bankenverband

Position paper

of the Association of German Banks on a legal framework conducive to AI

July 2025

Lobby Register No R001458
EU Transparency Register No 0764199368-97

Bundesverband deutscher Banken e.V.
(Association of German Banks)
Burgstraße 28
10178 Berlin | Germany
Telephone: +49 30 1663-0
www.bankenverband.de

USt.-IdNr. DE201591882

Introduction

The European Union's Regulation laying down harmonised rules on artificial intelligence (AI Act)[1] creates a comprehensive legal framework to facilitate secure, trustworthy production and use of artificial intelligence. The European Union has thus become a global pioneer in regulating AI. Meanwhile, other regions are world leaders in the development and profitable application of AI. It is therefore crucial that the European legal framework is applied in a manner that facilitates innovation and economic growth. Otherwise, Germany, and indeed all of Europe, will be unable to consistently utilise the opportunities that AI has to offer. This includes:

1. Ensuring that the regulation, which has not yet undergone specification by the European Commission and national legislative bodies, be implemented practically, with legal certainty that is harmonised across the entire European Union. Only then will it offer a net benefit to businesses.

2. Guaranteeing consistent interactions with existing supervisory requirements for banks, and avoiding duplicate regulations.

3. Ensuring that data protection requirements align with the regulatory requirements within the AI Act.

The private banks in Germany have the following proposals, designed to ensure that the Act be implemented with an eye to the future.

1 Requirements for implementing the AI Act

Parts of the Act apply as of February 2025, and other provisions will be implemented by August 2027; unless, of course, regulatory deadlines are adjusted once more. Too many parts of the regulation are still awaiting specification in the form of guidelines, harmonised standards, national implementation laws, etc. These specifications should be finished within the next few months. The following, in particular, must be in focus during specification and application of the Act.

Harmonised definition of AI

The definition of Artificial Intelligence is, obviously, essential for defining the scope of application of the AI Act. If the definition is too broad, it could end up including conventional IT systems, which would burden the economy for no discernible reason. If, on the other hand, the definition

[1] Regulation (EU) 2024/1689 from 13 June 2024.

is too narrow, it will create loopholes, which would jeopardise the political aims of the regulation and their technological neutrality. Despite this, the definition of AI within the regulation still begs several questions. These must be addressed in order to ensure legal certainty.

The banking industry is calling for a definition of AI within the European Economic Area that is both appropriate and selective. After all, the degree to which computer-supported analysis and data processing takes place across an extremely unique software landscape, in all functions and departments, is practically unique to the sector. The majority of these IT systems are conventional and do no use machine learning or self-optimisation in any form. Therefore, they are not AI in accordance with the definition in the AI Act. However, other use cases are more ambiguous: basic statistics processes, such as linear and logistic regressions, do indeed have a very limited capacity to 'learn'. However, there is no black box here, their capabilities are reproducible at all times. They therefore do not represent any of the risks that the regulation is designed to address.

We therefore welcome the fact that the European Commission provided a more precise definition of AI in their Guidelines from February 2025.[2] The guidelines do more than promote a harmonised, European understanding of the concept; they also use specific examples to further define which systems are to be considered Artificial Intelligence and which are not. The guidelines clarify, among other things, that the regression process, which has long been established by the banks as part of credit checks for lending, is not to be considered AI.

However, European Commission Guidelines are not legally binding, and simply provide assistance for entities and supervisory bodies. The Association of German Banks is therefore calling for consistent application of these guidelines within the European Union and throughout all Member States. This is the only way to achieve a harmonised supervisory praxis that offers both legal certainty and equal treatment at all locations and for all market participants. Remember: if the definition of AI is too broad, it will distract from truly risky AI applications that must, justifiably, be subject to legislative guidelines and a dedicated supervisory system. The focus must be on managing the characteristic challenges and risks associated with advanced AI, including questions of falsification, lack of transparency and autonomous decision-making.

Clear and narrow distinctions for high-risk AI applications

In addition to a ban on AI practices that are fundamentally incompatible with European law and shared values, the AI Act focuses on regulating high-risk AI systems. Providers and operators of high-risk AI systems must, in the future, prove that the AI systems meet the regulatory

[2] "Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)", C (2025) 924 final, 2 February 2025.

requirements before making use of such systems, in order to prevent damages to the health and safety, or even the fundamental rights, of people living within the European Union.

