Hogan Lovells

News

AI regulation in financial services: navigating the EU AI Act in a layered regulatory landscape

12 May 2026

Banks, insurers and financial intermediaries are not newcomers to algorithmic decision making. Credit scoring models have been in production for decades, and actuarial pricing has long relied on statistical inference. The EU AI Act (Regulation (EU) 2024/1689) adds a new horizontal regulatory layer on top of these established practices. This creates a complex compliance landscape, interacting in particular with the GDPR and existing financial services regulation and multiple regulators independent from each other.This article provides a high-level overview of how the EU AI Act applies to the financial services sector, the key compliance challenges it raises, and the most relevant recent regulatory developments, including the Digital Omnibus Package, setting out proposals aimed at simplifying digital regulation, including AI-related rules.

Banks, insurers and financial intermediaries are not newcomers to algorithmic decision making. Credit scoring models have been in production for decades, and actuarial pricing has long relied on statistical inference. The EU AI Act (Regulation (EU) 2024/1689) adds a new horizontal regulatory layer on top of

these established practices. This creates a complex compliance landscape, interacting in particular with the GDPR and existing financial services regulation and multiple regulators independent from each other.

This article provides a high-level overview of how the EU AI Act applies to the financial services sector, the key compliance challenges it raises, and the most relevant recent regulatory developments, including the Digital Omnibus Package, setting out proposals aimed at simplifying digital regulation, including AI-related rules.

The EU AI Act in financial services: Setting the regulatory baseline

The EU AI Act entered into force on 1 August 2024, and its provisions are being phased in progressively. It is the first comprehensive horizontal regulation of AI in the EU and establishes a risk-based framework that applies across all sectors, including financial services.

The EU AI Act classifies AI systems into four risk tiers. **Prohibited practices** (Article 5) cover AI uses considered unacceptable, such as social scoring by public authorities or real-time remote biometric identification in public spaces. **High-risk AI systems** (Articles 6–49) are subject to extensive compliance requirements, including risk management, data governance, transparency, human oversight and conformity assessments. **Limited-risk (transparency) obligations** (Article 50) apply to certain AI systems (e.g. chatbots, deepfake generators) and require disclosure to users. Finally, **minimal-risk AI systems** are not subject to the substantive requirements applicable to high-risk systems, though voluntary codes of conduct are encouraged.

In addition to defining risk categories, the EU AI Act structures compliance around the allocation of responsibilities along the AI value chain. It distinguishes between several regulated actors, including providers (those who develop an AI system or place it on the market), deployers (those who use an AI system under their authority), as well as importers, distributors and authorised representatives. In financial services, the most relevant roles are typically those of provider and deployer.

This distinction has practical importance for financial institutions. Where an institution develops and

uses its own AI system - for example, a proprietary credit scoring model - it will generally qualify as both provider and deployer and will therefore bear the full set of obligations applicable to high-risk AI systems. By contrast, where an AI system is procured from a third-party vendor, the institution will usually act as a deployer, with obligations focused on the use of the system, human oversight, monitoring, logging, incident reporting and the performance of a fundamental rights impact assessment prior to first use.

However, the allocation of roles is not static. Article 25 of the EU AI Act provides that a deployer may be reclassified as a provider where it makes substantial modifications to a high-risk AI system. This scenario is particularly relevant in financial services, where models supplied by third parties are frequently customised or fine-tuned using proprietary data or adapted to internal credit and risk policies.

Taken together, the risk-based classification and the provider–deployer model form the structural backbone of the EU AI Act. Understanding these elements is a necessary starting point for assessing how the Regulation applies in practice to AI systems deployed across the financial services sector.

High-risk AI in financial services: Scope, classification and practical boundaries

Annex III of the EU AI Act classifies as high-risk certain AI systems commonly deployed in financial services, notably those AI systems intended to be used for evaluating the creditworthiness of natural persons or establishing their credit score (with an exception for financial fraud detection), as well as systems used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

A key question for the sector is the scope of the EU AI Act's definition of an AI system (Article 3(1)), which focuses on machine-based systems capable of inferencing outputs with a degree of autonomy. The recent European Commission's July 2025 guidance has brought greater clarity by confirming that the definition is not intended to capture simpler traditional statistical models and rule-based systems. For a sector that has deployed statistical models at scale for decades, this clarification is significant. At

the same time, the assessment is not purely formal and remains fact-specific. Where statistical techniques are combined with automated inference, adaptive elements or decision-making functionalities, questions of scope may still arise.

This uncertainty directly affects compliance strategies and risk assessments, forcing institutions to make conservative assumptions in the face of potential enforcement risk.

