German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

on the European Commission's proposal from 19 November 2025 for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 und (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – COM(2025) 836 final

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:

Berlin, 23 February 2026

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
https://die-dk.de/

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Comments on the European Commission's proposal from 19 November 2025 for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 und (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – COM(2025) 836 final

TABLE OF CONTENTS **Page**

Comments on the European Commission's proposal from 19 November 2025 for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 und (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – COM(2025) 836 final

I. General

The German Banking Industry Committee (GBIC) hereby submits its comments on the European Commission's proposal COM(2025)836 (Digital Omnibus on AI). The aim of the proposal is to simplify the application of the AI Regulation (EU) 2024/1689 in practice, to reduce administrative burdens and thereby strengthen innovation and Europe's ability to compete on the global stage. **The GBIC expressly supports these aims.** In the following, you will find our comments on the current status of the proposal, which are not yet final, as we reserve the right to make further comments by the end of the consultation period.

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

Nevertheless, the practical feasibility of the AI Regulation depends largely on clear operational guidelines that are appropriate for the target audience, as well as realistic transition and implementation periods. Particularly in the case of complex sets of requirements (especially for high-risk AI systems), there is a need for reliable scheduling, since institutions have to organise implementation in multi-stage projects and approval processes and must anticipate specific requirements in terms of both content and timing. While it does make sense that the Digital Omnibus on AI is linked to the availability of "adequate measures in support of compliance" (standards, common specifications, guidelines), the regulation must be designed in such a way that it does not lead to new legal uncertainty and an inability to plan long-term.

In addition, the term "adequate measures in support of compliance" remains too vague. This lack of clarity further compounds the inability to plan over the long-term. Legal clarification as to which measures are to be considered "adequate" therefore seems to be essential.

II. On the amendments proposed by the European Commission

1. Amended application and transition periods, Articles 111 and 113 of the AI Act; greater flexibility regarding the entry into force of obligations for high-risk AI (amendments in particular to Article 6, Article 50, Chapter III of the AI Act)

The Digital Omnibus on AI provides for a reorganisation of the application and transition periods for key obligations under the AI Act. For obligations under Chapter III (high-risk AI systems), entry into force is partly linked to the presence of "adequate measures in support of compliance" (in particular harmonised standards, common specifications and guidelines). In addition, Article 113 of the AI Regulation provides for backstop dates to ensure the latest date of application.

Comments on the European Commission's proposal from 19 November 2025 for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 und (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – COM(2025) 836 final

The objective is appropriate and we welcome it in principle. This approach recognises that implementing complex requirements requires robust guidance.

- **Need for clarification and amendments**

In the current proposal, the conditional approach, however, creates considerable legal uncertainty and an inability to plan long-term. The point in time at which the Commission determines that "adequate measures in support of compliance" are in place cannot be predicted by the obligated parties, neither in terms of timing nor content. Against this background, the associated grace period of only six months for high-risk AI systems pursuant to Article 6(2) in conjunction with Annex III of the AI Act is clearly too short.
This short grace period is practically impossible to implement, especially for financial institutions in the credit industry. The implementation of the extensive obligations under Chapter III of the AI Act requires early and reliable planning, particularly with regard to governance structures, internal control mechanisms, IT adjustments, documentation and the integration of existing risk and compliance processes. It is not possible to carry out reliable resource and project planning when neither the specific date of application nor the content of the relevant guidelines and standards have been determined. Financial institutions cannot regularly reserve capacity for future requirements whose content is still undefined. There is therefore a considerable risk of placing an excessive burden on obligated parties.

- **Backstop dates and static postponement**

The backstop dates provided for in Article 113 of the AI Act are generally welcome as a contribution to legal certainty, as they set an absolute latest date of application. However, in the opinion of the GBIC, this should not merely serve as a backstop. Instead, it would be appropriate to postpone application of the obligations for high-risk AI systems under Annex III of the AI Act further into the future. A fixed application date from December 2027 for all high- risk AI would better reflect the actual implementation cycles, the complexity of the requirements and close links with existing regulatory requirements.

- **Guideline quality**

In addition, there is a need for clear requirements when formulating the promised guidelines. They should be formulated in a manner that is more closely tailored to their target audience and is more relevant in practice. Clear and specific guidelines are required, geared to practical implementation, for example in the form of question-and-answer catalogues or standardised application scenarios for financial practice. This would increase legal certainty, avoid regulatory duplication and support the effective and appropriate implementation of the AI Act in the banking sector.

