

Brussels, 11 March 2026

Digital Fitness Check

The European Fund and Asset Management Association (EFAMA) welcomes the Digital Fitness Check and the European Commission's initiative to review the EU Digital Rulebook and assess how it can be improved to better support innovation and help position Europe as a global leader in critical technologies.

The European investment management industry plays a crucial role in steering capital toward investments that deliver long-term value for clients, promote economic prosperity, and enable Europe to pursue its strategic interests. Moreover, our firms operate in a highly regulated environment, widely regarded as a safe and robust framework that protects investors and addresses risks to the EU's financial stability.

We consider that much of the EU's digital regulation, which is horizontal in nature and applies across multiple sectors, overlaps with the detailed, sector-specific rules already applicable to the investment management industry. This creates unnecessary duplication and additional burden, particularly where the risks targeted by digital regulation are already addressed under existing financial regulatory frameworks.

In this paper, we set out key digital legislative files that could be significantly simplified, in particular by removing duplicative obligations for firms in the financial services sector.

EU AI Act

Financial Services as a Strategic Sector for AI Innovation

We welcome the European Commission's focus on AI as a strategic priority and the approach set out in the 2025 'Apply AI Strategy' communication.

At the same time, we note that financial services is not currently identified as one of the 'key industrial sectors' targeted for sectoral policy flagships under the Strategy. Nevertheless, the document explicitly acknowledges that future iterations may extend to additional strategic sectors, stating that *'the actions below could be complemented in the future by new initiatives in other sectors – such as finance'*.

In this vein, we would encourage the European Commission to consider including financial services as a strategic sector under future iterations of the Apply AI Strategy. The asset management industry exhibits precisely the 'untapped AI potential' that the Apply AI strategy aims to unlock. The European asset management industry plays a vital role in capital allocation, managing over €33 trillion in assets on behalf of European investors. AI can enhance data quality, operational efficiency, compliance processes, and investment decision-making, all of which are crucial to economic resilience, long-term savings, and the financing of the real economy.

Including the financial services industry in future iterations of the Apply AI Strategy would enable the European Commission to implement specific sectoral initiatives and actions to boost and facilitate AI uptake in our industry.

One such initiative could be developing **sector-specific financial data spaces**. Access to high-quality, standardised data remains challenging, as asset managers depend on diverse, complex, and often sensitive datasets. Moreover, there is currently a lack of harmonised taxonomies and frameworks to facilitate privacy-compliant, secure, and interoperable data sharing across jurisdictions.

EFAMA considers that the development of a European Financial Data Space, with a dedicated pillar for capital markets and asset management, would be highly beneficial to the financial industry overall. This space should enable secure, GDPR- and MiFID II-compliant access to standardised datasets, including ESG data, pricing feeds, and corporate actions. Such access is essential for training AI models and supporting cross-border digital services, especially for mid-sized firms that lack the depth of proprietary data.

It is key for the relevance of financial data sets to the asset management industry that these include:

- standardised anonymisation and privacy-preserving data-sharing toolkits,
- interoperable API frameworks to ease integration
- clear liability and access rules under the Data Governance Act.

A well-designed financial data space would unlock efficiency, transparency and innovation in data-driven asset management.

Simplification of the EU AI Act

EFAMA has developed a detailed document outlining certain provisions under the EU AI Act that remain unclear. The way these provisions are ultimately interpreted and applied will significantly determine the burden they impose. This document is included as an Annex at the end of this paper, and we hope that the Commission clarifies these interpretive issues in a way that allows for a balanced approach to implementing the EU AI Act.

We note that asset managers must comply with a comprehensive set of obligations covering due diligence, risk management, governance, and internal controls under the regulatory frameworks to which they are subject, including MiFID II/MiFIR, UCITS, AIFMD, and DORA. Several obligations introduced by the AI Act could overlap with these frameworks if not properly managed.

Future guidance under the AI Act should therefore aim to streamline AI-specific obligations and integrate them into the existing financial regulatory framework. Doing so would simplify compliance processes and remove unnecessary barriers to innovation, without compromising safety or consumer protection. This alignment is particularly important in the context of horizontal legislation such as the AI Act, which applies across sectors with widely different levels of AI maturity, data infrastructure, and risk exposure.

We consider Recital 158 of the EU AI Act to be a critical reference point for the effective implementation and future improvement of the regulatory framework as it applies to financial entities. Recital 158 seeks to ensure coherence and avoid duplication by acknowledging that certain obligations under the AI Act may be integrated into, or partially adjusted in light of, existing sectoral financial governance rules. This reflects that EU financial services legislation already includes internal governance and risk-management requirements that apply to financial institutions when they use AI in the provision of their services.

However, Recital 158 primarily focuses on streamlining obligations for credit institutions under Directive 2013/36/EU (Capital Requirements Directive – CRD). In particular, it refers to aligning providers' procedural obligations relating to risk management, post-market monitoring, and documentation with existing CRD requirements and supervisory procedures. The recital further envisages limited derogations regarding providers' quality management systems and the monitoring obligations imposed on deployers of high-risk AI systems. These derogations are explicitly contemplated for credit institutions, insurance undertakings, and 'other types of financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services law'.

We believe the scope of Recital 158 should be expanded to cover a wider range of entities and potential derogations.

