance.
- Post-Market Monitoring and the Right to Erasure: Additional clarity is needed on how the requirements in Articles 17 and 72 of the AI Act are to be handled in relation to the data subject's right to erasure
- Fundamental Rights Impact Assessment: Overlap with GDPR and Financial Sector Regulation: The AI Act introduces a requirement to conduct a Fundamental Rights Impact Assessment (FRIA) for certain AI applications. This assessment overlaps in many ways with a Data Protection Impact Assessment (DPIA) under the GDPR, as well as sector-specific requirements in financial regulation (e.g., the Insurance Distribution Directive and the Product Oversight and Governance (POG) requirements for insurance undertakings and distributors). This overlap risks creating duplicate obligations and unnecessary burdens for businesses.

Question

What are possible negative consequences of the application of digital EU legislation for cross-border trade with non-EU countries?

GDPR: Cross-border data transfers

There 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.

Unfortunately, the data protection authorities do not apply the **risk-based approach** inherent in the GDPR in this respect. This often makes solutions that are very low risk in nature, such as business video-conference solutions, much harder than they should be. Art. 24 and 32 GDPR provide for a risk-based approach to the determination of technical and organisational measures for the protection of data subjects. Although this risk-based approach is not explicitly stated in Chapter V, it should be made clearer, e.g. through EDPB Guidelines, that it also applies here without restriction. Further simplification of transfers of personal data to third countries should be considered particularly for low-risk transfers.

Furthermore, it should be ensured that the requirements on the Binding Corporate Rules (BCRs) are scaled back to what is strictly required by its Art. 47 GDPR. The EDPB's recommendations 1/2022 expanded the requirements that had previously applied to Controller BCRs (see WP 256 and WP 264 of the Article 29 Working Party) after only a short period of application. They now must reflect the full range of GDPR requirements. In addition, BCRs must include a wide array of supplementary measures that go beyond the requirements of Article 47 GDPR. These extensions significantly exceed what is necessary to implement the Schrems II ruling. Above all, the lengthy approval process makes BCRs increasingly unattractive in practice as a tool for data transfers to third countries within corporate groups.

Question
What areas, if any, do you perceive as incoherent and unclear in terms of concepts used across different laws, definitions, or scope of the rules?

The Digital Operational Resilience Act (DORA) overlaps with Article 274 of Commission Delegated Regulation (EU) 2015/35. Clarification is needed for physical on-site inspections of cloud service providers. Also more efficient use can be made of recognised certification and audit reports (preventing duplicating audits by financial entities); Clarification on how DORA relates to Solvency II (which rules should take precedence) is also needed.

With regard to DORA, it is recommended that the DORA reporting is streamlined and that a more proportional and efficient DORA application is enhanced. The third-party risk management of DORA should be aligned with the outsourcing rules in Solvency II and guidance should be aligned to avoid confusion for financial entities (because of the large amount of regulatory documents such as the DORA Act, Delegated Acts, Q&A's on European level, Q&A's on national level etc. Also, financial entities can be assisted by establishing a centralised repository of subcontractor information at European level. A standard contract addendum at EU level for DORA requirements can help financial entities to make their contracts DORA-compliant. In addition, more efficient use of recognised certifications and audit results of critical ICT service providers to avoid duplication of audits could be helpful.

Question
In what areas, if any, do you consider that changes could be made to optimise the cumulative impact of the rules? In particular, where do you identify, in practice, that obligations in different rules lead to duplications of costs or processes?

Significant resources are devoted to preparing and regularly updating risk assessments under Solvency II, DORA, the GDPR, the AI Act and other regulatory frameworks. To reduce duplication and administrative burden, standardized templates and tools for such assessments should be made available on a continuous basis, enabling companies to conduct evaluations without having to assess the regulatory compliance of the tools themselves

We observe significant overlaps in digital regulatory requirements related to risk management across the AI Act, GDPR, CRA, DORA, Solvency II and the Insurance Distribution Directive (IDD). Clarification of the interfaces and

interaction between the AI Act's high-risk requirements and these frameworks would be beneficial, in particular with regard to the following areas:

1. Accuracy, robustness, and cybersecurity (Article 15)
2. Risk management system (Article 9)
3. Data and data governance (Article 10)
4. Technical documentation (Article 11)
5. Transparency and record-keeping (Articles 12–13)
6. Human oversight (Article 14)
7. Quality management system (Article 17)
8. Post-market monitoring (Articles 17 and 72)

Clarifying these interfaces would reduce overlap, avoid duplicate obligations, and improve regulatory coherence for companies operating across multiple EU digital and sectoral frameworks.

Question
Are there areas of digital law where you currently identify a disproportionate administrative burden stemming from reporting obligations?