In Annex III, the AI Act defines AI use-cases that must be assumed to have a high risk.[3] AI system providers must check whether their AI systems are considered high-risk and then ensure that these systems conform with the regulatory requirements. Our members might, in particular, make use of AI systems to evaluate the creditworthiness of natural persons (Annex III No. 5(b)) or for employment and workers' management (Annex III No. 4), both of which are considered high-risk applications.

AI systems used for the purpose of detecting financial fraud are explicitly excluded from the high-risk AI systems for evaluating creditworthiness named in Annex III No. 5(b). We understand this to refer to AI systems that provide support for preventing money laundering and financing terrorism, to screen for sanctions or to identify fraudulent payment transactions. The European Union should clarify this in their guidelines on high-risk AI systems, which they have said are forthcoming. In addition, these guidelines should include specific use-cases for high-risk AI systems and be published as soon as possible – before the current advised date of February 2026.

Refining separation of roles and extending grandfathering to providers

The AI Act regulates the various participants in the AI value chain in accordance with their role (e.g. provider, operator, distributor, etc.). However, uncertainties remain as to the separation between the role of the provider and that of the operator, including, for example, in the event that a financial institution cooperates with another enterprise, or if an AI system is used within the corporate structure of several banks. This hampers legal certainty and could, as a result, hinder progress. The AI Office should therefore clarify the separation of these roles.

This is particularly important for the question as to whether AI systems already in use will be grandfathered in. The law excludes the operator of high-risk AI systems from the obligations listed in the regulation in the event that the system was placed on the market or put into service before 2 August 2026, and that no significant changes were made to its design thereafter.

A bank that, for example, develops its own high-risk AI system to write references and only operates the system for its own use is, according to the text of the regulation, not just the operator of the system, but also the provider, and would therefore be fully subject to the requirements as of August 2026. Considering the strict sanctions, affected parties might feel obligated to discontinue use of any such AI system due to an abundance of caution. At the same

[3] See Article 6(2) AI Act.

time, however, a footnote in the European Commission's guidelines on the definition of AI systems from February 2025 states that all systems distributed or operational before 2 August 2026 will be subject to the grandfather clause in Article 111(2). The European Commission should fix this contradiction by specifying that the grandfather clause applies both to the operator *and* the provider.

There are also open questions concerning the role of the downstream provider. This is particularly relevant in the context of generative AI based on large language models, that is those largely created by non-European providers. The regulation calls these General-Purpose AI Models (GPAI models). Banks could become downstream providers if they integrate such models into their own AI systems.

The AI regulation states that downstream providers receive transparency information from GPAI providers (Annex XII). However, it is unclear whether the downstream provider also has a legal responsibility in accordance with the regulation. The information the downstream provider has a right to receive would certainly not be adequate to fulfil this responsibility. This is particularly true for the integration of a GPAI model into a high-risk system. It would, in this case, only be possible to fulfil the obligations of a provider in cooperation with the original GPAI model provider; this provision would mean, therefore, that it would be practically impossible to use generative AI for high-risk applications. In addition, there is a need to clarify whether banks, as downstream providers, would be subject to additional reporting obligations to the AI Office, as they could in fact be considered a provider of a general-purpose AI system.

The Association of German Banks therefore calls for the AI Office to clearly delineate these roles.

Ensuring a level playing field and efficient supervisory structures

As addressed above, the AI Act relies on further specification at a later date, in some cases via the European Commission or its AI Office, in some cases by individual member states.

An internal survey of our members revealed that in most cases, the existing rules are simply not ready for implementation. Legislators have yet to create multiple level 2 and 3 regulations, not to mention harmonised European norms. Right now, it seems highly unlikely that these norms will be created on schedule. The norms are supposed to demonstrate how requirements for high-risk AI systems – such as the prescribed risk and quality management systems – could be implemented in practice.