First, the recital should extend beyond its current focus on credit institutions and insurance undertakings. Greater clarity is needed on which sectors and entities qualify as 'other types of financial institutions', and how specific AI Act obligations will be aligned with their existing sectoral requirements. While it was understandable that earlier iterations of the AI Act concentrated on credit institutions and insurance undertakings, given that the high-risk AI use cases listed in Annex III, paragraph 5(b) and (c), relate to credit scoring and life insurance, the AI Act is ultimately a horizontal instrument based on a risk-based approach. As such, it will require a wide range of financial entities to review and, where necessary, adjust their governance frameworks regarding the use of AI. Clear guidance is therefore needed to ensure that these adjustments are coherent with, and not duplicative of, existing financial regulatory obligations.

Second, as regards the limited derogations currently envisaged, we consider that further overlaps between the AI Act and sector-specific financial regulation should be identified. The Commission should undertake a more detailed assessment of relevant sectoral frameworks to determine where additional limited derogations may be justified. This assessment should go beyond the two areas explicitly mentioned in Recital 158 (i.e. the quality management system of providers and the monitoring obligations for deployers of high-risk AI systems).

For example, in the case of investment funds, relevant frameworks would primarily include Directive 2009/65/EC (UCITS Directive) and Directive 2011/61/EU (AIFMD), as well as MiFID II for firms providing investment services or performing investment activities. A structured mapping exercise between these frameworks and the AI Act would help ensure regulatory coherence, avoid duplication, and preserve the effectiveness of existing financial supervisory arrangements.

DORA

The implementation of the Digital Operational Resilience Act (DORA) was a massive undertaking for the asset management industry, particularly in terms of system upgrades, governance documentation, and staff training. DORA has now moved from 'project mode' to business-as-usual, but making the framework operational and efficient remains a key challenge. Our members report high ongoing compliance costs under DORA.

EFAMA believes the DORA framework could be further simplified to ensure it remains risk-based and proportional. To achieve genuine simplification, EFAMA recommends that the Digital Omnibus prioritise the following areas.

Simplifying ICT incident reporting

Simplification efforts should first focus on ICT incident reporting requirements. The number of reporting fields in ICT incident reports should be reduced, focusing on the data points that are truly necessary for supervisory purposes. Simplifying the structure of incident reporting templates would significantly reduce the administrative workload for firms, especially those with multiple regulatory reporting obligations under DORA, GDPR, and the AI Act.

Reporting deadlines should also be extended to ease compliance burdens while maintaining timely and meaningful information flows to supervisors. Allowing firms additional time to verify the accuracy and completeness of incident reports would improve data quality and reduce the need for subsequent corrections or follow-up requests.

Finally, the incident classification framework should be reviewed to ensure that only incidents of critical relevance trigger reporting obligations. Minor events with limited or no systemic impact should not fall within the reporting scope, allowing both firms and supervisors to focus resources on incidents that present genuine operational or systemic risks.

Improving proportionality in the application of DORA

A stronger, more consistent application of the principle of proportionality is necessary throughout the DORA framework. In particular, smaller investment fund managers (IFMs) and ICT providers that do not support critical or important functions (CIFs) should be excluded from the scope of the more onerous obligations. Similarly, lower levels of subcontracting should be exempt and not automatically trigger the same compliance requirements as those applicable to larger or systemically important entities.

More broadly, proportionality should be reinforced across all layers of ICT oversight to ensure that smaller firms are not subject to the same regulatory expectations as large, systemically important financial institutions.

Streamlining registers of information (ROI) and reporting processes

The current requirements relating to registers of ICT providers and related reporting processes could also be simplified. Firms should be required to maintain only a single register of ICT providers and report through a single, consolidated channel, either at the local or group level. Ensuring the harmonisation of registers and reporting processes would remove duplication and significantly improve operational efficiency.

Further simplification could be achieved by providing a simplified format for the register of information (ROI). For the majority of small and medium-sized firms, immediate cost savings could be realised if a simplified format or basic Excel template were made available. This would reduce the need for external consultancy support and specialised tooling. To complement this, centralised guidance on validation checks and a testing environment would help firms implement the requirements more efficiently and reduce the resources currently spent locating, interpreting and implementing technical guidance.

Enhancing the oversight framework for ICT third-party providers

The oversight regime for ICT third-party providers should also be reviewed and streamlined. While the industry welcomes the new supervisory regime for systemically critical third-party providers (CTPPs), financial entities would benefit from greater visibility into the outcomes of supervisory assessments to inform their own risk management processes. Access to aggregated data on ICT providers' use could also help firms assess concentration risks and improve transparency across the market.

At the same time, the current obligation for asset managers to maintain detailed records of all ICT providers and subcontractors is disproportionate and often duplicative, particularly where those providers are themselves regulated under DORA. For smaller and non-systemic financial firms, the requirement to continuously collect, verify, and update this information creates a significant compliance burden while providing limited additional supervisory value. The current approach risks becoming a formal compliance exercise rather than a tool for effective risk oversight.

Simplification efforts should therefore focus on clarifying the respective responsibilities of financial entities and critical ICT providers, avoiding redundant oversight obligations, and reinforcing proportionality in the

application of the DORA framework. In particular, registers of ICT third-party providers should exclude providers that do not support critical or important functions (CIFs), focusing supervisory attention where it delivers genuine risk oversight benefits.

Clarifying contractual requirements and regulatory overlaps

Further simplification could be achieved by introducing a standard set of contractual conditions between financial entities and ICT providers, particularly to clarify the obligations incumbent upon ICT service providers, to rebalance the negotiating power currently held by large technology providers vis-à-vis regulated financial clients.