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).

The insurance sector welcomes the extension – proposed in the Digital Omnibus - 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. Moving forward, the European Commission should consider whether also other data subject rights could be potentially abused and may need refinement. In practice, the increasing deployment of AI has facilitated the exercise of other rights, sometimes in ways that display abusive elements. As a result, the already high compliance pressure, stemming from the current regime on data subject rights, could further intensify.

Reporting obligations across regulatory frameworks
The insurance sector is subject to extensive national and European reporting obligations, each requiring submission through different systems. As a result, companies must navigate a wide range of reporting processes across regulatory frameworks, recipients, platforms, and technical solutions.

We recommend that the Commission conduct an analysis of how companies' administrative reporting burdens can be reduced. A coordinated EU-level project should be launched to analyze reporting requirements across the European Commission's Directorates-General and European supervisory authorities. We see significant potential in assessing whether data requested in one report could be derived from other existing requirements—possibly submitted to another authority. Authorities should therefore be required to consider whether the data they request is already available or whether other existing sources can meet their needs.

We therefore call on the European Commission to take responsibility for managing the overall effect of national and EU-level reporting obligations across different systems. The Commission should set minimum requirements for data reuse and ensure that authorities, to the greatest extent possible, use existing data before imposing

new reporting obligations. A cross-institutional approach is essential to avoid double reporting and unnecessary administrative burdens. To achieve this, authorities need a clearer and more coherent understanding of the full scope of data that companies are required to report—across supervisory authorities, tax authorities, and statistical requirements. Only with such an overview can real simplification take place.

Incident Management and Reporting Across Regulatory Frameworks

A single incident can potentially trigger multiple parallel and overlapping reporting processes, creating unnecessary duplication and increasing the risk of non-compliance. An insurance company may be required to report an incident to authorities under the following frameworks:

- **GDPR:** Notification of a personal data breach to the data protection authority within 72 hours (extended to 96 hours in the Digital Omnibus).
- **AI Act:** Reporting of an incident or malfunction within 15 days.
- **DORA:** Reporting of major ICT incidents within 4 hours.
- **CRA (if applicable to the financial sector):** Early notification of a vulnerability or incident within 24 hours.

In addition to significant resource costs for companies, the fragmented incident reporting rules require duplicative work, as deadlines and reporting obligations are not streamlined. Companies must spend critical time ensuring compliance rather than addressing the incident or vulnerability itself. The European Commission has already proposed, in the Digital Omnibus, the creation of a single reporting platform. The initiative aims to ensure that security incidents across multiple frameworks are reported once centrally, following the *report once, share many* principle, and that reporting templates are harmonised. In practice, this would allow companies to report centrally at the EU level instead of to multiple national authorities. There is a clear need for the Commission to streamline reporting processes and criteria - particularly deadlines and taxonomie - across digital legislation. A single, harmonised reporting process would significantly reduce compliance costs for companies and free up resources for actual incident management and mitigation.

Question

What challenges do you identify in the governance structures of the digital rules?

There are concrete 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.

To guarantee clear, consistent, and effective oversight of AI, financial 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.

Question

Please share any other remarks that you find important for the Commission to take into account in conducting the Digital Fitness Check. Please share any evidence, data, practical examples and analysis.

Complementarity Between DORA and the Cyber Security Act's Cyber-Certification Framework

On 20 January 2026, the European Commission presented a draft revision of the Cyber Security Act (CSA). As part of this proposal, a renewed European framework for cybersecurity certification of ICT products, services,

processes, and managed security services is being introduced. The scheme is intended as a practical and voluntary tool for companies, enabling them to demonstrate compliance with EU legislation and thereby reduce the burdens and costs associated with regulatory implementation. The Commission states that a primary objective of the cyber-certification framework is to address the fragmented regulatory landscape and the complexity of horizontal and sector-specific rules.

The Commission indicates that the renewed framework will initially reduce administrative burdens for entities covered by the NIS2 Directive. However, it also presents a clear opportunity to streamline and simplify the implementation of DORA, particularly the obligations under DORA Chapter V on ICT third-party risk management. Under Chapter V, financial entities are responsible for managing ICT third-party risks in accordance with DORA. This includes the requirement that financial entities only enter into contracts with ICT service providers that meet appropriate information security standards (e.g., ISO-27001, NIST, etc.).

We recommend that the Commission use the fitness check to analyse how the cyber-certification framework for ICT services could help reduce financial entities' extensive obligations to ensure that ICT third-party providers comply with applicable law and maintain adequate security, contingency plans, and incident management. The reduction of administrative burdens for NIS2-covered entities should also benefit actors subject to DORA in areas where the requirements of the two frameworks are equivalent.