

## Digital Omnibus

EFAMA welcomes the Digital Omnibus legislative proposals, and in particular the targeted amendments introduced to the GDPR and the AI Act. The proposed amendments aim to reduce unnecessary administrative burdens and provide legal clarity within the existing regulatory framework while preserving its core objectives.

Under the AI Act, the proposal maintains its core objective of establishing a comprehensive legal framework for the development and deployment of AI systems, grounded in a risk-based approach to safeguarding the fundamental rights of EU citizens. Similarly, we consider the proposed changes to the GDPR to be limited in scope and carefully calibrated, providing greater legal certainty while not substantially altering existing rights and protections, particularly the right to privacy and the protection of personal data.

Below is EFAMA's position vis-à-vis the provisions proposed under the Digital Omnibus.

### 1. Changes to GDPR

We consider that the changes proposed to the GDPR framework under Article 3 of the Digital Omnibus legislative proposal will provide legal certainty for industry in key areas.

Data is the primary input for the development, training, and testing of AI systems, and there must be clear alignment between the GDPR and the EU's AI framework for companies to effectively develop and deploy AI systems. In this context, we welcome the European Commission's Strategy for Data, published alongside the Digital Omnibus legislative proposals in November 2025, which sets out the Commission's ambition for the EU to take a leading role in the global data economy.

Overall, we consider the proposed changes to the GDPR to be positive, and we broadly welcome the European Commission's efforts to adjust an already robust legal framework. These adjustments aim to preserve the EU's priorities in data protection, fundamental rights, and cybersecurity, while also providing clearer rules for companies to access and use data in ways that support the development and deployment of critical technologies, such as AI. We consider the proposed amendments to be targeted and technical in nature, intended to provide the legal certainty and clarity firms need to innovate and use data responsibly.

The asset management sector is already subject to robust EU requirements on cybersecurity, data protection, and business conduct, positioning the asset management industry well to develop and deploy AI systems responsibly. Given the scale and importance of the sector, even

incremental AI-driven efficiency gains can deliver meaningful macroeconomic benefits. Prioritising AI adoption in asset management would therefore strengthen the EU financial ecosystem, improve investor outcomes, and enhance global competitiveness, particularly in a context where strong data governance and ethical AI are becoming key differentiators.

### **Amendments to Article 4 GDPR (Definitions)**

Article 3(1) of the Digital Omnibus introduces a targeted amendment to Article 4 of the GDPR by clarifying the circumstances under which information should be considered personal data within the scope of GDPR. In particular, it confirms that information about a natural person does not automatically constitute personal data for any other person or entity merely because another entity can identify that individual. Where an entity cannot identify the natural person concerned, taking into account the means reasonably likely to be used by that entity, the information should not be regarded as personal data for that entity and, therefore, to be out of scope of the GDPR framework.

In practice, however, asset management firms already operate robust data governance frameworks as part of business-as-usual operations. We therefore do not expect this amendment to trigger material or immediate changes to internal processes. Rather, it should provide greater legal certainty and help avoid disproportionate GDPR safeguards for datasets that pose no meaningful privacy risk. By reinforcing a risk-based, contextual assessment of identifiability, the amendment supports responsible data use while preserving the GDPR's core principles.

In the longer term, we hope this clarification will enable greater flexibility in the use of effectively de-identified datasets for data analytics and AI model development, particularly where entities have no realistic means of identifying the underlying individuals. To ensure legal certainty in practice, we also look forward to the Commission's work under the newly proposed Article 41a GDPR, which mandates the development of EU-level criteria to determine when pseudonymised data can no longer be considered personal data.

### **Amendment to Article 9 GDPR – Processing of special categories of personal data in the context of AI**

Article 3(3) of the Digital Omnibus adds a new point (k) to Article 9(2) of the GDPR, creating a narrowly defined legal basis for processing special categories of personal data in the development and operation of AI systems or AI models. Importantly, this provision does not encourage or normalise the use of personal data for AI development. Rather, it is designed as a legal fallback to address situations in which such data are inadvertently identified in datasets used for training, testing, or validation.

Read together with the proposed new Article 88c GDPR, which clarifies that certain AI-related processing may rely on legitimate interests (further analysis below), Article 9(2)(k) provides residual legal certainty while maintaining strict safeguards. In practice, asset managers already operate within robust governance frameworks in a highly regulated environment where investor protection remains central. Moreover, the use cases in which an asset manager would require personal data are limited in scope and often involve the client as a data subject that already expressly consents to the processing of such data in the context of its usual contractual relationships with the asset manager.

