Brussels, 13 March 2026
FINAL

EACB Position Paper on the AI Omnibus

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 29 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,400 locally operating banks and 35,150 outlets cooperative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 228 million customers, mainly consumers, retailers and communities. The cooperative banks in Europe represent 91 million members and 747,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Table of Contents

Introduction

Artificial intelligence (AI) has become a central issue for the European Union's economic future. Mario **Draghi's and Enrico Letta's reports** warn that the EU risks falling behind global competitors in digital technologies, including AI, and stress that competitiveness depends on stronger innovation, the ability to scale companies, and **regulation that supports,** rather than hinders, **technological development**.

Draghi highlights AI as a key driver of productivity but points to Europe's weaknesses in investment and core infrastructure, calling for clearer and more **predictable rules** to avoid slowing innovation. From a Single Market perspective, Letta argues for modernised, simpler EU rules that better support digital technologies and make it easier for companies to operate.

These concerns are directly relevant to the AI Act, which the Commission is now seeking to simplify through the AI Omnibus by proposing a series of what it describes as 'targeted amendments'.

While **we support and welcome the Commission's intention to simplify** certain aspects of the AI Act, we believe that a stronger and **more appropriate decision** would have been **to focus**, in the months preceding

the AI Act entry into application of key provisions on 2 August 2026, **solely on Art. 113**, commonly referred to as the **'stop-the-clock' measure for high-risk AI system requirements**.

The stop-the-clock responds to real implementation challenges and aligns with the calls by Draghi and Letta for a more pragmatic approach. Its inclusion within a broader package of amendments raises concerns. Combining the stop-the-clock with broader changes risks accelerating negotiations on all proposed amendments, without sufficient time to properly consider the merits and possible downsides of the Commission's proposals. This will not serve the objectives of a meaningful omnibus.

In terms of timing, it should be noted that the applicability of the provisions, particularly those concerning high-risk AI systems, is imminent (2 August 2026). To ensure long-term planning capabilities, it is therefore imperative that the AI Omnibus on AI or any postponement of the deadline be adopted sufficiently in advance of 2 August 2026.

Key priority – Carving out the 'stop-the-clock' provision from the AI Omnibus

The success of the AI Act will largely depend on how workable its rules are in practice. At this stage, cooperative banks, and the banking sector more broadly, are facing significant uncertainty due to the absence of clear, operational rules and guidelines, some of which are still under development. Many high-risk AI system obligations are also expected to be further specified through EU standards that have not yet been developed. In addition, delays in the designation of national competent authorities and conformity assessment bodies add to this uncertainty. Taken together, these factors create substantial compliance uncertainty.

As a **primary solution**, we strongly **recommend** that the co-legislators **carve out the 'stop-the-clock' provision** from the AI Omnibus and **present it as a standalone proposal**, rather than bundling it together with the other amendments included in the AI Omnibus.

With regard to the wording in Art. 113, the suggestion in the text that the Commission would adopt a decision confirming that adequate measures in support of compliance with Chapter III are available, in order to trigger a shorter (6 months) deadline, introduces legal uncertainty and confers a subjective discretionary power on the Commission. This conditional approach creates considerable legal uncertainty and an inability to plan long-term, as obligated parties cannot predict the point in time at which the Commission would determine that such 'adequate measures' are in place, neither in terms of timing nor content.

The core question remains when support measures and standards would be deemed sufficient by the Commission. This is particularly important given the complexity of our members' internal AI and model landscapes, as well as the possible need for external supervisory approvals for changes. For these reasons, **we suggest the deletion of any references to the Commission's decision power**.

In addition, from the perspective of cooperative banks and financial institutions more broadly, the conditional approach creates significant operational challenges. Implementing Chapter III obligations requires multi-stage internal planning, including governance adjustments, IT changes, documentation and alignment with existing risk-management and approval cycles. Institutions cannot indefinitely reserve capacity for future requirements whose content and timing are unknown.

Finally, the current inconsistency in application dates, 2027 for Annex III and 2028 for Annex I, creates uncertainty. **We** therefore **suggest a single, clear 2028 application date for both Annex III and Annex I**.