The grace period for existing systems provided for in Article 111(2) of the AI Act should also clearly define the conditions under which it can be assumed that systems "*are subject to significant changes in their designs*" after they have been placed on the market or put into service. This is because it largely determines whether and to what extent the grace period actually provides grandfathering protection in practice.

Comments on the European Commission's proposal from 19 November 2025 for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 und (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – COM(2025) 836 final

2. Amended AI literacy requirements (Article 4 AI Act)

The revised version of Article 4 of the AI Act stipulates that a general obligation to ensure AI literacy within a business will no longer be addressed to the same extent as before. Instead, measures to promote general AI literacy are to be supported by the Commission and the member states. Specific training and literacy requirements in the context of the use of high-risk AI systems remain unaffected by this.

The departure from a potentially narrow or formalistic interpretation of Article 4 of the AI Act is generally to be welcomed, as it dispenses with a rigid, normatively over-regulated training obligation and thus – as previously implied by the AI Office – no narrow or formalistic interpretation of the literacy requirements are to be applied.

Regardless of this, however, there is already a structural need for training and qualification in banking practice, which arises indirectly from regulatory requirements (including Article 13 DORA on governance). Deleting or removing Article 4 would not therefore lead to any actual relief measures, but would require clear contextualisation and consistency with financial supervisory law.

In order to prevent fragmentation and new uncertainties, member states' initiatives to promote AI literacy should be harmonised to the greatest extent possible. Central coordination and binding EU-wide guidelines from the Commission are needed to ensure that providers and deployers are not confronted with differing national requirements and expectations.

3. Extended use of sensitive personal data for bias management (new Article 4a AI Act; amending Article 10(5) AI Act)

The AI Omnibus restructures the legal base for using special categories of personal data for bias detection and correction. Article 10 (5) of the AI Act is to be deleted and its underlying approach is to be moved to a new Article 4a. In substance, the approach previously limited to high-risk AI, is to be broadened to cover all AI systems and GPAI models (Article 4a (2)).

The GBIC welcomes this approach, as it establishes for the first time a clear European legal framework for bias management involving the use of special categories of personal data within the meaning of the GDPR. This is consistent with proposals to adapt the GDPR as part of the Digital Omnibus (COM(2025) 837).[1]
The fact that the new Article 4a of the AI Act links the legality of such data processing to strict and appropriate safeguards is especially positive. This includes, in particular, the requirement that effective bias detection or correction cannot be achieved by less intrusive means (such as anonymised or synthetic data). This approach complies with the requirements of the GDPR and at the same time creates a robust basis for effective bias management in practice.

[1] See, in particular, the assessment in GBIC comments on Article 3 of the European Commission's proposed 'Digital Omnibus' Regulation of 19 November 2025 amending the GDPR of February 2026.

Extending this framework beyond high-risk AI systems to all AI systems and GPAI models is also appropriate. It reflects the practical reality that fairness, non-discrimination and model validation are not issues confined to high-risk applications. Overall, these clarifications strengthen the data basis for quality and risk assessments and increase legal certainty when using special categories of data in AI-enabled processes.

- **Need for clarification and adjustment (consistency between AI Act↔GDPR)**

In order to avoid inconsistency between the AI Act and the GDPR and to ensure legal certainty, Article 4a of the AI Act should establish a robust and directly applicable legal basis for the processing of sensitive data for bias management in the situations covered. At present, there is a structural inconsistency between the Recital 6, which point to a broader application (beyond high-risk AI deployers), and Article 4a(1), which still refers only to high-risk AI systems. In addition, Article 4a(2) appears to extend the approach, but the wording "may apply" is ambiguous and risks divergent interpretations, particularly as regards the conditions of necessity and proportionality. This ambiguity may lead to additional legal uncertainty under Article 9 GDPR rather than providing the intended clarification.

We therefore recommend integrating the substance of Article 4a(2) into Article 4a(1), so that the scope and legal effect are clearly extended to all AI systems and GPAI models (and, where relevant, AI models more generally), in line with the recitals.

