PensionsEurope's position paper on the EC digital omnibus regulation proposal

March 2026

www.pensionseurope.eu

PensionsEurope acknowledges the Commission's initiative to simplify the EU digital rulebook through the digital omnibus package. We recognise the importance of a robust digital operational resilience framework for the financial sector, as well as the need for appropriate safeguards for the processing of personal data.

Pension funds invested a lot of resources to meet the extensive requirements set out under the Digital Operational Resilience Act (DORA) to improve their operational resilience. At the same time, pension funds also comply with the General Data Protection Regulation (GDPR), which modified several aspects of pension provisions, including the recording of data processing and procedures for data breaches.

However, we would like to reiterate our concerns[1] that second pillar pension funds differ profoundly from other financial entities and that the application of the principle of proportionality should be reinforced.

Applying DORA uniformly, regardless of the type of financial entity, does not work for IORPs and other types of pension funds, as occupational pensions are often managed through social partners and linked to employer affiliation. Small and less complex financial entities, such as most of the IORPs, should consequently not be subject to the same obligations as systemically critical players.

DORA should stop diverting pension funds' resources from core operational objectives. A principle-based approach of DORA would help to achieve effective ICT risk management and avoid unnecessary ICT controls. Against that background, we believe the digital omnibus proposal should lead to further changes to DORA, beyond incident reporting, and not focus on the centralisation of incident reporting.

Furthermore, while maintaining high standards of personal data protection, we believe that meaningful simplification of the GDPR needs to be achieved with additional legal basis for data health processing where necessary, in particular in areas creating legal uncertainty for pension funds. Such changes would materially reduce the operational burden on pension funds.

Both above-mentioned amendments to DORA and the GDPR would ensure that the Commission's simplification agenda[2] is delivered in practice and that unnecessary complexity is effectively removed, in line with the messages conveyed at the ECOFIN Council[3].

1. Simplification of DORA requirements for pension funds

1.1. Simplification of ICT incident reporting is necessary, but not through EU centralisation

Concrete simplification could be achieved in the field of major ICT-related incidents reporting by reducing the number of reporting fields and extending reporting deadlines in ICT incident reporting. Focusing on the impact on critical or important functions would also help in easing the compliance burden on pension funds while ensuring that NCAs receive meaningful information.

Under DORA, the criteria to classify major ICT-related incidents do not sufficiently consider the real impact on critical or important services. Those criteria are overlapping and counterproductive as non-material

[1] PensionsEurope's answer to the EC call for evidence on the digital omnibus package, October 2025 (here)
[2] Commission's communication on implementation and simplification, February 2025 (here)
[3] Council conclusion on simplifying the Union's financial services regulation, December 2025 (here)

incidents can be categorized as major, creating superfluous reporting for IORPs and as well as for NCAs.

The criteria for classifying major ICT-related incidents should therefore be revised to focus primarily on material impact on critical or important functions.

However, simplification must not be interpreted as requiring the creation of a centralized EU reporting hub, as proposed in the Commission omnibus proposal on the "*digital acquis*". From the perspective of the funded pension sector, such a hub would only increase cost and complexity, disrupt already established communication channels with NCAs, and risk introducing delays and fragmentation. Rather than simplifying the framework, a centralised reporting hub would add an additional reporting layer without clear supervisory benefits.

We would like to highlight that level 1 of DORA already establishes effective mechanisms for the sharing of information. Article 19(6) requires NCAs, upon receipt of incident notifications, to convey details of major ICT-related incidents promptly to the ESAs, the ECB, CSIRTs, resolution authorities, and the SRB, as well as other relevant public authorities under national law. This provision ensures thorough cross-authority information flows without the need for a new centralised structure.

1.2 The register of information and subcontracting requirements should be simplified

DORA requirement to maintain detailed records of their ICT service providers and their subcontractors creates a costly, excessive regulatory burden and is difficult to interpret both for financial entities and supervisors. Excessively granular registers do not enhance supervisory oversight and risk overwhelming both pension funds and competent authorities with unnecessary data. This is inconsistent with the principle of proportionality. Thus, focusing on critical and important functions under the register of information would help to simplify the delivery of information of pension funds by reducing the number of data points required.

Moreover, clarifying the definition of ICT services would help to ensure higher legal certainty in the subcontracting chain, as regards responsibilities when services are outsourced to financial entities. The Commission Q&A clarifying the issue should be directly embedded within DORA level 1 to ensure that outcome.