At the same time, financial entities should be allowed to apply DORA contractual clauses with greater flexibility in accordance with the principle of proportionality. For example, in the case of services that consist solely of data transmission and do not include the provision of the related platform, it should be possible to rely on qualitative service-level objectives. Similarly, financial entities that have not been designated as subject to Threat-Led Penetration Testing (TLPT) should not be required to impose contractual obligations on ICT providers to participate in or cooperate with TLPT exercises.

Finally, overlapping regulatory requirements should be avoided. Financial entities already subject to DORA should be excluded from the scope of the Cyber Resilience Act to ensure a clear delineation between horizontal and sector-specific regulatory frameworks.

Single entry point (SEP)

EFAMA does not currently have a unanimous position on the centralisation of incident reporting through the Single Entry Point (SEP) proposed under the Digital Omnibus legislative package, which is currently under discussion by the co-legislators under the ordinary legislative procedure. Nevertheless, we would like to offer a few observations that could help simplify the development of any future framework in this area.

First, the Digital Omnibus proposal aims to streamline the information reported for incident reporting, building on the experience gained under the Digital Operational Resilience Act (DORA) and the reporting templates already developed under that framework. DORA is a key regulatory framework for asset management companies, which are subject to its cyber-incident reporting obligations. Implementing DORA has already required significant investments by firms, both in terms of initial implementation and ongoing compliance costs.

However, the current legislative proposal does not introduce any substantive simplification of the reporting requirements themselves (i.e., neither regarding their format, content, or timing). Instead, it primarily changes the destination of the reports, shifting them from national competent authorities (NCAs) to a centralised reporting mechanism managed by ENISA. As a result, we do not expect the proposal to significantly reduce the number of data fields or the reporting burden for firms. If the objective is to enhance competitiveness and reduce unnecessary compliance costs, the focus should be on simplifying the reporting requirements themselves (i.e. as suggested in our aforementioned recommendations regarding DORA simplification).

Second, the proposed centralisation of incident-reporting frameworks could introduce additional operational complexity. Under the current approach, incident reporting requirements across different regulatory frameworks (i.e. DORA, GDPR, NIS2, and CER) may need to be consolidated into a single reporting format. When designing common reporting templates, there is a risk that the specific characteristics of smaller financial entities or specialised business activities may no longer be adequately reflected, particularly if reporting frameworks are calibrated to the needs of critical infrastructure operators. This could lead to disproportionate reporting efforts and costs for financial entities whose systemic importance and risk profile

differ significantly. The principle of proportionality should therefore be carefully respected to avoid unnecessary administrative burdens.

In this context, a potential alternative approach could preserve the benefits of coordination while limiting some of the risks associated with full centralisation. Rather than replacing existing reporting channels, the framework could introduce a **Data Sharing Hub** acting as a coordination mechanism. Under this model, NCAs would remain the primary point of contact for financial entities submitting incident reports. Once received, reports would be shared with the Data Sharing Hub, which would then make the information available to the relevant EU authorities and stakeholders involved in the response process.

Such a model would maintain established supervisory relationships while improving coordination and information sharing at the EU level. To ensure effectiveness, the Data Sharing Hub should rely on **harmonised reporting standards across the EU**, rather than allowing national authorities to determine their own reporting formats. A uniform EU-level data-sharing system could, over time, simplify reporting obligations and reduce costs, particularly for firms operating across multiple jurisdictions that currently need to report incidents to several NCAs. It could also facilitate faster incident analysis and a more coordinated response to potential cyber threats.

In addition, concentrating sensitive incident data within a fully centralised reporting system could make it an attractive target for cyberattacks. A more decentralised data collection model, supported by a coordination hub, may therefore reduce the risk associated with the concentration of highly sensitive information.

Finally, the proposed SEP implementation timeline raises questions. According to the proposal, the SEP would become operational only after the successful completion of a pilot phase, with an 18-month deadline from the entry into force of the amending regulation. The obligation for companies to use the SEP would then depend on the European Commission confirming that the system developed by ENISA is fully functional and publishing this assessment in the Official Journal of the European Union.

However, the proposal also foresees that, if the Commission determines that the central reporting system is not fully operational, companies would still be required to use it 24 months after the entry into force of the amending regulation. This raises concerns regarding legal certainty and operational readiness. If the SEP's functionality cannot be fully guaranteed within this timeframe, further safeguards or flexibility mechanisms should be considered.

GDPR, Anti-Money Laundering and KYC Digital Portability

The Digital Fitness Check should address the persistent legal uncertainties regarding the interplay between the GDPR and the EU's Anti-Money Laundering (AML) framework. Asset managers operating globally or within large groups face significant barriers when sharing KYC and 'know-your-transaction' data across entities due to restrictive interpretations of data protection rules. To ensure a truly fit-for-purpose digital framework, the Commission should explicitly recognize the sharing of information for AML/CFT purposes as a 'substantial public interest' under the GDPR. This recognition is essential to eliminate the current reliance on individual consents for intragroup data transfers, which are often impractical or legally fragile in a financial services context. Providing a clear, harmonized legal basis will enable seamless data flows for global risk oversight, reducing administrative burdens and enhancing the effectiveness of financial crime detection through advanced digital tools, without compromising the European Union's high data protection standards.

