Insurance Europe messages on the upcoming Digital Omnibus

Introduction

The insurance industry believes that greater simplification and alignment in EU digital legislation are urgently needed. Insurers face unique challenges in implementing multiple digital requirements while also managing sensitive personal data and ensuring the continuity of critical services.

The forthcoming Digital Omnibus package from the European Commission provides a unique opportunity to address these challenges and make EU digital legislation more coherent and streamlined.

Insurers contribute to digital transformation, first and foremost by helping to build resilience in the face of increasing and evolving cyber risk. In addition to ensuring their own digital operational resilience, insurers increasingly offer cyber insurance solutions, which focus on prevention, risk management, and post-event support. Secondly, through their uptake of digital solutions, insurers increase efficiency, improve consumers' journeys, and promote financial inclusion. Additionally, insurers' data use, which is inherent to their business model, is fundamental for risk analysis, risk mitigation and prevention, and, therefore, for offering services and products consumers need and expect. As such, insurers' use of data and technologies is pivotal to increasing the insurability of risks. It is also key for detecting and preventing fraud.

However, insurers are increasingly challenged by a growing patchwork of complex, overlapping, and sometimes inconsistent digital regulations. This regulatory landscape – spanning artificial intelligence, cloud, data protection and cybersecurity – has become particularly complex and burdensome for insurers, thereby diverting valuable resources from innovation and customer services.

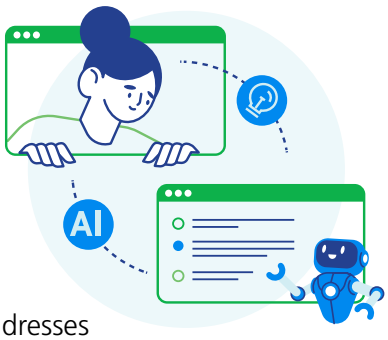
Therefore, a simplified regulatory framework will be essential to enable the sector to invest confidently in digital innovation, support customers, and contribute to Europe's economic resilience.

Against this background, Insurance Europe invites EU policymakers to implement **several guiding principles** to ensure digital legislation is fit for purpose and simplified:

- Real burden reduction: Eliminate obligations that are duplicative, immaterial or of limited value.
- Clarity and transparency: Avoid relabelling complexity as simplification. Communicate intentions and impacts openly.
- Coordination across layers: Ensure alignment between Level 1, 2 and 3 rules, avoiding divergence between the European Commission, European Supervisory Authorities (ESA) and other involved authorities.
- Evidence-based rulemaking: Give time for implementation and evaluation before revising rules.
- Respect implementation realities: What looks simple on paper may be complex in practice — engage companies early and give them enough time to implement legislation.
- Limit external reporting from insurers to any authority – rather exchange relevant data amongst different authorities
- Aim for global coherence where there are contradictions or where EU level guidance is missing.

In addition, Insurance Europe **puts forward concrete recommendations** in a number of policy areas that would ensure the simplification of EU digital rules.

Detailed messages by policy area



Artificial Intelligence

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. 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.

Solvency II Framework

In the context of organisational and prudential requirements, for example, there are requirements to establish and operate sound internal control mechanisms, effective procedures for risk assessment and effective control and safeguard arrangements for information processing systems. Articles 41, 44 and 46 of Solvency II require all insurance and reinsurance undertakings to have in place an **effective system of governance** which provides for sound and **prudent management of the business**.

Articles 38 and 49 of the Solvency II Directive also sets out the requirements regarding the **outsourcing** of functions and activities (eg collaboration with data vendors). Insurers are required to take appropriate arrangements to mitigate the

risks related to the use of third-party service providers and ensure that the outsourcing does not impair the quality of their internal control and the ability of the competent authorities to monitor compliance with all their obligations, while remaining fully responsible for discharging all their obligations under legislation (even when several third-party providers are involved).