DORA also imposes that contracts with ICT third-party providers are continuously updated to reflect changes in ICT services or when contracting parties change. The contractual terms of requirements under DORA are burdensome and need to be reviewed. Moreover, contractual terms trigger a relevant burden for ICT third-party providers; IORPs, especially mid and small institutions, are facing major difficulties in finding providers willing to deliver ICT services, and their availability only comes at a high cost.

1.3 Third-party and ICT risk management should be streamlined

It is both disproportionate and duplicative to oblige financial entities to retain legal responsibilities on critical third-party ICT service providers (CTPPs) that are already under EU-wide oversight. This approach has limited added value in terms of risk management, diverting resources from core operational responsibilities, and ultimately diminishing the overall efficiency of the regulatory framework. Financial entities should be able to rely on the outcomes of EU-level oversight.

Allowing financial entities to access the audit results produced by the ESAs Joint Examination Team (JET) under the DORA would avoid having financial entities conduct audits on CTPPs, tackle the issue of the duplication of audits, and reduce administrative burdens.

Furthermore, DORA establishes an extremely granular, and comprehensive framework for ICT risk management. Such granularity risks diverting internal resources away from the management of material and genuinely relevant ICT risks. Therefore, the framework should focus on critical and important functions to avoid disproportionate requirements with limited added value.

1.4 The simplification of DORA Level 2 legislation is needed

The granular approach of the level 2 measures, both implementing and delegated acts, gives little flexibility in implementing DORA requirements compared to the level 1 text. The compliance costs that level 2 legislation has put on pension funds are disproportionate compared to the benefits brought by DORA, as some requirements do not bring better ICT risk management. Therefore, we would ask the EC and the Council to ask the ESAs to deliver on DORA level 2 simplification, as the Council recently asked the AMLA to "*to adopt a simpler and more targeted approach to developing Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS)*"[4] .

1.5 Focusing the DORA review on the simplification

The DORA Level 1 review clause provides for the possibility of a Commission legislative proposal - after consulting the ESAs and the ESRB- by 17 January 2028. In light of the issues identified above, which may require further assessment by the Commission, the review should prioritise simplification measures aimed at delivering a more principle-based framework. Taking into account the length of the legislative process for the Digital Omnibus package, we further suggest that the DORA review be brought forward.

[4] Council conclusion on simplifying the Union's financial services regulation, December 2025 (here)

2. Simplification of GDPR requirements for pension funds

2.1 Health data processing for pension benefits (Article 9 GDPR)

Pension funds are, in certain circumstances, legally required to process health data to assess entitlement to retirement, disability, or serious illness benefits.

PensionsEurope recognises that, in several Member States, IORPs and other types of pension funds are already able to rely on Article 6(1)(b) GDPR (performance of a contract), in conjunction with Article 9(2)(b) and/or Article 9(2)(h), where the processing of health data is objectively necessary to fulfil a legal or contractual obligation under a statutory or collectively agreed pension framework. In those jurisdictions, supervisory practice has provided legal certainty and operational stability.

However, in other Member States, the absence of a legal basis to process health data for the sole purpose of assessing whether the retirement benefit should be provided under Article 9(2) has created legal and operational uncertainty, particularly where explicit consent is considered the only viable legal basis. This may expose pension funds to risks linked to the withdrawal of consent, potentially affecting their ability to verify entitlement to benefits that are otherwise due under the applicable pension rules.

Under the Spanish pension legislation, beneficiaries must submit medical documentation to demonstrate that the relevant legal contingency has occurred. While this voluntary submission may indicate a willingness to have health data assessed for this limited purpose, the current wording of Article 9 requires explicit consent in the absence of a specific legal basis. This creates both legal and operational uncertainty. In particular, a beneficiary could refuse or later withdraw consent, preventing the fund or scheme manager from verifying statutory entitlement and potentially obliging it to deny the payment of a benefit that is otherwise due under the law or contract.

While the Digital Omnibus proposal introduces new provisions for processing special categories of data related to artificial intelligence systems and biometric identity verification, it does not explicitly address the situation where the processing of health data is strictly necessary to comply with legal or contractual obligations related to the management and payment of pension benefits.

Against this background, PensionsEurope considers that the Digital Omnibus could provide targeted clarification to ensure legal certainty among EU MSs. Any new provision should confirm that processing of health data (without explicit consent) is permitted where strictly necessary for the recognition, management, or payment of pension benefits under a legal or contractual framework and should explicitly state that it is without prejudice to existing national practices and legal bases currently relied upon under Articles 6 and 9 GDPR.

The objective is not to replace or disrupt functioning national models, but to ensure legal certainty in Member States where a normative gap or divergent interpretation currently exists that requires explicit consent for the processing of necessary health data for the recognition, management, or payment of pension benefits.