Moreover, the concept of 'reliance' on third-party due diligence should be transformed from a theoretical legal provision into an operational reality. Currently, asset managers face significant technical barriers when attempting to leverage KYC work already performed by other financial entities, leading to redundant processes and a fragmented client experience. We call for the establishment of EU-wide technical standards for digital KYC portability. It is essential that clients are empowered to share a comprehensive

digital compliance profile that includes not only identity data but also verified attributes such as Beneficial Ownership (BO), PEP status, and Source of Wealth. By leveraging the EU Digital Identity Wallet, the industry can achieve full digital interoperability. This is particularly crucial within financial groups to ensure a 'single risk view' and to allow asset managers to rely on pre-verified digital profiles without unnecessary administrative duplication.

Tokenisation & DLT

EFAMA is actively engaged in policy discussions on tokenisation and distributed ledger technology (DLT), which we consider to have significant potential across the asset management value chain, from the issuance of tokenised funds and investment in crypto-assets to harnessing the efficiencies of blockchain-based trading and settlement.

By embracing DLT, asset managers can deliver superior value to clients through enhanced liquidity, cost reductions, and 24/7 accessibility, positioning Europe as a leader in a fully digitised financial ecosystem. These advancements not only help keep our industry relevant but also mobilise greater European savings into productive capital markets, supporting the EU's transition to a more sustainable and digitally enabled economy and boosting retirement savings.

In this context, we consider it key to create a legal framework that fosters innovation while ensuring investor protection and market integrity. EFAMA therefore strongly supports the DLT aspects of the Market Integration and Supervision Package (MISP) legislative proposal tabled by the European Commission.

Overall, we are extremely pleased to note the comprehensive review of the current regulatory framework to adapt it to DLT technology, the necessary changes to the EU's experimental sandbox legislation, and the clear ambition to build a framework that is future-proof and not already obsolete at the time of adoption.

EFAMA supports the reforms under the MISP package as a step in the right direction towards a future-proof legal framework that enables innovation in this area, subject to the modifications proposed below.

DLT PR

We welcome the expansion of the pilot regime to a new threshold of EUR 100bn in total aggregated market value for admitted instruments. This is certainly an improvement and absolutely necessary if the DLT PR is to enter a new phase of growth and attract a healthy level of operators. However, we would also like to make the following observations:

- It is not entirely clear how securities that are not digitally native, but that also have a traditional presence, would be treated. Such hybrid securities could quickly breach the EUR 100bn cap.
- Tokenised funds represent a very small, but high-growth portion of the mutual fund market. Other jurisdictions have no thresholds or flexible thresholds, which could make the EU DLT PR quickly irrelevant even in its updated form.
- We note that there is greater facility in amending these thresholds through an EC-delegated act without the need to resort to a change in the primary legislation. Nonetheless, a full removal of market value thresholds should be considered. Under a risk-based approach with proportionate requirements, higher (or no) thresholds could already be built into the DLT PR.

Unbundling of CSD services

- We are fully supportive of the proposal to allow an investment firm, regulated market, credit institution, or CASP to provide individual CSD services such as notary and central account keeping services.

- We question, however, the very low threshold of EUR 10bn (simplified regime), which would also apply to any providers of DLT notary or central account keeping.
- The final requirements and ensuing Level 2 standards by ESMA should not be more restrictive than the provisions laid out in national regimes for DLT securities registration. If the EC regime proves more restrictive, authorisations under existing national frameworks should be grandfathered.

Settlement Scheme

We were very pleased to encounter the 'settlement scheme' proposal within the DLT PR and the opening up for DLT central account keepers to take on this role. This absolutely supports the innovative, competitive solutions we would like to see brought to market by entities that fully leverage the power of DLT technology.

Some of the provisions appear too restrictive, breaking participation in the scheme before it even has a chance to become a proven business model (similar to what happened with the unfortunately low thresholds for the DLT PR when it was negotiated in 2020-2021).

- Confinement to the simplified regime at EUR 10bn maximum for aggregate total market value is once again too low and would severely restrict participation.
- The restriction of a maximum of 2 settlement schemes per DLT central account keeper appears arbitrary and too restrictive.
- Most significant in the design of the settlement scheme is the availability of payment options. Settlement schemes would be limited to central bank money, which seems odd given the need to fully leverage DLT and to retain the entire trading and post-trading workflow on-chain.
- Securities registered with DLT notaries should automatically benefit from on-venue trading eligibility and financial and central bank collateral eligibility.

UCITS holdings of Stablecoins

Technology neutrality is a broad theme we see reflected in the proposed updates to CSDR, DLT PR, and MiCA. These reforms are, however, incomplete if the buy-side of the equation is not taken into account. As we have signaled, UCITS regulation and the Eligible Assets Directive (EAD) were previously not entirely clear regarding UCITS funds' ability to hold stablecoins for payment purposes. We have previously sought such interpretive guidance and would appreciate if ESMA could clarify that stablecoins can be held for settlement purposes either as an ancillary liquid asset or because eligible asset requirements under art. 50 (1) of UCITS are met. Such guidance is outstanding and would be greatly appreciated by the buy-side community.