Furthermore, Article 19 of the Delegated Regulation (EU) 2015/3546 containing implementing rules for Solvency II establishes detailed **data accuracy/quality requirements**, in particular in relation to the data used in the calculations of the technical provisions.

Insurance Distribution Directive (IDD)

The **product oversight and governance** (POG) requirements under the Insurance Distribution Directive (IDD) are also relevant for the use of AI, in particular in relation to the identification of the target market and the design/placing on the market of products. These provisions regulate the design of new insurance products and ensure that all insurance products meet the needs of their specific target market, regardless of the techniques used in said products.

Moreover, the IDD also requires (Article 20) that any insurance product that is proposed to a customer shall be consistent with their **demands and needs**, which addresses the risks of unsuitable products being sold to customers.

In addition, rules on **advice** (Article 20) apply wherever a personal recommendation is provided to a customer, regardless of whether that recommendation is provided by a human or AI actor.

Article 17(1) of the IDD also requires insurance distributors to **act honestly, fairly and professionally** in accordance with the best interests of their customers.

There are also requirements on insurers to establish fair and efficient claims and **complaints handling** processes (Article 14).

Recommendations

- Provide appropriate clarification 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. Such guidance should focus on showing where existing Solvency II/IDD requirements already meet AI Act obligations for insurers, and where additional measures are required, to prevent duplication and provide implementation clarity.
- Provide explicit clarification that traditional statistical methods, including generalised linear models (GLMs), are outside the scope of the AI Act as they do not fall under the definition of an AI system. This clarification will help to avoid ambiguity, inconsistent interpretation, and unnecessary burden for companies and supervisors regarding existing statistical analysis and modelling and also help focus the definition on the more salient characteristics of machine learning, ie inference and autonomy.

Cloud

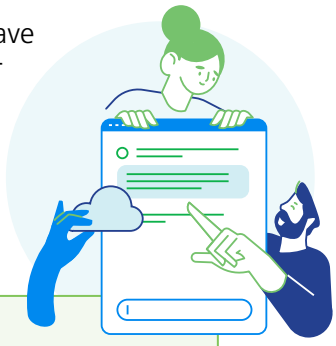
Use of recognised certifications and audit reports of critical ICT service providers

The Digital Operational Resilience Act (DORA) establishes an EU-wide oversight framework for critical ICT (information and communication technology) third-party providers. At the same time, insurers are required to continuously monitor the third-party ICT service providers they engage. The general rule under the Solvency II framework is that insurers remain fully responsible for discharging all of their obligations when they outsource functions or any insurance activities. The ultimate responsibility lies with the outsourcing institution.

Article 274 of Commission Delegated Regulation (EU) 2015/35 demands that the written agreement between the insurance or reinsurance undertaking and the service provider clearly states the requirement that the insurance or reinsurance undertaking has "effective access to all information relating to the outsourced functions and activities, including carrying out on-site inspections of the business premises of the service provider". However, providing for regular on-site inspections of cloud service providers seems unnecessary for supervisory authorities or for the internal audit function and is not necessary to achieve supervisory or monitoring objectives. On-site audits give limited insights into service performance - it would be more relevant therefore to focus on the provider's compliance with applicable laws and information security standards. For example, rather than focusing on physical on-site inspections, which become less relevant given the remote nature of cloud computing, supervisory authorities or internal audit functions should be able to rely on independent assurance by third party certification bodies or compliance with relevant standards.

However, when an ICT service supports a critical or important function, Article 8(3) of Delegated Regulation (EU) 2024/1773 stipulates that institutions must not rely solely on third-party certifications or audit reports provided by the service provider over the long term. Consequently, despite the presence of recognised certifications, financial institutions are still required to conduct their own audits.

This obligation applies even when the European Supervisory Authorities (ESAs) have already audited the same service provider under their powers concerning critical ICT service providers. Such audits demand significant preparation and entail considerable costs. As a result, it is not feasible to extend these audits to an unlimited number of providers. This constraint may inadvertently increase concentration risk, as institutions tend to rely on a limited number of 'known' service providers.