The new version of Article 9 GDPR still requires controllers to actively avoid collecting and processing special categories of personal data through appropriate organisational and technical measures. Where such data are nevertheless identified, they must be removed. Only where removal would require disproportionate effort does the provision allow an alternative approach,

i.e. effectively protecting the data without undue delay from being used to generate outputs or from being disclosed or otherwise made available to third parties. In this sense, we consider that clarifying the concept of ‘disproportionate effort’ will be crucial to ensure that firms are not subject to excessive scrutiny or unrealistic expectations when responding to incidental identification of special categories of personal data. Any guidance should recognise practical and technical constraints in large-scale or complex datasets and allow firms to rely on reasonable, risk-based assessments when determining whether removal is feasible, provided that effective safeguards against use and disclosure are in place.

From an asset management perspective, the practical relevance of this provision is limited for core investment activities. One of the few relevant scenarios concerns the processing of health data in the context of pension scheme management. Under certain national frameworks, managers must assess medical documentation to determine whether a retirement benefit is payable, i.e. in cases of disability, dependency or serious illness. While beneficiaries voluntarily submit such documentation, Article 9 of the GDPR currently requires explicit consent in the absence of a specific legal basis, creating unnecessary operational complexity and the risk that a refusal could prevent verification of entitlement and result in denial of the benefit. Where processing is strictly necessary to comply with legal obligations and assess eligibility, this requirement appears unjustified. Given that the draft Omnibus Regulation already introduces additional exemptions under Article 9(2), it would be appropriate to add a specific ground covering the processing of health data strictly necessary for the management, recognition or payment of retirement benefits, subject to appropriate safeguards.

### **Amendment to Article 35 GDPR – Data protection impact assessments**

The amendments introduced to Article 35 by new paragraphs 4, 5, and 6 aim to further harmonise and centralise the EU framework for data protection impact assessments (DPIAs). In particular, the proposal empowers the EDPB to develop EU-wide lists of processing operations that do, or do not, require a DPIA, as well as a common template and methodology for conducting DPIAs, to be adopted by the Commission through implementing acts and reviewed periodically. This represents a shift away from the current fragmentation resulting from divergent national supervisory authority lists and approaches.

Overall, this development is positive. Greater centralisation and harmonisation at the EU level should help simplify compliance for firms operating cross-border, including asset managers, and reduce legal uncertainty around when a DPIA is required. A common methodology and template could also promote more consistent and risk-focused DPIAs, supporting a more proportionate application of the framework. In particular, the review and rationalisation of cases where a DPIA is required could help refocus efforts on genuinely high-impact processing activities, including certain AI-driven use cases, rather than encouraging a largely formalistic or defensive approach to DPIAs.

At the same time, the practical impact of these changes will depend on how narrowly or broadly the future EU-level lists and methodology are defined. For asset managers, many data processing activities, including AI-related use cases, are already treated as DPIA-relevant by default due to their scale, complexity, or perceived risk. The effectiveness of this amendment will therefore hinge on whether it leads to meaningful simplification and prioritisation in practice, rather than merely replacing national lists with an equally expansive EU-level framework.

## **New Article 41a GDPR – Means and criteria to assess re-identification risk**

Article 41a introduces a new provision empowering the Commission to adopt implementing acts specifying the means and criteria for determining when data resulting from pseudonymisation no longer constitute personal data for certain entities. Pseudonymisation plays a central role in enabling the use of data for analytics and AI development while reducing risks to data subjects. Greater legal clarity in this area could materially affect firms' ability to use data in a compliant and scalable manner.

Overall, we support the provision's objective to shift the assessment of re-identification risk toward a more structured, evidence-based approach that considers the state of the art and the characteristics of typical data recipients. By allowing the use of Commission-defined means and criteria as an element to demonstrate that re-identification is not reasonably likely, Article 41a has the potential to reduce legal uncertainty around when pseudonymised data should still be treated as personal data for a given entity. This could be particularly relevant for AI training, testing, and validation activities, where access to large datasets is often essential and where the inability to rely on pseudonymisation can create practical barriers to data use.

Moreover, EFAMA encourages the co-legislators to consider embedding clear minimum standards directly in the Regulation itself, thereby ensuring immediate legal certainty and setting a baseline that is both workable and supportive of industry. Establishing this minimum bar at the level of the legal text would provide a stable foundation for compliance, while still allowing the Commission to introduce further technical specifications or clarifications where necessary.