Furthermore, the relaxing of requirements for bias management should not be undermined by additional secondary obligations that are practically impossible to fulfil. In particular, obligations to check or remove data from the database should not be designed in such a way that they either come to nothing or create new legal uncertainty. In addition, the wording of the provision must take into account that the broad scope of Article 9(1) GDPR can also cover "mixed data sets", thereby unnecessarily complicating fairness and bias analyses. In this regard, we refer to comments in the GBIC position paper on the Digital Omnibus.

4. Streamlining of registration requirements through self-assessment of certain high-risk AI systems (Article 6(3, 4) and Article 49 AI Act)

Under Article 6(3) of the AI Act, providers may already self-asses, under the conditions set out therein, that certain AI systems listed in Annex III as not high-risk. The Omnibus amendment does not alter this self-assessment mechanism as such. Rather, it amends Article 6 (4) in conjunction with Article 49(2) AI Act to remove the obligation to register those systems in the EU database where the provider has concluded, on the basis of Article 6(3), that the system is not high-risk. The self-assessment is to be documented pursuant to Article 6(4) AI Act and made available to the competent authorities upon request. The remaining material requirements of the AI Act, in particular those pursuant to Article 50 et seq. AI Act, remain unaffected.

In principle, the removal of the registration requirement can be considered a pragmatic measure to reduce administrative burdens, particularly for AI systems developed and used internally. However, the practical impact may remain limited if the scope and consequences of incorrect self-assessment are not clearly regulated and the remaining obligations under the AI Act remain unchanged. This This may result in legal and liability uncertainty and could diminish the practical effectiveness of the intended relief.

- **Need for clarification and adjustment (consistency between AI Act↔GDPR)**

From a data protection perspective, additional clarification is needed, particularly for externally sourced AI systems. Where Annex III systems are exempted from registration in the EU database following a provider self-assessment under Article 6(3), downstream users may no longer be able to readily verify the basis on which a system is considered "not high-risk". For deployers, this lack of transparency is not merely a compliance issue under the AI Act; it directly affects their ability to meet GDPR accountability requirements when integrating third-party AI into processing operations. In practice, uncertainty as to whether a "non-high-risk" qualification is based on an official conformity assessment or on a provider's self-assessment complicates vendor due diligence, the allocation of roles and responsibilities (e.g. controller/processor arrangements), and the assessment of appropriate safeguards, including the need for a DPIA.

To preserve transparency without reinstating the full registration burden, targeted provider-to-deployer disclosure obligations should be introduced. Providers placing AI systems on the market should be required to clearly indicate whether the "non-high-risk" qualification relies on a self-assessment under Article 6(3), and to provide a concise summary of the key reasons and underlying assumptions relevant for deployers' governance and data protection compliance. This would support GDPR-compliant third-party risk management, facilitate integration into existing control frameworks, and increase legal certainty overall.

5. Flexibility in post-market monitoring (amendments to Article 72 et seq. AI Act)

We welcome, in principle, the planned relaxation of post-market monitoring by removing the requirement for a mandatory, rigid monitoring plan. The focus on flexible, risk-based guidelines by the Commission opens up the possibility of aligning post-market monitoring more closely with the actual use case, the specific risk profile and existing internal control and monitoring processes.

However, in practice, the added value of this new regulation depends largely on the specific wording of the promised guidelines. These must be geared towards implementation, tailored to the target audience and sufficiently specific so as to enable institutions to implement post-market obligations consistently and efficiently. Clear guidance is needed that points to possible solutions rather than merely describing known problem areas in abstract terms. A structured presentation, for example in the form of question-and-answer catalogues or standardised application scenarios, would increase legal certainty and greatly simplify effective implementation of post-market obligations.

6. Powers of the authorities to protect fundamental rights and fostering cooperation with market surveillance authorities (amendments to Article 77 of the AI Act)

We generally welcome the consolidation of regulatory powers provided for in Article 77 of the AI Act and the involvement of market surveillance authorities in the exchange of information between authorities. Centralised coordination of requests for information and documentation appears to be an appropriate way of avoiding multiple requests, streamlining procedures and reducing the administrative burden on businesses.

However, this assessment depends on certain requirements: consolidation should therefore be accompanied by a strict transparency requirement. Although requests from other authorities are to be channelled through the market surveillance authorities, the current regulation does not provide for affected market participants to be informed that information is being requested, when this is happening, or at whose instigation. For businesses, this leaves unanswered the question of when and in what context – possibly involving infringements of fundamental rights – access to, in particular, sensitive, confidential or business-critical data is granted.