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

EFAMA Guiding Principles – Regulatory questions

Contents

Section 1: Definition and Scope of AI Systems.....	2
Section 2: Definition and Responsibilities of ‘Provider’ vs ‘Deployer’	4
Section 3: Group Structures.....	6
Section 4: Cases Involving GPAI Systems	8
Section 5: Fine-Tuning of AI Systems.....	11
Section 6: Cases Involving Open-Source AI Systems	13
Section 7: Interrelation with Other Regulations (i.e. MiFIR, GDPR).....	14
Section 8: Transparency Obligations (Article 50 EU AI Act).....	15
Annex : Non-exhaustive list of software systems or programming approaches that do not fall under the scope of the AI system definition in Article 3(1) AI Act	18

Question / Case description	EFAMA Position (where available)	Feedback EU AI Office
<h2 style="color: #0070C0;">Section 1: Definition and Scope of AI Systems</h2>		
<p>In the Commission Guidelines on the definition of an artificial intelligence (AI) system, published on February 6, 2025, Section 5.2 (Systems outside the scope of the AI system definition), paragraph 42 states that systems used to improve mathematical optimisation or to accelerate and approximate traditional, well-established optimisation methods—such as linear and logistic regression—are not considered AI systems.</p> <p>Moreover, paragraph 45 of the guidelines creates confusion by implying that linear or logistic regression methods may still be in the scope of the AI system definition (although paragraph 42 explicitly excludes them) when ‘permitting adjustments of their decision-making models in an intelligent way’.</p> <ul style="list-style-type: none"> • Could you clarify the boundary between excluded traditional methods and those that might be in scope due to such “intelligent” adjustment capabilities? • What are the key criteria or characteristics that might exclude certain supervised learning models — such as linear or logistic regression — from falling under the definition of an AI system, despite being 	<p>We consider that, as stated in paragraph 42 of the Commission Guidelines on the definition of an artificial intelligence system, linear or logistic regression methods should be <i>a priori</i> de-scoped.</p> <p>Simple supervised learning models (i.e. linear and logistic regression, Decision Trees, and other rule-based Systems) should generally fall outside the scope of the AI system definition under the AI Act, especially when used independently or in isolation.</p> <p>However, certain models can also serve as components within more complex AI architectures (i.e. deep learning networks), where they contribute to final classification or decision layers. In such integrated contexts, the system should be assessed holistically.</p> <p>The following characteristics and criteria are key when determining whether a supervised learning model, such as linear or logistic regression, should fall out of the scope of the AI Act (please see our Annex for a non-exhaustive list of algorithms and optimisation that we consider should not fall within the definition):</p> <ul style="list-style-type: none"> • Degree of autonomy: Do these models operate independently or execute fixed 	

<p>part of the broader category of supervised learning?</p>	<p>rules? -> They execute fixed, predefined rules. No autonomy is involved post-training; they apply static coefficients to inputs.</p> <ul style="list-style-type: none">• Adaptivity: Can the model adjust itself after deployment? -> No. They require manual retraining and do not adapt to new data without human intervention.• Complexity of inferencing: Do they generalise opaque or high-dimensional patterns? -> No. They model only linear relationships (or log-linear for logistic regression) and cannot capture complex or non-obvious patterns.• Explainability and traceability: Can the outputs be fully explained? -> Outputs are directly traceable to input variables and associated coefficients, making them fully interpretable.• Context of use: Are they used alone or within broader systems? -> Both. When used alone, they are transparent and low-risk. However, they may be embedded as components in complex AI systems, in which case their role must be assessed within that broader context.	
---	---	--

Section 2: Definition and Responsibilities of ‘Provider’ vs ‘Deployer’

<p>Definition of Provider – AI as part of a product/service</p> <p>Within the definition of a Provider is the wording ‘or puts into service’.</p> <p>Would AI be considered ‘put into service’ if used as input to a company's product or service?</p> <p><i>For example, a company might use AI for investment research, supporting an investment decision (i.e. the service an asset manager provides).</i></p> <p><i>Would this be considered being ‘put into service’, bringing one into the definition of ‘Provider’?</i></p>	<p>An asset manager using AI tools internally—for example, to analyse large datasets, support investment decisions, or inform risk assessments—should not be considered a ‘provider’ under the AI Act. In this case, the AI system is not made available to third parties or placed on the market under the asset manager’s name. The AI system functions entirely as an internal tool, operated under the organisation's direct control, and used exclusively by employees or internal systems.</p> <p>Classifying such internal deployment as equivalent to commercial provisioning would be disproportionate and counterproductive. Forcing internal users into a provider role would create regulatory friction without improving transparency or safety. No external user interacts directly with the AI system, nor is a separate AI product being marketed.</p>	
<p>Definition of Provider – client-facing</p> <p>Within the definition of a Provider is the wording ‘or puts into service’.</p> <p>Would this apply to <u>client-facing</u> AI use cases run on 3rd party system (i.e. GPTs)?</p> <p><i>For example, enabling clients to access AI-generated summaries of their portfolio performance or recent market news. This may initially be shared via email or via an external user interface, where they can directly ask questions. It would be run on 3rd party systems (i.e. from OpenAI). Would this bring us into the definition of ‘Provider’?</i></p>	<p>When asset managers use third-party AI systems to generate investment insights, commentary, or risk analytics—and then share these results with clients—they are providing outputs, not the AI system itself. The client receives an interpreted or post-processed result, typically reviewed or contextualised by the asset manager. This is fundamentally different from making the AI system itself available. The client does not interact with the system, nor does the model operate autonomously in the client's service. The asset manager exercises editorial control and human oversight, assuming responsibility for the accuracy and relevance of the output. As such, the</p>	