These specifications are essential; they will ensure that regulatory requirements can be implemented with legal certainty. Considering the detailed requirements and their effects, which may have sweeping consequences, market participants must be involved, early and often, in the

creation of these requirements. In addition, enterprises will need an adequate amount of time to implement these requirements. The sheer mass of specifications to come already begs the question: will there be adequate market consultation? The European Commission must carefully examine the current timetable and extend it if necessary.

And of course, implementation throughout the EU should be as harmonised as possible. Divergence, or, worse, a patchwork of disparate national interpretations, will distort competition and must be avoided at all costs. It is therefore essential that member states coordinate closely in the European AI committee and its sub-committees. Similarly, the expert authorities charged with monitoring the regulation on a national level must also work closely together to ensure harmonised interpretation of the law.

The German government is required, by August of this year, to appoint or create the supervisory authority that will oversee the regulations in the AI Act. According to a hearing, they intend to spread responsibility for market surveillance of AI in the financial sector across several authorities. Existing supervisory financial authorities are to be responsible for those AI systems directly involved in financial services, while the Bundesnetzagentur, Germany's telecommunications authority, is to supervise all other AI systems used by financial institutions. This division of responsibility is in direct contradiction to the fundamental goal of providing efficient, uncomplicated supervision without any duplicate structures. It must already be clear that two different supervisory bodies could lead to confusion about who is responsible for what, not to mention potential conflicts and redundancies. To avoid this confusion, financial supervisory authorities should be solely responsible for monitoring AI systems in banks, regardless of the actual system application. The Bundesnetzagentur can act as a central coordination and competence body, guaranteeing consistent supervisory practice by coordinating with financial supervisory authorities and the authorities responsible for other regulated sectors.

2. Coordination with existing banking supervisory law

The regulation rightly identifies the high standards that already exist within the financial sector as a result of existing regulatory and supervisory requirements; it acknowledges these when detailing risk management requirements, as well as the requirement to set up a quality management system.[4] The existing, comprehensive rules for bank supervision apply regardless

[4] See Article 17(4) (Quality management system) and Article 26(5) sentence 5 (Obligations of deployers of high-risk AI systems), recital 158 of the Act, among others.

of the technology in use, and necessarily also include AI systems. The requirements listed in the AI Act will therefore already be covered in large part by existing requirements for banks.

In principle, we welcome efforts by the European Banking Authority to align requirements in the Act with existing requirements for bank supervision. However, it is very important that they identify those AI Act requirements that are already being met by the banks, as there is clearly no need for duplicate implementation of these measures. In the event of discrepancies between the AI Act and the existing legal framework for banks, the legislative body must also clarify which rules shall take precedence. If there are such discrepancies, it is extremely important that supervisory authorities and regulators do not, under any circumstances, attempt to provide 'clarity' in the form of *additional* regulations and standards. Experience has shown that doing so simply creates the opposite effect. It increases regulatory complexity, is detrimental to clarity and in the end does not provide the desired clarity, but instead raises additional questions. Banks should not be put in a situation in which they must meet requirements from the AI Act that stand in direct contradiction to existing supervisory regulations.

There is no need to amend the existing supervisory rules for banks. Doing so is not just unnecessary: it simply cannot be justified in light of the fact that legislators have repeatedly emphasised their intention to improve Europe's competitive position and simplify the legal framework.

In addition, this approach must be adopted across the European Union, with harmonised supervisory practices across all member states and supervisory authorities. After all, the largest European banks are already supervised by joint supervisory teams as coordinated by the European Central Bank. This highlights the need for close coordination between European and national supervisory bodies, and also emphasises the importance of putting market surveillance in the hands of those authorities already familiar with financial supervision (see information above on supervisory structures). Such coordination would facilitate the use of established audit practices and promote the use of existing experience and knowledge.

Concerning reporting serious incidents, we call for the use of already established reporting methods and platforms (BaFin's MVP) currently in use for financial institutions within the context of the Payment Services Directive (PSD) and the Digital Operational Resilience Act (DORA). This will keep reporting as streamlined and efficient as possible, so that the time, effort and benefits remain proportional and, above all, practical. In addition, to ensure legal clarity in light of the obligation to report serious incidents, the crime of "the infringement of obligations under Union law intended to protect fundamental rights" pursuant to Article(3) No. 49 point c AI Act should be defined more precisely, to ensure that the stated goal of avoiding duplicate reporting

obligations for those providers already subject to regulation is effective.