2.2 Clarification is needed of an activity that is "*not data-intensive*" (Article 13 GDPR)

The Commission proposes exempting data controllers from disclosing a wide range of information to the data subject where personal data is collected from them for situations involving a clear and circumscribed relationship and an activity that is "*not data-intensive*,".

While PensionsEurope welcomes efforts to reduce unnecessary administrative burden, the concept of "*not data-intensive*" remains vague and risks creating legal uncertainty for pension funds, which regularly process large volumes of personal and sensitive data over long periods. Clear criteria or a definition at Level 1 would enable data controllers to assess with confidence when the exemption applies and would ensure consistent interpretation and enforcement across Member States.

2.3 Timelines for breach notification template and high-risk circumstances list (Article 33 GDPR)

The deadlines set out in Article 33(c) for publishing a harmonised notification template for personal data breaches to supervisory authorities, as well as the list of circumstances where such breaches pose a high risk, are unnecessarily long.

The European Data Protection Board has been tasked to prepare those templates and lists, to be sent to the Commission within 9 months of the entry into application of the regulation. Taking into consideration the length of the Commission's process to adopt those implementing acts, we believe that this does not align with the overarching goal of simplification to ensure the timely and practical implementation of the digital legislation.

2.4 Pseudonymisation and re-identification standards (Article 41a GDPR)

The text empowers the Commission to define, through implementing acts, the technical means and criteria for determining when pseudonymised data can no longer be considered personal data for certain entities. We believe that minimum standards for effective pseudonymization should be included directly in the Level 1 text of the Regulation to ensure immediate legal certainty, given the significant impact of the GDPR's scope of application. Such an important political issue should not be delegated to level 2 legislation, which only supplements the level 1 legislation.

Annex

Proposed amended wording for Article 9(2) GDPR (Article 3 of Digital Omnibus)

Without prejudice to the application of Articles 6(1)(b), 9(2)(b) and 9(2)(h), amend Article 9(2) GDPR by adding the following new point (m):*"(m) processing is strictly necessary for the recognition, management or payment of retirement, disability, dependency or other related pension benefits, where such processing is required by contract or legal provision governing the pension plan, for the sole purpose of verifying and administering the conditions for entitlement, and is subject to appropriate and specific safeguards to protect the fundamental rights and interests of the data subject, including data minimisation, purpose limitation, restricted access and professional secrecy. This provision shall not affect the validity of other legal bases currently relied upon under this Regulation for the process of health data related to the treatment of certain pension benefits"*

About PensionsEurope

PensionsEurope represents national associations of pension funds and similar institutions for workplace and other funded pensions. Some members operate purely individual pension schemes.
*PensionsEurope has **21 member associations** in 16 EU Member States and 3 other European countries[5].*

*PensionsEurope member organisations cover different types of workplace pensions for **over 65 million people.** Through its Member Associations, PensionsEurope represents over **€ 2,5 trillion of assets** managed for future pension payments. In addition, many members of PensionsEurope also cover personal pensions, which are connected with an employment relation.*

*PensionsEurope also has **13 Corporate and Supporter Members,** which are various service providers and stakeholders that work with IORPs.*

*PensionsEurope has established a **Central & Eastern European Countries Forum (CEEC Forum)** to discuss issues common to pension systems in that region.*

*PensionsEurope has established a **Multinational Advisory Group (MAG),** which delivers advice on pension issues to PensionsEurope. It provides a collective voice and information sharing for the expertise and opinions of multinationals.*

What PensionsEurope stands for

- *A regulatory environment encouraging workplace pension membership.*
- *Ensure that more and more Europeans can benefit from an adequate income in retirement.*
- *Policies which will enable sufficient contributions and good returns.*

Our members offer

- *Economies of scale in governance, administration and asset management.*
- *Risk pooling and often intergenerational risk-sharing.*
- *Often "not-for-profit" and some/all of the costs are borne by the employer.*
- *Members of workplace pension schemes often benefit from a contribution paid by the employer.*
- *Wide-scale coverage due to mandatory participation, sector-wide participation based on collective agreements and soft-compulsion elements such as auto-enrolment.*
- *Good governance and alignment of interest due to participation of the main stakeholders.*

Contact :
PensionsEurope
Montoyerstraat 23 rue Montoyer – 1000 Brussels
Belgium
Tel: +32 495 21 62 61
info@pensionseurope.eu

[5] EU Member States: Austria, Belgium, Bulgaria, Croatia, Finland, France, Germany, Greece, Hungary, Italy,Lithuania Luxembourg, Portugal, Romania, Spain, Sweden. Non-EU Member States: Iceland, Norway, Switzerland.