	<p>manager remains the user of an AI system, not its provider. Even in cases where the client is informed that AI played a role in the analysis, this remains a matter of methodology transparency, not system provisioning. As long as the asset manager does not market or repackage the system, provider obligations should not apply.</p>	
<p>Definition of Provider – ‘having developed’ an AI system or GPAI model</p> <p>It remains unclear, under Article 3(3) of the AI Act, whether the reference to a provider as someone who ‘develops an AI system or a general-purpose AI model or has an AI system or a general-purpose AI model developed’ requires that the system or model be specifically developed — or at least significantly tailored — for a particular client and intended area of application.</p> <p>In other words, in cases where development is outsourced (i.e. to an external vendor), what level of control, customisation, or naming rights over the AI system is required for the asset manager to be considered a provider?</p>		
<p>Definition of Deployer – Access to data sets from the AI provider’s system or product</p> <p>According to Art. 3(4) of the EU AI Act, ‘deployer’ means a natural or legal person, public authority, agency, or other body <u>using an AI system under its authority</u>, except where the AI system is used in the course of a personal non-professional activity.</p>	<p>It should be clarified that “using an AI system under its authority” does not extend to merely receiving AI-generated data sets or products from an AI provider’s system by electronic transfer or access to such data via API.</p>	

Section 3: Group Structures

Internal Group Provider using Third-Party AI

A legal entity is part of a larger group. It has implemented a third-party AI system without modification. The entity then offers access to this tool to other legal entities within the same group, enabling them to use it. In this scenario, it is crucial to clarify the contractual setup—whether there is a single central contract or each legal entity has an individual one.

In this scenario, the first entity remains solely a **Deployer** because it has implemented a third-party AI system without making any significant modifications or enhancements. Simply enabling internal access to this AI tool across multiple legal entities within the same group does not constitute a substantial modification, so the original third-party vendor should remain the sole **Provider**.

Contractual Setup:

If the contractual arrangements are decisive in classifying entities as either Providers or Deployers, a possible workaround could involve each legal entity within the group concluding a direct individual contract with the third-party Provider. Although this would increase the contractual complexity, it would support maintaining each entity's status as a Deployer.

Group-Level Provider, Local Entity

Modification. Entity A has implemented a third-party system, enabling another entity within its group (entity B) to access the AI tool. Entity B performs a substantial modification of the original AI system (please note that we have a specific understanding of 'substantial modification' for the purposes of Article 25 of the EU AI Act, which should be clearly distinguished from mere fine-tuning — see Section 5 on 'Fine-tuning of AI systems').

In this scenario, if entity B uses the modified tool only internally, meaning it does not make it available to other entities or external parties, **it should not be classified as a Provider** since one cannot be considered a Provider toward one's own employees. In that case, its role would remain purely internal, and thus, entity B would retain the status of an internal Deployer/User without Provider responsibilities under the EU AI Act.

	<p>However, entity B assumes the role of a Provider if the modified AI system is distributed or provided to other legal entities within the group. Even though the initial AI system was obtained from another internal group entity, the significant modifications or enhancements resulted in a substantially new or altered AI system.</p>	
<p>In the context of using a vendor AI system, please clarify if the definition of “other persons dealing with the operation and use of AI systems on their behalf other persons dealing with the operation and use of AI systems on their behalf” in article 4 includes employees of the vendor providing the system. Does the deployer of a vendor AI system need to ensure that the employees of the respective vendor of the AI system have a sufficient level of AI literacy?</p>	<p>Limit the obligation to one’s own organisation and downstream users to avoid duplication across different organisations</p>	
<p>Authorised Representative Requirements</p> <p>Where a Global Head Office is based outside the EU and GPAI capabilities likely owned by this non-EU office, clarification is needed as to whether, when the non-EU office makes available AI Systems to a group company or office in the EU, the requirement to appoint the EU entity as an “Authorised Representative” applies (Article 54: “Prior to placing a general-purpose AI model on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.”).</p>		

Section 4: Cases Involving GPAI Systems

<p>Definition of Provider – system powered by 3rd-party LLMs</p> <p>Within the definition of a Provider is the wording “body that develops an AI system or General Purpose AI model”. Would any level of development internally of an AI system (even when provided by a 3rd party) bring us into the scope of the requirements of providers of AI systems?</p> <p><i>For example, if a company created an internal AI assistant, where the assistant is powered by 3rd party models (i.e. OpenAI’s GPT series) but the company has developed other system components (i.e. the user interface, document processing, vectorisation).</i></p> <p><i>Would this be considered ‘developing an AI system’, or is the company categorised as only a deployer?</i></p>	<p>An organisation remains a deployer when it integrates a third-party AI model (i.e. a foundation model such as GPT) with minimal custom components, as long as these additions do not affect the model’s core functionality, purpose, or risk profile.</p> <p>However, once internal development reaches a point where it introduces new functionalities that alter how the AI system processes inputs, generates outputs, or is used in a different (potentially higher-risk) context, the system may be considered to have undergone a substantial modification. In that case, the organisation would effectively become the provider.</p> <p>This determination should follow a risk-based approach and align closely with the reasoning of substantial modifications: what matters is not whether the model is technically changed, but whether the integrated system represents a material shift in use, functionality, or risk (see Section 5 on ‘Fine-tuning of AI systems’).</p>	
<p>We require further clarity on what should be considered as ‘internal use’ for the purposes of the carve-out in Recital 97: <i>‘The obligations laid down for models should in any case not apply when an own model is used for purely internal processes that are not essential for providing a product or a service to third parties and the rights of natural persons are not affected’.</i></p>	<p>Where an AI system with an integrated GPAI model is used internally and not provided to other deployers, the asset manager should not be subject to the obligations of a provider of an AI system, nor should it be considered a provider of the GPAI model.</p>	