The layered compliance challenge: Regulatory interplay and regulators overlaps

Beyond role allocation, financial institutions must also reconcile the EU AI Act with existing sector specific regimes. Although the European Banking Authority (EBA)'s November 2025 mapping exercise concluded that there are no significant contradictions between the EU AI Act and existing banking and payments legislation, this does not mean these two frameworks integrate seamlessly or that compliance with prudential supervision automatically results in compliance with the EU AI Act. The EBA noted that, while the EU AI Act envisages targeted derogations or other types of regulatory synergies for some requirements, it does not provide such synergies for other high-risk obligations (e.g. human oversight, data governance and cybersecurity), even where EU financial services law already contains extensive requirements (notably under DORA and CRR/CRD). Prudential regimes focus on financial stability, while the EU AI Act is centred on the protection of fundamental rights. As a result, institutions will often be able to leverage existing model risk and ICT controls, but will still need to evidence and operationalise EU AI Act requirements in parallel, particularly in areas such as bias testing and data governance.

In parallel, the GDPR restricts automated decision-making (which may arise in credit-scoring scenarios where a credit institution draws strongly on the score) and requires meaningful information to be provided to individuals (which operate in parallel to those transparency obligations under the EU AI Act). It also requires a data protection impact assessment for high-risk automated processing, while the EU AI Act requires a fundamental rights impact assessment for high-risk AI systems (i.e. different

instruments with different scopes, triggers and addresses). Financial institutions deploying credit scoring models must carry out both and ensure consistency, despite the absence of a formal alignment mechanism or clear guidance on how conflicts should be resolved.

Taken together, this results in a layered compliance landscape in which overlapping regulatory frameworks may apply simultaneously, sometimes duplicating obligations and, in other cases, pulling institutions in different compliance directions.

Furthermore, since AI Act and GDPR matters may be enforced at country level by different regulators having either competing or overlapping competences, this multiple-layer regulatory framework is factored by a fragmentation of competent regulators and natural lack of coordination, which is not addressed by European legislations. Thus, legal uncertainty and enforcement priorities will directly result from this fragmentation.

Recalibrating the framework: The Digital Omnibus Package

In November 2025, the European Commission published the Digital Omnibus Package, proposing targeted amendments to several digital regulations, including the EU AI Act and the GDPR. While the legislative process is ongoing and the final text may still evolve, the main areas of reform are now taking shape.

Postponement of high-risk obligations

One of the most consequential amendments in the Digital Omnibus on AI is the postponement of the application date for high-risk requirements. Recent negotiating texts suggest a move towards fixed application dates, with high-risk AI systems under Annex III expected to become subject to the core obligations in late 2027, and product-embedded systems at a later stage. While this direction appears to be gaining traction, the legislative process remains ongoing, and the final timetable has yet to be confirmed. The proposed postponement would provide additional breathing room for the market, while aiming to improve predictability around implementation timelines.

Facilitating data use for AI

The Digital Omnibus Package proposes targeted adjustments to the GDPR, and the EU AI Act aimed at facilitating the use of data in AI development while maintaining core safeguards. On the GDPR side, it clarifies that legitimate interest may serve as a legal basis for developing and operating AI systems (subject to additional safeguards and a reinforced right to object), and introduces a limited framework allowing the residual presence of special category data in datasets. In parallel, the AI Act Omnibus proposes to ease conditions for processing special category data for bias detection, an approach that has been questioned by supervisory authorities. The scope and practical impact of these changes remain subject to the outcome of the ongoing legislative negotiations.

The supervisory coordination gap

Under the EU AI Act, market surveillance of AI systems used in financial services remains primarily with national financial supervisors, supported by EU-level coordination through the AI Office and sectoral bodies such as the EBA, EIOPA and ESMA.

While the Digital Omnibus seeks to reduce fragmentation by strengthening the AI Office's role for certain systems, it does not eliminate the potential for overlap with prudential supervision at the use-case level. As a result, EU AI Act compliance and prudential oversight are likely to continue evolving in parallel, rather than within a fully unified supervisory framework.

What practitioners should do now

Institutions should not wait for full regulatory clarity, which may reasonably take years. Every AI system currently in use must be mapped against the EU AI Act's risk categories, extending model risk management frameworks to cover bias, data governance and monitoring, and ensuring governance and contractual arrangements support both provider and deployer obligations.

Financial institutions should continue to monitor developments at both the EU level (AI Office, EBA, EIOPA, ESMA) and the national level (ACPR, BaFin, Bank of Spain, CSSF and equivalents), and maintain the organisational flexibility to adjust course as the regulatory framework stabilises. This will require coordination across legal, compliance, data and risk functions.

While the Digital Omnibus might hopefully provide targeted relief, it will not remove the underlying complexity of the regulatory landscape, making early, flexible governance a key differentiator.

Authored by Rémy Schlich, Clara Lazaro, Anais Ligot, and Joanna Rozanska.

Contacts

Rémy Schlich

Senior Associate

Paris

Email me

Clara Lázaro

Senior Associate

Madrid

Email me

Anaïs Ligot

Senior Associate

Paris

Email me

Joanna Rozanska

Senior Associate

Madrid

Email me