Recommendations

- Ensure that audit obligations faced by financial institutions allow for a more efficient use of recognised certifications and audit reports, so that financial entities are not required to duplicate their efforts and carry out individual audits of the same service provider independently of one another.
- Allow financial institutions to access the results of audits carried out by the ESAs' Joint Examination Teams under DORA. This could potentially eliminate the need for duplicative audits by each institution of the same service provider.
- Financial institutions should be able to adjust the audit obligation proportionally to selected parts of the services provided by a critical ICT service provider, as this provider may also deliver services that are not critical for the institution.
- Provide appropriate clarification that in relation to ICT services, insurers only have to focus on complying with the relevant provisions in DORA, which should take precedence over the Solvency II outsourcing rules.

Cybersecurity

Simplification through the revision of the Cybersecurity Act (CSA)

The revision of the Cybersecurity Act planned for late 2025 provides an opportunity to simplify cybersecurity reporting burdens for companies. Specifically, addressing duplications of reporting of cyber incidents under different legislations, timelines and to different authorities should be addressed to reduce administrative burdens. Clarity should be ensured in the rules across jurisdictions as well as the interplay between pieces of legislation on the same issues. Further to this, any future certification in cybersecurity should be pursued mindfully, with greater transparency and opportunities for stakeholder participation in the process.

Recommendations

- Ensure consistent and comparable reporting formats across jurisdictions to avoid differing interpretations. Provide a risk-based approach of thresholds for required reports, to allow concentration on relevant incidents and avoid unnecessary, low-risk reports.
- Issue clear and consistent guidance to member states, to prevent the emergence of conflicting national frameworks.
- Ensure stakeholder participation and transparency in potential future certification schemes
- Provide institutions with insight into the authorities' expectations regarding the criteria for incident reporting. Each institution currently spends many resources determining the reporting threshold based on its own interpretation, which risks creating significant variation in what is reported.

Cyber Resilience Act (CRA) – Digital Operational Resilience Act (DORA) Overlap

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 financial services industry calls for 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. DORA covers the entire lifecycle of these systems, from development to decommissioning, and includes risk-based management, incident handling, vulnerability management, and customer communication strategies.

Recommendations

- Issue a clear exemption from the CRA measures for financial entities subject to DORA in order to address the duplication of cybersecurity requirements between the two frameworks.
- Coordinate digital legislation to uphold coherence and reduce implementation burden

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is the central piece of cybersecurity legislation for the financial sector. DORA entered into force in January 2025. Financial entities have been preparing for implementation over the last two years, during which time the level 2 measures and regulatory technical standards were being finalised.

The first DORA reporting cycles began in 2025, with financial entities submitting their registers of information to the national competent authorities. The first cyber incident reports have also been filed under DORA, highlighting the real application of the measures and the burden they entail. The recommendations below address areas where companies have faced disproportionate burden to comply with DORA, highlighting where simplification and increased proportionality would be necessary to lighten the time and costs associated with the regulation.

It is important to note that further amendments under DORA should be made in a seamless way to the existing requirements to prioritize stability for existing templates and reduce disruption, avoid additional adaptation costs and further development and testing for companies that have already invested heavily in to comply with DORA.

The specific recommendations include:

Streamline DORA reporting:

- Reduce the **administrative burden** of the cyber incident reporting under DORA.
- Improve data processing practices to make the **registers of information reporting more efficient and effective**.
- Streamline the reporting process of the registers of information.
- Align DORA guidelines and reporting requirements.
- Establish a **centralised repository of subcontractor information at European level**.

Ensure a more proportional and efficient DORA application:

- **Enhance proportionality** in DORA to ensure that independent of size, undertakings with a low risk profile face reduced and risk-based requirements.
- Refine and clarify the **definition of 'ICT services'** (without extending the scope) under DORA.
- Address the duplication of requirements within corporate groups for **intra-group IT service providers**.
- Create a template as guidance for the annual risk framework evaluation in DORA.
- Enable more efficient use of **recognised certifications and audit results** of critical ICT service providers.