<p><i>For example, are Asset Managers who develop a GPAI model—either through their own IT function or via an ICT provider— under their own name or trademark, and integrate it into their own AI system that is used for internal purposes, subject to the obligations applicable to models in addition to those for AI systems?</i></p>		
<p>Internal Group Provider with GPAI-developed AI system</p> <p>A legal entity is part of a larger group. This entity uses generative AI technology (i.e. GPT-4) to create a new AI system. This newly developed AI solution is provided to other legal entities within the group, which use it without further modifications.</p>	<p>In this scenario, the entity’s classification depends on how it utilises the generative AI technology (i.e. GPT-4):</p> <ul style="list-style-type: none"> • If the entity merely employs a GPAI system (such as GPT-4) by providing basic prompts and subsequently creating a simple internal tool from its output, without any substantial modification, it should generally not be considered a Provider. In this case, the entity acts purely as a Deployer/User, essentially leveraging the generative AI's standard capabilities without fundamentally altering the underlying model. • However, if the entity performs a substantial modification by creating a new or distinctly tailored AI system, its role shifts to that of an AI system Provider. This classification is due to its substantial contribution to creating or significantly customising the AI solution provided internally across different legal entities within its group. 	

Centralized API Integration and Decentralised Usage

A legal entity is part of a larger group structure. A central legal entity within the group (i.e. a dedicated IT service provider) has centrally integrated a GenAI Tool (i.e. GPT-4) via an API onto a shared platform. This centralised integration is subsequently made accessible to individual legal entities across the group.

Each group entity independently decides how and in which processes it utilises the centrally provided API-based GPAI. Importantly, none of the entities performs any significant modification, fine-tuning, or enhancements of the AI model itself. Instead, each entity merely accesses and uses the API functionality as provided, possibly incorporating custom prompts or use cases without altering the underlying system.

The central legal entity (such as a dedicated internal IT service provider) that integrates the GPAI via API onto a shared platform would also typically be categorised as a Deployer, provided it has not made substantial modifications, retraining, or enhancements to the underlying generative AI model. Merely integrating an externally provided API-based GPAI into a central platform does not constitute significant modification; thus, the Provider role remains explicitly with the external third-party vendor (i.e. OpenAI for GPT-4).

Section 5: Fine-Tuning of AI Systems

When does fine-tuning or modifying an existing AI system lead to a requalification as a provider under the EU AI Act?

- In particular, can modifying or training a third-party AI system be considered a form of *developing* an AI system, thus triggering provider obligations as per Article 3(3)?

To support clarity in the application of the AI Act, it would be helpful to distinguish between *fine-tuning* and *substantial modification* as follows:

- **Fine-tuning:**

Fine-tuning involves adjusting an existing AI system—typically by training it on additional, often proprietary data—to improve performance within its original scope. By adjusting parameters and/or performing additional training on specific datasets, the AI system’s performance on a specific task is improved, leading to specialisation.

In our view, fine-tuning should not automatically shift a deployer into a provider role, provided that:

- The AI system’s core function and risk profile remain unchanged.
- The enhancements do not introduce new risk factors or ethical issues.

That said, fine-tuning is inherently challenging and can sometimes fall in a grey zone. If new datasets lead to material changes—such as unintended biases or altered ethical considerations—these adjustments might cross the threshold into what should be deemed a substantial modification.

	<ul style="list-style-type: none"> • Substantial modification: <p>A substantial modification occurs when changes significantly alter the system's intended purpose or risk characteristics. Examples include:</p> <ul style="list-style-type: none"> • Repurposing the system for a different, higher-risk application. • Integrating new components that transform the system's functionality. • Introducing training data that causes significant, unforeseen biases. <p>In such cases, the deployer would effectively launch a new version of the AI system, thereby assuming a provider's responsibilities.</p>	
<p>Could the AI Office provide examples to clarify the distinction between:</p> <ul style="list-style-type: none"> - modifications that do not amount to a substantial modification, and - those that do, thereby shifting a deployer into the role of a provider? 		

Section 6: Cases Involving Open-Source AI Systems

<p>Definition of Provider – open source</p> <p>Within the definition of a Provider is the wording “body that develops an AI system or General Purpose AI”. Does any level of development internally of an AI system (even when provided by a 3rd party) bring one into the scope of the AI system Provider’s obligations?</p> <p><i>For example, an entity uses an open-source SLM or LLM that runs on its own infrastructure <u>without being trained on its data</u>.</i></p> <p>While internal-only use of open-source models should generally not trigger provider obligations, the lack of a legally accountable original provider makes this an inherently difficult line to draw. In many real-world scenarios, what appears to be a pure deployment can, in effect, become a provision, not because of technical modification but because of legal accountability gaps. This uncertainty warrants further clarification from regulators, particularly for corporate groups relying on open-source AI in cross-border or multi-entity contexts.</p>	<p>In principle, entities that operate unmodified open-source AI models solely for internal use, whether on-premise or in a private cloud, should be considered deployers, not providers. The logic here is clear:</p> <ul style="list-style-type: none"> • The entity does not develop, commercialise, or place the model on the market. • The model is used as-is and integrated strictly within internal operations. • There is no external offering of the model under the entity’s name or brand. <p>Under these conditions, provider obligations under the AI Act should not apply.</p>	
<p>Open-Source Generative AI Fine-tuned Internally</p> <p>A legal entity is part of a larger group. It has implemented an open-source generative AI model (i.e. Mistral or Llama 3) and subsequently retrained or fine-tuned it using its proprietary internal data. The customised generative AI system is then made available internally and shared with other entities within its group.</p>	<p>We consider it crucial that the AI Office clarifies the distinction between a substantial modification and fine-tuning of a system. This will be key in determining which changes to an open-source model would qualify an entity as a provider or deployer when enabling access to the AI system for other entities within its group (see Section 5 on ‘Fine-tuning of AI systems’).</p>	