3 Further development of the GDPR to promote AI use

The growing prevalence and significance of AI technologies pose structural and normative challenges to existing data protection law. While the EU General Data Protection Regulation (GDPR) provides a uniform framework for the protection of personal data across Europe, it was developed nearly a decade ago and is not yet fully tailored to the specific technical and functional characteristics of AI systems. In practice, a large number of practical legal issues arise in relation to the AI Act. This necessitates the clarification of provisions and the coherent alignment of data protection requirements with the regulatory framework of the AI Act.

The aim must be to, on the one hand, guarantee the effective protection of personal data and safeguarding the fundamental rights, including in the context of data-driven AI applications. At the same time, it is imperative to establish innovation-friendly regulatory frameworks that sustainably promote both technological competitiveness and the development of trustworthy AI systems at the national and European levels. It is therefore necessary to further develop the GDPR in key application areas to provide regulatory clarity and enable legally sound and trustworthy AI applications.

Although data protection authorities are already attempting to offer guidance on questions of interpretation[5], there remains a significant need for further support and clarification from lawmakers and the supervisory authorities responsible under both the AI Act and the GDPR. Legal provisions and supervisory practice alike should form a consistent and coherent regulatory framework. This is clearly demonstrated by the examples below.

Legal certainty for the use of training data for AI systems

The development and training of AI systems in the banking sector regularly requires the use of extensive data sets. In addition to publicly available information, institutions also rely on internal data sources, such as those derived from operational processes or customer communications. In order to meet data protection requirements, anonymising or at least pseudonymising the data prior to its use in AI training is considered the more compliant approach.

.

[5] See https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf, among other examples.

Both processes – anonymisation or pseudonymisation – are, however, considered data processing pursuant to the GDPR. In practice, therefore, there is not enough legal certainty as to how these measures can be carried out in compliance with data protection requirements. Though it is worth noting that the European Data Protection Board has already addressed the question of pseudonymisation and anonymisation in the context of AI.[6]

In addition, the follow-up question arises as to whether the data sets processed in this manner are to be legally classified as anonymised or pseudonymised in the further course of the training process. This is important insofar as anonymised data no longer fall within the scope of application of the GDPR. Pseudonymised data, on the other hand, remain subject to the GDPR, even though any inference as to the identity of the data subject is, in practice, excluded without access to additional information

Automated training processes for AI systems in particular, however, also beg the question as to what extent traditional data subject rights – such as the right of access or right to erasure pursuant to Article 15 et seq. GDPR – can be implemented meaningfully and proportionately by the relevant party. AI models, after all, do not usually process training data in a way that would allow the data to be connected, at a later date, to a particular data subject, at least not without significant amounts of additional information.

Against this backdrop, a legal clarification addressing the following points seems necessary:

- Lawfulness of pre-processing measures: Anonymising and pseudonymising measures should be explicitly recognised as lawful processing operations, provided that appropriate technical and organisational protective measures are in place.

- Clarity regarding the data protection status of prepared data sets: There is a need for harmonised, union-wide criteria that differentiate between anonymised, pseudonymised and personal data in the context of machine learning.

- Amendment of data subject rights for pseudonymised training data: In scenarios where the re-identification of individuals is practically precluded, it should be examined to what extent data subject rights can be appropriately amended in order to avoid disproportionately impede the functional implementation of AI applications.

[6] https://www.edpb.europa.eu/news/news/2025/edpb-adopts-pseudonymisation-guidelines-and-paves-way-improve-cooperation

Synchronise the data protection impact assessment according to GDPR and fundamental rights impact assessment according to the AI Act

The data protection impact assessment pursuant to Article 35 GDPR, as well as the fundamental rights impact assessment for high-risk AI systems required under Article 27 AI Act, pursue the common objective to systematically identify, assess and – where possible – mitigate the potential risks to the rights and freedoms of natural persons prior to the development of technical systems. Both instruments are based on the preventative risk management approach found in the European Charter of Fundamental Rights, but are, to date, neither substantively nor methodologically aligned.