In the opinion of the banking industry, it is absolutely essential that the coordinating body has an obligation to provide such information. Market participants must at least be informed about which authority initiated a query, for what purpose and in what legal context the requested information is to be used.

III. Further need for improvement

1. Lack of clarification on the definition of AI systems and need for unified interpretation (Article 3 No. 1, Article 2, Recitals 12 AI Act)

Despite individual improvements, the Digital Omnibus on AI has failed to address key interpretation problems found within the AI Act. The definition of AI systems in accordance with Article 3, in particular, remains unclear and is interpreted heterogeneously in practice. The Omnibus does not address this structural bottleneck, even though it specifically cites existing delimitation issues.

The definition remains broad and does not focus on a specific technology, leading to a lack of legal certainty. Financial institutions require a clear distinction between classic software and AI systems in order to ensure they appropriately meet their obligations. The Omnibus on AI does not reduce confusion regarding definitions – in particular, it does not clarify whether statistical processes such as logistic regression will, in the future, be considered subject to relevant prudential AI obligations. This despite the fact that such regressions only have a limited ability to learn and have a completely different risk profile to that of advanced AI systems.

The European Commission's guidelines from February 2025 also do not provide unambiguous clarity. They do clarify that models such as linear or logistic regressions represent "basic data processing" and are therefore not included in the definition of AI. However, it remains unclear where exactly the border between basic and complex data processing lies. It is also unclear whether or not this categorisation applies only to the optimisation of traditional processes, or also to applications such as classification, forecasts or scoring.

There is additional uncertainty regarding the criteria of many years of use as an indication of "basic data processing".[2] There is no definition of many years, the criteria is not practical and it also contradicts the AI Act's approach of not focusing on a specific technology, as the classification depends on historic use and not on function or risk.

[2] According to the EC guidelines: "An indication that a system does not transcend basic data processing could be that it has been used in consolidated manner for many years."

Overall, the guidelines do no provide adequate operationalisable criteria. Financial institutions are therefore unable to reliably determine whether or not software is to be categorised as an AI system. This room for interpretation increases the risk that national supervisory authorities will diverge in their interpretations as to the definition of an AI system. The GBIC is therefore calling for a unified, consistent and harmonised application of the definition of AI in order to guarantee legal certainty and a level playing field.

2. Lack of clear distinction between high-risk AI systems; clarification on exclusion of fraud prevention systems (Article 6, Annex III lit. 5, Article 7 AI Act).

The Digital Omnibus on AI still has not solved the underlying question as to what, exactly, counts as a high-risk AI system and what does not. The European Commission has announced, in their communication from 4 December 2025, that they would be publishing additional guidelines on the application of Article 6 and Annex III. However, the proposed amendments currently do not contain any concrete tightening of the definitions. These clarifications, however, are necessary and should be included in the guidelines in order to remove the existing legal uncertainty and difficulties with interpretation.

The GBIC calls, in particular, for clarification that in contrast to AI supported systems for performing credit checks on natural persons, AI systems designed to prevent fraud are not subject to high-risk regimes. This includes, in particular, AI systems that provide support for preventing money laundering and financing terrorism, screening for sanctions or to identifying fraudulent payment transactions. This explicit exception is key to risk and resource planning, as fraud prevention systems are a significant component of compliance architecture. Without clear confirmation from the European Commission, however, there is a risk that national interpretations will differ, leading to a fragmented application of the AI Act.

There is thus an urgent need for guidelines to be published as soon as possible. These guidelines should (1) set out clear criteria for determining which applications are high-risk, (2) provide practical application examples and (3) clearly confirm that fraud prevention systems are not included in this category. Considering the significant effect they will have on planning for projects, resources and compliance, these guidelines must be published much earlier than originally planned, so that institutions can integrate requirements from the AI Act efficiently and consistently into existing governance and monitoring processes.

3. Clarification of roles in the AI value added chain (Article 3 lit. 4-13, Articles 16-29, Articles 52-55, Annex XII AI Act)

The distinction between the roles of provider and deployer remains unclear – in particular for AI systems based on GPAI models. While the Digital Omnibus on AI does expand the AI Office's supervisory role to specific GPAI supported systems, the responsibilities along the value-added chain remain imprecise and in need of clear definitions. In the financial sector, in particular, in which AI models are embedded within complex technical and organisational structures, there is uncertainty regarding which deployers are responsible for conformity, monitoring and reporting obligations. This is particularly true in the case of fine tuning, significant changes or integration into proprietary systems.