Section 7: Interrelation with Other Regulations (i.e. MiFIR, GDPR)

<p>For asset managers, MiFID II imposes strict model governance requirements, particularly in investment decision-making. However, these use cases may not be classified as high-risk under the EU AI Act unless they directly impact retail investors.</p> <p>Do you anticipate the introduction of specific guidance to clarify how asset managers should align MiFID II's model governance requirements with the EU AI Act's AI oversight framework?</p>	N/A	
<p>The EU AI Act permits the processing of special categories of personal data under strict conditions for detecting and correcting bias in AI systems. However, the GDPR imposes stricter limitations on such processing, generally requiring explicit consent or another valid legal basis.</p> <p>How can AI providers and developers reconcile these potentially conflicting requirements? What legal basis or safeguards can they implement to ensure compliance with both the AI Act and the GDPR while effectively mitigating bias in AI systems?</p>	N/A	
<p>The EU Commission's Joint Research Centre identifies existing standards (i.e. ISO/IEC 42001) that partially meet the requirements of the AI Act and highlights areas where further standard development is needed. What is the current status so companies can leverage these standards in the next step to streamline compliance with the AI Act?</p>		

Section 8: Transparency Obligations (Article 50 EU AI Act)

<p>Under Article 50(2) of the AI Act, providers of AI systems that generate synthetic images must ensure their outputs are marked in a machine-readable format, allowing them to be identified as artificially generated. However, the responsibility for disclosing deepfakes falls on deployers (users) under Article 50(4) of the AI Act. Since providers are only required to embed machine-readable markings, how can deployers technically mark and differentiate deepfakes from other synthetic images? What mechanisms or best practices can deployers use to ensure compliance with their disclosure obligations?</p>	<p>We believe that the responsibility for visibly marking AI-generated images should solely rest with the providers. It is burdensome for deployers to distinguish between deepfakes and other synthetic images. If providers are only required to embed machine-readable markings, it becomes operationally challenging for deployers to identify and differentiate deepfakes from other AI-generated content.</p>	
<p>According to Article 50 of the EU AI Act, “deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated.” In this context we seek specification of the interpretation of “public interest” whether the provisioning of (i) prospectus information, (ii) any product related information, or (iii) marketing material related to funds could be considered as informing the public on matters of public interest. In this context, clear guidelines or examples clarifying the threshold with respect to such “matter of public interest” would be welcomed.</p>	<p>Fund-related documents such as prospectuses, product sheets, and marketing materials should be considered outside the scope of Article 50(4) and should therefore not trigger a disclosure obligation for AI-generated content.</p> <p>There are two reasons for this position: These documents are not “matters of public interest” in the sense intended by the AI Act:</p> <p>Firstly, fund materials are legally required disclosures or commercial communications directed at a specific audience — namely, investors and clients. They do not serve the broader public in the way that political commentary, news reporting, or content related to public safety or democratic discourse does. The purpose of these</p>	

	<p>materials is to inform about the characteristics and risks of a financial product, not to shape public opinion or influence general societal outcomes. In this sense, they do not fall within the scope of public interest. Applying AI disclosure requirements in this context would blur the line between public-interest communication and regulated financial product documentation.</p> <p>Secondly, even if fund documents were to be considered matters of ‘public interest’, they would fall under the exception set out in Article 50(4), read in conjunction with Recital 134, as these documents are always subject to human oversight and formal approval.</p> <p>Regardless of whether a portion of a fund document is initially drafted using AI-based tools, the final version is always reviewed, validated, and approved by the responsible financial institution. Depending on the jurisdiction and document type, this includes legal teams, compliance, product managers, and often regulatory authorities. This means there is editorial accountability. Where a human takes full responsibility for the content, and the AI-generated portion is reviewed and potentially modified, the rationale for mandating a disclosure disappears. Moreover, in the context of asset management, any output that reaches the client or public has already passed through established layers of control and legal responsibility.</p>	
--	--	--

Annex : Non-exhaustive list of software systems or programming approaches that do not fall under the scope of the AI system definition in Article 3(1) AI Act

A principle-based approach offers greater clarity and consistency than evaluating systems on a case-by-case basis. The contrary would lead to an inherently ambiguous exercise, given that the status of software as an AI system often depends on the context of its implementation. Rather than identifying specific software systems, we propose that systems employing certain (primarily deterministic) algorithms or optimisation methods should not be classified as AI systems. We also consider that if integrated into more complex algorithms (i.e. Deep Learning), the system should be classified based on the overarching model, not its components. Confirmation is needed on whether systems using statistical methods (i.e. logistic regression) are out of scope.

Here are some examples (non-exhaustive) of algorithms or optimisation methods that, if used independently in software, should not be classified as an AI system:

Optimisation Methods

- Decision Trees/ Rule-Based Systems (If-Then Rules)
- Quadratic Optimization
- Gradient Descent
- Stochastic Gradient Descent (SGD)
- Newton's Method
- Trust-Region Methods
- Naive Bayes
- Expectation-Maximization (EM)
- GARCH (Generalized Autoregressive Conditional Heteroskedasticity)
- Principal Component Analysis (PCA)
- Bayesian Inference

Regression Models

- Polynomial Regression
- Linear Regression
- Logistic Regression
- Multiple Linear Regression
- Ridge Regression

Clustering Models

- K-Means and Hierarchical clustering