Summary:

1) Carve-out Art. 113 from the AI Omnibus proposal
2) Adjust Art. 113 by deleting any references to the Commission's discretionary decision power and suggest a single, clear 2028 application date for both Annex III and Annex I.

Comments on the Commission's suggested changes to the AI Omnibus

Do not amend AI Act Art. 4 on AI literacy

AI literacy is an essential skill for everyone involved in the development and use of AI systems. In sectors such as banking, organisations frequently work with various external suppliers and subcontractors. As AI technologies become increasingly integrated into products and services throughout supply chains, the importance of ensuring sufficient AI literacy is similarly emphasised.

We do not support the Commission's proposal to amend Art. 4 of the AI Act; instead, we believe that it should remain the responsibility of each organisation to ensure their staff possess the level of AI literacy appropriate to the types of AI deployed within their operations.

Amend AI Act Art. 10 AI Act and Art. 4a AI Omnibus regarding processing of special categories of personal data for bias detection and correction

We propose clarifying that the requirement to detect and correct bias should not obligate providers or deployers to collect special categories of personal data unless such processing is already necessary for delivering their products and services. Collecting and processing special categories of data involves new risks and imposes additional regulatory burdens, as organisations must maintain robust controls to ensure careful handling of this data. Both the current amendment with **Art. 4a and Art. 10(5) of the AI Act lack sufficient clarity regarding whether the duty to detect and control bias necessitates collecting special categories of personal data, or whether providers of high-risk systems would be deemed non-compliant with Art. 10 AI Act and Art. 4a of the AI Omnibus** if they attempt to address bias using only existing or synthetic data. We emphasise the importance of practical guidance to help organisations meet this requirement.

Moreover, **we do not support the proposed change relocating AI Act Art. 10(5) from Chapter III, Section 2 (high-risk system requirements) to Chapter I (general provisions)**. Such a move creates uncertainty regarding which party is responsible for detecting and correcting bias. This obligation is especially difficult for deployers, as they may lack the necessary technical details and access to the system. We recommend that this responsibility should remain a requirement tied to the system, with the provider as the primary party responsible for fulfilling the obligation.

Amend AI Act Art. 6 point 4 as proposed by the Commission

In line with the Commission's drive for regulatory simplification, **we endorse the proposed amendments to Art. 6(4) of the AI Act relating to the registration of AI systems**. Specifically, we support the requirement for providers of AI systems that are used in high-risk areas but for which the provider has concluded that they are not high-risk to maintain documentation and assessment records regarding the applicability of Art. 6(4). This approach aligns well with existing financial services regulations, which emphasise that compliance measures should be proportionate to the level of risk posed by the system. The Commission's changes reinforce this

principle. Banks already have robust internal control and risk management obligations, which are further strengthened by oversight from national competent authorities and sector-specific regulators. As such, we do not consider the original AI Act registration requirements to offer additional protection for individuals affected by these AI systems beyond what is already ensured through sectoral regulation.

Preserve consistent requirements regardless of company size

The AI Omnibus proposal seeks to extend to small and mid-cap companies certain advantages that were initially reserved to SMEs. While simplification is a legitimate objective for small businesses, it should not result in a lowering of security requirements for AI systems, nor should it create an uneven playing field. It is important to recall that the value, sensitivity and volume of data processed by a company are not necessarily proportional to its size. Therefore, requirements must remain consistent regardless of the entity's size, in order to preserve overall market trust and a high level of protection for user's data.

Further changes not addressed in the AI Omnibus

Amend AI Act's definition of an 'AI system' to exclude well-established statistical methods

The AI Omnibus proposal presents a timely and important opportunity to clarify in the Level 1 legal text of the AI Act that well-established statistical methods, such as logistic regression (LR) and generalised linear models, are decades-old, transparent and already regulated techniques and therefore fall outside the scope of the definition of an AI system under the AI Act.