## **New Article 88c GDPR – Confirmation that processing in the context of the development and operation of AI may qualify as legitimate interest**

Article 88c introduces a new, AI-specific provision clarifying that the processing of personal data in the context of the development and operation of AI systems or AI models may, where appropriate, rely on the legitimate interest legal basis under Article 6(1)(f) GDPR. This clarification is welcome, as it provides greater legal certainty for AI-related processing activities that are necessary for the controller's interests, while reaffirming that such processing remains subject to the existing balancing test and does not apply where Union or national law explicitly requires consent.

The provision also places clear emphasis on safeguards and accountability. Processing under Article 88c must be accompanied by appropriate organisational and technical measures to protect the rights and freedoms of data subjects, including data minimisation at the stages of data selection, training, and testing, protections against the disclosure of residually retained data, enhanced transparency, and an unconditional right for data subjects to object. These elements help ensure that the clarification does not weaken existing data protection standards, but rather situates AI development more clearly within the GDPR's established risk-based framework.

From an asset management perspective, Article 88c could support responsible AI development by clarifying the conditions under which legitimate interests may be relied upon in practice, without altering the underlying safeguards or shifting the balance of rights. In this context, the asset management sector is well placed to rely on this clarification, given its existing obligations under EU data protection, cybersecurity, and business conduct rules.

## **Changes to the AI Act**

### **Amendment to Article 4 AI Act – AI literacy**

The Digital Omnibus on AI amends Article 4 of the AI Act by shifting the obligation on AI literacy from a binding requirement on providers and deployers to an encouragement role for the Commission and Member States. This change clarifies that measures to promote AI literacy are no longer framed as a direct compliance obligation subject to supervision and enforcement, but rather as a policy objective to be supported at the EU and national levels.

This amendment is welcome, as it removes a potential administrative burden that could have been difficult to operationalise and supervise in practice, for both firms and competent authorities. In highly technical sectors, requiring firms to formally demonstrate compliance with a broadly framed AI literacy obligation could risk becoming a box-ticking exercise without necessarily improving the effective and responsible use of AI systems.

In practice, firms already have strong incentives to invest in AI literacy to remain competitive and to deploy AI systems effectively and safely. This is particularly the case in technology- and data-intensive sectors such as financial services, where innovation, digital capabilities, and the skilled use of ICT systems are core drivers of performance. Against this background, encouraging AI literacy through guidance, best practices, and capacity-building initiatives appears more proportionate and better suited to supporting AI uptake than a prescriptive compliance obligation.

### **Amendment to Article 113 AI Act – Phased application of obligations for high-risk AI systems**

The Digital Omnibus on AI introduces a revised, more flexible application timeline for the obligations applicable to high-risk AI systems under the AI Act, effectively creating a ‘*stop-the-clock*’ mechanism. In particular, the application of Chapter III obligations to high-risk AI systems listed in Annex III is conditional on the availability of adequate compliance-supporting measures, as confirmed by a Commission decision, with a longstop date of 2 December 2027 in the absence of such a decision. This approach represents a significant adjustment to the original timeline, under which these obligations were scheduled to take effect in August 2026.

This amendment is welcome. The AI Act establishes an extensive, technically complex framework, and additional time is needed for firms to design, implement, and operationalise compliant governance, risk management, and control frameworks, particularly for high-risk AI systems.

At the same time, the revised mechanism introduces uncertainty, as firms must monitor the timing and content of the Commission’s supporting compliance measures and the adoption of the corresponding decision that triggers the application of obligations. While EFAMA welcomes the development of EU-level guidance, standards, and other implementation tools, predictability and simplicity remain critical for effective planning. In this context, consideration could be given to setting a single, fixed application date further in the future, such as 2 December 2027 for Annex III high-risk AI systems, which is already foreseen in the text as a backstop. A fixed date would provide legal certainty, facilitate internal planning, and avoid requiring firms to track multiple conditional triggers, while still allowing sufficient time for the Commission’s support measures to be developed and incorporated.



## ABOUT EFAMA

EFAMA is the voice of the European investment management industry, which manages around EUR 33 trillion of assets on behalf of its clients in Europe and around the world. Its membership consists of 29 national associations, 52 global asset managers, and 27 associate members. We advocate for a regulatory environment that supports our industry's crucial role in steering capital towards investments for a sustainable future and providing long-term value for investors.

Besides fostering a Savings & Investments Union, consumer empowerment and sustainable finance in Europe, we also support open and well-functioning global capital markets and engage with international standard setters and relevant third-country authorities. EFAMA is a primary source of industry statistical data and issues regular publications, including Market Insights and the authoritative EFAMA Fact Book.

More information is available at [www.efama.org](http://www.efama.org)