In addition, typical situations within the banking industry create further uncertainty in regard to roles, for example in the case of AI systems that are used by multiple institutions within a group, or models that are developed jointly with third-party providers. In these cases, where technical responsibility, training and governance are shared, the distinction between the roles of provider and deployer becomes blurred.

A clear and binding distinction between roles defined by the AI office would reduce these structural uncertainties and make it significantly easier to integrate complex, GPAI based models into existing structures within the banks.

4. Relationship between the requirements in the AI Act and existing bank regulatory requirements; use of established reporting channels and harmonisation of supervisory practices (Article 9, Article 17, Article 62 et seq. AI Act)

The AI Act acknowledges that the financial sector already practices especially comprehensive risk and quality management. The existing, comprehensive rules for bank supervision apply regardless of the technology in use, and necessarily also include AI systems. As such, many of the requirements within the AI Act are already covered. In light of this, in a resolution from November 2025, the EU parliament determined that the existing sector-specific regulations are fundamentally suitable to also address the risks posed by AI. Key requirements from the AI Act are already covered by existing prudential frameworks, such as CRR/CRD IV, DORA, CCD, MCD and PSD. The EBA's gap analysis from November 2025 came to the same conclusion, stating that there are significant overlaps in the contents of these regulations and that financial supervisory law already encompasses requirements put forward by the AI Act to a great extent.

At the same time, the AI Act currently reflects the financial services regulatory framework only in a limited and largely non-systematic manner. While the Act contains certain integration points (including the quality management-related mechanism in Article 17(4) and further sector-relevant linkages, Art. 26 sec. 5 UAbs. 2, Art. 26 sec. 6 UAbs. 2, Art. 18 sec. 3 und Art. 19 Abs. 3 AI-Act), the requirements under Articles 9 to 15 of the AI Act, in particular, contain extensive requirements for risk management, data governance, technical documentation, human oversight and cyber and IT security.This creates a practical challenge for financial institutions. They must implement these obligations without any concrete guidelines on how they interact with other supervisory structures, leading to legal uncertainty as well as parallel and in some cases redundant governance and compliance structures.

To strengthen regulatory coherence, avoid duplicate regulations and increase legal certainty, it would make sense to systematically expand the integrative mechanism proposed in Article 17(4) AI Act to other overlapping obligations. This would reduce regulatory burdens without reducing the level of protection, by ensuring that tried and tested supervisory control and monitoring structures are used when implementing obligations related to AI.

In addition, the GBIC is calling for market surveillance duties to be placed, to the extent possible, in the hands of experienced financial supervisory authorities. Such coordination makes it easier to use established audit practices and knowledge on the risks, business models and monitoring structures within the banking sector.

Existing systems should also be used for reporting obligations in the case of a serious incident. Institutions have access to well established processes using the MVP Portal (the BaFin's reporting and publishing portal), which is used for PSD, DORA and other obligations. Use of this infrastructure would guarantee efficient, proportional reporting processes and avoid additional burdens. In order to promote legal clarity, the crime of "the infringement of obligations under Union law intended to protect fundamental rights" (Article 3 No. 49 lit. c AI Act) should be specified further in order to prevent duplicate reporting and to coherently embed requirements within the existing supervisory framework.

5. Explicit interaction of DPIA (Article 35 GDPR) and FRIA (Article 27 AI Act)

The data protection impact assessment detailed in Article 35 GDPR, as well as the fundamental rights impact assessment for high-risk AI systems in accordance with Article 27 AI Act both have the same goal, which is to systematically identify, evaluate and minimise – if possible – potential risks and freedoms to natural persons before technical systems are developed. Both instruments are based on the preventative risk management approach found in the European Charter of Fundamental Rights. However, at present they are not in alignment with one another in terms or either content or methods. As the goal in each instance is the same, systematic coordination of both assessments seems logical. At present, the requirements run in parallel, so that there is a risk of redundant assessment processes, potentially in different departments due to distributed responsibilities, as well as potentially contradictory judgements as to which legally protected rights are affected. We call for the data protection impact assessment and fundamental rights impact assessment to be more closely coordinated, both structurally and in terms of content, in order to avoid duplicate bureaucratic burdens and increase the practical, legal coherence of these assessments.