While the Omnibus introduces several improvements, some interpretation issues under the AI Act remain. In particular, the definition of AI systems under Art. 3 is still broad and interpreted differently in practice. Financial institutions require a clear distinction between classic software and AI systems to ensure they appropriately meet their obligations. For example, it is not always clear whether statistical processes such as LR will, in the future, be considered subject to relevant prudential AI obligations, even though such regressions have a limited learning capacity and a very different risk profile compared with advanced AI systems.

The February 2025 Commission Guidelines on the definition of an AI system clearly state that *'systems used to improve mathematical optimisation or to accelerate and approximate traditional, well-established optimisation methods, such as linear or logistic regression methods, fall outside the scope of the AI system definition'*. However, they do not provide unambiguous clarity regarding the boundary between basic and complex data processing, or whether this distinction applies only to optimisation of traditional processes or also to applications such as classification, forecasts or scoring.

The absence of explicit legislative wording has already resulted in diverging interpretations by some national authorities who have doubts and raised questions in the context of the AI Board whether LR qualifies as an AI system under the Act. Others Member States (including BE, CZ, DE, IE, IT, ES, NL, GR, SE) and the ECB confirmed in June 2025 the view that credit scoring based on LR should not be considered an AI system[1].

The AI Omnibus offers an opportunity to introduce a simple, explicit clarification directly into the AI Act.

[1] Meeting of the AI Board Subgroup of AI in Financial Services, 6 June 2025. Minutes on the meeting are avaialble here.

Ensuring the AI Act itself explicitly excludes statistical methods such as LR and generalised linear models would prevent fragmentation, support coherent supervision, and avoid inconsistent classification across jurisdictions. Looking at LR specifically, misclassifying it as AI system would:

- Impose disproportionate compliance burdens on banks and not only on banks[2], treating all logistic regressions as high risk could require remediation for more than 50% of a bank's models, creating a significant documentation and compliance workload and making it difficult to meet AI Act deadlines for high-risk systems. Moreover, the more constraints and obligations are added to such systems, the harder it becomes for them to operate optimally, which can increase development costs and extend deployment times.

- Create a mismatch between the AI Act's high-risk requirements and the real risk profile LR models. LR relies on well-understood, highly explainable statistical methods already covered by existing Model Risk Management frameworks (documentation, governance, backtesting, validation, etc.). Applying the full set of high-risk AI obligations to such models would divert regulatory focus away from emerging technologies that pose genuinely higher risks.

Without explicit exclusion, supervisors risk being forced to divert scarce resources toward more transparent and explainable low-risk statistical methods rather than the high-risk, opaque, adaptive AI systems the Act aims to regulate.

➢ **We ask to use the AI Omnibus to explicitly amend the AI Act's definition of an 'AI system' so that LR and comparable long-standing statistical techniques, are clearly excluded when used on a stand-alone basis.**

This small but essential clarification would:

- Reinforce the Commission's own interpretative guidance
- Ensure Union-wide regulatory certainty
- Prevent disproportionate burdens on low-risk tools
- Strengthen competitiveness and supervisory coherence
- Enable the AI Act to focus on *actual* AI risks

Clarify the definition of 'machine-based' in the AI Act for alignment with DORA

While the AI Act and DORA regulate different subject matters, AI capabilities are increasingly embedded within ICT services and assets governed under sectoral digital resilience frameworks. In this context, legal coherence requires that the notion of a 'machine-based system' be interpreted functionally, so that the presence of an AI component does not automatically extend regulatory scope to the entirety of an ICT infrastructure where the AI performs only an auxiliary or narrowly defined function. Against this background, the definition of an AI system in Art. 3(1), together with the definitions of GPAI models (Art. 3(63)) and GPAI systems (Art. 3(66)), are particularly relevant given the increasing integration of GPAI models into ICT services and assets, often as embedded components of broader systems.

Especially because of the AI Omnibus proposal, we consider it important to clarify that the term 'machine-based' in the definition of an AI system is interpreted in a manner consistent with the functional approach

[2] Joint statement on 'Understanding Credit scoring: Techniques and Distinctions from Artificial Intelligence'. Additional documents and papers on the matter have been shared with both DG CNECT and DG FISMA.

used under DORA for ICT services and assets. Under DORA, ICT services are assessed based on whether they support the performance of a business activity, and financial entities remain fully responsible for compliance when relying on such services, including where they are provided by third parties (Art. 28(1)(a) DORA). A similar functional approach is reflected in Q&A DORA030 - 2999, which clarifies how embedded or ancillary ICT components should be assessed.