Recommendations

Streamline DORA reporting:

- Reduce the **administrative burden** of the cyber incident reporting under DORA.
  - Simplify the **amount of documentation needed** for the register of information;
  - Raise the **thresholds for classifying a major incident** (e.g. EUR 100,000) in order to reduce unnecessary reporting for incidents that are not of high severity.
  - Introduce flexibility into the **time-based thresholds** to account for sectoral differences of the impact of outages.
  - Ensure reporting focuses on **system-critical incidents** and allow interim reports to use estimates or rounded figures to ensure that during the crisis, the focus remains on crisis management rather than reporting.
  - Introduce clear guidance on **remediation measures and risk assessments**, to support entities in the communication of these measures and assessments to the national authorities.
  - Create a **European cyber incident reporting template** that is compatible to all reporting regimes (e.g. DORA, GDPR) to reduce the manual input into multiple templates that is currently required.

- Improve data processing practices to make the **registers of information reporting more efficient and effective**, including enhancing the templates to minimise repetitive manual data entry (e.g. LEI codes across multiple sheets).
  - Standardise **column codes and naming** to mitigate avoidable errors caused by header mismatches and code discrepancies between ITS and national templates.
  - Eliminate **non-essential fields**, consolidate duplicates and simplify the ROI data structure. For example, the template does not accept submissions unless all mandatory fields are completed, regardless of whether the field is relevant to the company. Fields should be allowed to be marked with 'not applicable' where the entity does not hold the relevant data.
  - Allow multi-value data fields (i.e. country of storage of data) to avoid the duplication of records when delivering the ROI.

- Streamline the reporting process of the registers of information
  - Streamline **validation** to occur only once, instead of separating this into national then European authority, in order to prevent unnecessarily compressing deadlines. Optimise the process to allow the guarantee of one validation to be recognised by another authority.
  - Streamline reporting into a **single submission** to avoid duplications for financial entities within one country having to report to multiple teams within one national authority, as well as those operating cross border reporting to multiple authorities. This applies especially to the reporting for third party service providers, who currently may need to be reported to multiple teams at national level and further times if operating cross-border.
  - Harmonise **digital submission interfaces** at national competent authorities level (e.g. XML/JSON-based) to integrate with firms' contract and procurement systems.
  - Allow IT tools at national level which facilitate the submission of the registers, for example tools to convert Excel files to XBRL format provided by the national authorities.

- Provide more points of feedback during the reporting process from the national authorities to the financial entities, to ensure that the reporting can be improved through the process and refined for the next submissions. The reason for validation errors should be communicated to the financial entity with sufficient time to allow for corrections.

- Align DORA guidelines and reporting requirements.
  - 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.
  - Avoid additional **national requirements** in addition to DORA, which undermines proportionality and creates hurdles for cross-border financial entities.
  - Align **guidance** on DORA to avoid confusion for financial entities, especially between the level 2 measures, FAQs, and national competent authorities instructions. A definitive set of guidelines on the ROI templates would be useful for financial entities, which could include examples of correct completion.
  - Create a **European ROI template** that does not alter existing templates and is aligned to the systems of the national competent authorities to facilitate the reporting of financial entities operating cross-border. This should be done in a harmonised way to ensure it would match the original ROI submissions and not entail new changes.

- Establish a **centralised repository of subcontractor information at European level** to complement the Global LEI index to enhance transparency and streamline due diligence processes.
  - 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.
  - Establish 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.