Against this backdrop, a systematic coordination of both assessments regimes seems necessary. The present concurrence of requirements harbours the risk of redundant assessment processes as well as potentially contradictory assessments concerning the need for protection of the legal rights affected. To avoid redundant administrative burdens and to enhance the practical legal coherence of these assessments, a stronger substantive and structural integration of the Data Protection Impact Assessment and the Fundamental Rights Impact Assessment is required.

It is therefore recommended to develop standardised, mutually aligned assessment and documentation formats (templates) that facilitate consistent assessments and prevent redundant procedures. It will be essential in this context to include specific assessment criteria and clear distinctions between data protection- and fundamental rights-specific evaluation aspects.

In addition, it should be evaluated whether and to what extent the implementation of effective risk-mitigating measures – such as technical procedures for pseudonymisation or anonymisation – objectively justifies a restriction or modulation of the assessment obligations. This could be achieved, for example, through a risk-adaptive design of the assessment obligations, whereby the use of data protection friendly design pursuant to Article 25 GDPR is incentivised.

This kind of systematisation and built-in flexibility would not only help to simplify the regulatory requirements, but would also promote that the AI Act is implemented with legal certainty in areas of application relevant to data protection. It is absolutely essential that there is consistency between existing data protection instruments and the measures introduced with the new AI Act, as this will ensure that standards are applied practically in a manner that protects fundamental rights. Establishing coherence between existing data protection measures and the newly introduced measures within the AI regulation is indispensable from the perspective of a fundamental rights-oriented and practicable application of the law.

Technical implementation of data subject rights within the scope of the AI Act

The data subject rights standardised in the General Data Protection Regulation (GDPR), particularly the rights of access (Article 15 GDPR), to rectification (Article 16 GDPR), to erasure (Article 17 GDPR) and to object (Article 21 GDPR), remain fully applicable without limitation in the context of AI systems. These rights constitute manifestations of legal positions protected by fundamental rights, whose effective protection must be ensured when applying the AI Regulation.

Considering the specific technical characteristics of many AI Systems – such as non-linear model architecture, high volumes of data and data-based training mechanisms – there is a considerable need for clarification regarding the technical implementation of these rights within the framework of the AI Act. In particular, the question arises under which technical conditions the deletion of personal data in accordance with Art. 17 GDPR can be considered legally effective.

A particular challenge arises in cases where personal data is not merely processed but used for model development and adaptation. The complete removal of individual data points can have significant impact on model integrity, system stability, or even the operational usability of the AI system. Practice has shown that existing model architectures have so far only been partially able to fully comply with the requirements of the GDPR.

As such, the need for precise, technical implementation strategies to safeguard data protection rights is increasingly drawing regulatory focus. The objective must be to strike a balance between the practical enforceability of data subjects' rights on the one hand and the promotion of innovation-friendly framework on the other.

From a technical perspective, the following solutions in particular are the subject of current discussions:

- Machine Unlearning: processes for targeted removal of specific information from trained models that does not require full retraining.
- Federated Learning: decentralised learning approaches in which data is processed locally, giving the data subject more control.
- Granular Access Controls: differentiated access design concepts which allow data to be deleted or limited selectively, without impairing overall functionality.
- Modular System Architecture: structural separation of model components to improve traceability and the ability to intervene in a targeted manner.

- Pseudonymisation and Data Masking: techniques for mitigating risks. However, the legal situation here is unclear, considering that parts of the data can still be traced back to the individual.

Despite the technical progress described above, it should be noted that there are still no uniform standards at an operational level that stipulate the legally compliant implementation of data protection requirements in the context of AI. This legal uncertainty poses practical and economic challenges, particularly for small and medium-sized enterprises and research institutions.

In light of gradual entry into force (phasing-in) of the AI Act, it seems essential from a practical perspective, that European and national legislators – possibly with support from supervisory authorities and standardisation institutions – create technical guidelines and minimum requirements for the effective protection of data subjects' rights. Otherwise, there is a risk of delays in the roll out of innovative AI solutions and a reluctance to invest due to regulatory uncertainty.

A lack of clarification would ultimately significantly jeopardise the objective of the AI Regulation, which is to promote innovation while maintaining fundamental rights protection standards.