Indeed, DORA adopts a functional and risk-based approach to the classification of ICT services, focusing on whether a service supports the performance of a business activity, rather than on the specific technology used or on formal distinctions between components. Responsibility for compliance remains with the financial entity even where ICT services are outsourced and supervisory expectations are calibrated accordingly. As AI models, including GPAI models, are increasingly embedded within broader ICT services and assets rather than deployed as standalone systems, a similar functional approach is necessary when interpreting the notion of a 'machine-based system' under the AI Act.

We believe this logic should also inform the interpretation of the AI Act, in order to ensure coherence between the two frameworks and avoid legal uncertainty or inconsistent supervisory outcomes.

Additional considerations

Align FRIA (AI Act) and DPIA (GDPR) obligations and interaction with GDPR

We suggest clarifying the relationship between the Fundamental Rights Impact Assessment under Art. 27 of the AI Act and existing risk-assessment obligations under the GDPR (in particular the DPIA under Art. 35).

In particular, these assessments may significantly overlap in certain use cases, particularly when high-risk AI systems rely on personal data. In such situations, the scope, methodology and documentation requirements can lead to duplicative compliance efforts. To avoid duplication and disproportionate compliance burdens, the AI Act should explicitly recognise equivalence or reuse mechanisms. Where a DPIA already covers relevant fundamental rights risks, a separate FRIA should not be required or should be allowed to rely on the existing DPIA. A single risk-assessment approach or mutual recognition of existing assessments should be introduced.

Similarly, the interaction between the AI Act risk-management framework and GDPR obligations should be clarified to ensure legal certainty and avoid conflicting supervisory expectations. In particular, alignment should be ensured regarding data-governance requirements, risk-assessment procedures, prior-consultation obligations and supervisory coordination between competent authorities.

We note that the AI Office is working jointly with the EDPB on guidelines addressing the interplay between the AI Act and the GDPR, which we believe could provide practical solutions to the issues outlined above and support consistent supervisory practice.

Clarify the responsibilities for AI systems embedded in ICT services

Further clarification is needed regarding the allocation of responsibilities where AI systems are embedded within ICT services, software solutions, or outsourcing arrangements provided by third parties. A functional and risk-based approach, consistent with DORA, should be ensured. We understand that among the various

guidelines the Commission is preparing there is one on the practical application of rules for responsibilities along the AI value chain. We believe this could represent an opportunity to provide the necessary clarity. Moreover, we also look forward to the implementation of Art. 25.4 on responsibilities along the AI value chain where the AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used for or integrated into high-risk AI systems.

Embedded third-party AI systems used for data analysis purposes

The AI Act should provide greater legal certainty regarding the treatment of AI components embedded within ICT systems or services supplied by third parties, where such systems are used solely for analytical, preparatory or technical support purposes (e.g. data analysis, risk assessment support, or processing functions).

In many cases, these systems do not autonomously produce decisions nor materially influence decisions affecting individuals or fundamental rights. However, banks may still face uncertainty as to whether they must comply with the full set of high-risk obligations.

While Art. 6(3) AI Act already provides a mechanism allowing providers to justify that certain systems listed in Annex III should not be classified as high-risk where they only perform supportive functions, its practical application remains unclear, particularly for embedded third-party components within broader ICT systems.

To ensure consistent supervisory practice, the AI Act should, for example, clarify through guidelines that AI systems performing purely preparatory, analytical or technical support functions within a broader decision-making process are presumed not to be high-risk, provided that:

- They do not autonomously determine outcomes affecting individuals or fundamental rights; and
- the deploying financial institution ensures appropriate safeguards in areas such as data governance, cybersecurity, privacy and ICT risk management.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Financial Markets, Payments, Digitalisation (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Director for Digitalisation (chiara.delloro@eacb.coop)