Ensure a more proportional and efficient DORA application:

- **Enhance proportionality** in DORA to ensure that independent of size, undertakings with a low risk profile face reduced and risk-based requirements.
  - This includes a proportional approach to the reporting documentation and scaled review intervals to alleviate excessive admin burden, as well as making the simplified ICT risk management framework available to a broader group of entities such as small and non-complex undertakings (SNCUs) already defined under Solvency II and subject to proportional requirements.
  - Clarify that a financial entity may meet its obligations on third party risks by ensuring the contractual flow-down of requirements to subcontractors and by overseeing that the ICT third party provider has the necessary processes and controls in place. Only in cases where specific risks or a lack of transparency have been identified should additional independent due diligence at subcontractor level be required, which is consistent with the principle of proportionality.

- Affirm that sole proprietorships, especially when using company equipment, should not be regarded as ICT providers. Individuals delivering ICT services to financial institutions under employment intermediation agreements (so-called body leasing) should also be excluded from the scope of DORA.
- Allow for a more proportional application of contractual provisions with regards to DORA through allowing an explicit differentiation besides the two variants of 'critical outsourcing' and 'non-critical outsourcing'.

- Refine and clarify the **definition of 'ICT services'** (without extending the scope) under DORA to ensure a more consistent understanding of the terms across jurisdictions. The unclarity leads to inconsistent interpretations and disputes with third parties, increasing the burden unnecessarily. The current scope enables robust and strategic third-party risk management.

- Address the duplication of requirements within corporate groups for **intra-group IT service providers.** These are currently subjected to the full scope of NIS2, despite typically being integrated into the group's unified system. The purely group-internal IT service providers should be exempt from the requirements of the NIS2 Directive, or, allowed to voluntarily follow DORA-aligned reporting obligations to reduce this clear overlap of cyber incident reporting.
  - Adress a similar situation for further providers who supply services to entities covered by DORA, but who are themselves subject to NIS2, who may be supporting the resolution of an incident whilst needing to report the same incident to a different authority.

- Create a template as guidance for the annual **risk framework evaluation** in DORA, based on the IDRS format.

- Enable more efficient use of **recognised certifications and audit results** of critical ICT service providers to avoid duplication of audits for the same entities. By allowing the use of recognised certifications already produced, instead of a new audit by the financial entity, this will reduce the administrative burden and duplication.
  - Allow financial undertakings to access the audit results conducted by the ESAs' Joint Examination Teams under DORA, which would further mitigate this duplication of audits for the same providers.

Data & AI

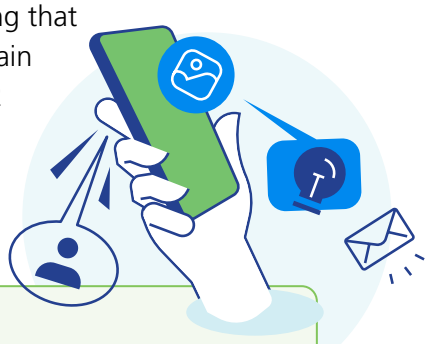
To enable artificial intelligence (AI) and data-driven innovation, the EU must focus on enhancing the usability, coherence and effectiveness of its legislative framework. The proliferation of overlapping legal instruments – including the General Data Protection Regulation (GDPR), AI Act and the Data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

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

Automated decision making under GDPR

For example, the application of **Art. 22 GDPR** regarding automated decision-making is often interpreted narrowly. Some data protection authorities claim that automated decisions cannot be considered "necessary" simply because humans have historically performed such tasks. They draw the conclusion that automated decision-making is not permissible and that an effective consent according to Art. 22 (2) (c) and Art. 7 (4) GDPR can only be given if the data subject has the opportunity to choose processing by a human being from the beginning. However, such a narrow interpretation of what can be considered necessary would prevent insurers and consumers from fully accessing the benefits of new technology.

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



Recommendation

- Automated-decision making should be allowed as long as it is subject to safeguard mechanisms. To ensure that Art. 22 does not become an obstacle to the development of new digital solutions, it should be clarified that it is a right of the data subject and not an ex-ante prohibition.

Interaction between GDPR, the Artificial Intelligence Act and other legislation

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

For example, impact assessments under GDPR Article 35 are not subject to a reporting obligation. By contrast, the AI Act imposes such a requirement for fundamental rights impact assessments under Article 27(3). A clarification is therefore needed to avoid not only a duplication but also an extension of the reporting obligations.

There are also risks about fragmented approaches in guidance and supervision, particularly within the financial services sector. Insurers are already subject to a robust EU regulatory framework in terms of both prudential and conduct rules.

Under current legislation, insurers deploying AI technologies could be subject to supervision by various authorities, including the relevant data protection authority, the insurance supervisory authority and a designated authority under the AI Act. This approach may result in duplication, inconsistencies and legal uncertainty.

Recommendations

- The relevant insurance supervisory authority should remain in charge of supervising the application of the AI Act. To ensure effective and coherent regulation, policymakers should clarify and streamline overlapping obligations, such as impact assessment requirements. 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 risks of overlap with existing GDPR obligations. A more flexible approach could be to closely align FRIA requirements with the existing DPIA requirements, thus avoiding overlap. At the very least, a sector-specific mapping/template could be developed aligning Art. 35 of GDPR (DPIA) with Art. 27 of the AI Act (FRIA) for insurers to avoid duplication and enable a single, coherent assessment pathway.
- A single reporting portal would greatly enhance the effectiveness of these requirements. To further ensure effective and coherent regulation, many national authorities issue guidelines on concepts of European legislation, but we think this is not the way forward: European legislation (such as DORA or the AI act) should be explained on a European level, to prevent national interpretation differences, possibly resulting in forum shopping. Only when national particularities play a role in interpreting the law, should national authorities give a national explanation, but there is no need for national authorities to explain European concepts and rules. If these national authorities feel there is a need for explanation, they should liaise with their European counterparts.

Legal basis for AI training

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

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

Recommendation

- Introduce a specific legal basis, beyond Article 10(5) AI Act, allowing the use of special categories of personal data for development and testing of AI models. Such legal basis should be narrowly scoped and conditioned on strict safeguards (purpose limitation, data minimisation, privacy-enhancing controls and documented governance, with independent auditability), without prejudice to the GDPR.

Anonymisation

In today's digital era, anonymisation plays a vital role in enabling various forms of data analysis. It is key to develop and evaluate new systems, products, and services. New EU legislation on data sharing also increasingly requires the anonymisation of data. For example, Article 18(5) of the Data Act mandates anonymisation when transmitting data to public authorities. To ensure coherence with the Data Act (e.g. Art. 18(5)), methodological clarification is needed on whether, and under which conditions, pseudonymised datasets held by a recipient without reasonable means of re-identification may be treated differently from personal data, particularly in controlled environments for AI testing/validation. This clarification should be without prejudice to the GDPR.

However, there is still **significant legal uncertainty** regarding when data is considered sufficiently anonymised. While the European Data Protection Board (EDPB) is expected to issue guidance on anonymisation soon, its Guidelines 01/2025 on pseudonymisation already suggest that the EDPB may adopt very strict standards in this area.

To provide legal clarity and support data-driven innovation while maintaining privacy safeguards, policymakers should adopt a relative approach to defining anonymised data, particularly in the case of pseudonymised information shared with third parties. Specifically, pseudonymised data should not be automatically classified as personal data in the hands of a third-party recipient if that recipient does not have access to additional identifying information and lacks any reasonable means - whether technical, legal, or practical - to re-identify the individuals. Re-identification should only be considered feasible where it is legally permitted and reasonably achievable without disproportionate effort.

Recommendation

- To ensure coherence with the Data Act, provide methodological clarification on the treatment of pseudonymised datasets in the hands of recipients without reasonable means of re-identification, without prejudice to the GDPR. Clarify that the identifiability of data should be determined relatively, based on whether the data controller can reasonably identify an individual.