Deloitte.
Legal

AI Supervision in the Financial Sector: Bafin Becomes a Market Surveillance Authority

What Banks, Insurance Undertakings and Asset Management Companies Need to Do Now

Published: August 2026

Regulatory classification, implications and recommended actions following the entry into force of the German AI Market Surveillance and Innovation Promotion Act (KI-MIG)

Executive Summary

Key message: With the entry into force of the KI-MIG, Bafin assumes responsibility, under the hybrid supervisory model applicable in Germany and alongside the Federal Network Agency (Bundesnetzagentur, BNetzA) as the central market surveillance authority, for the sector-specific market surveillance of AI systems that are directly connected with regulated financial activities. Compliance with the AI Act (Regulation (EU) 2024/1689) therefore becomes part of day-to-day financial supervision. Management bodies should consequently not treat AI governance as an isolated innovation or IT matter, but should integrate it into their existing compliance, risk management and outsourcing governance frameworks.

- **Immediate need for action:** The obligations relating to AI literacy and prohibited AI practices already apply; the transparency obligations under Article 50 of the AI Act have applied since 2 August 2026.
- **Documenting the allocation of responsibilities:** Bafin is responsible for AI systems that are directly connected with regulated financial activities; horizontal applications may fall within the remit of the Federal Network Agency. Financial entities should document this allocation for each application in their AI inventory.
- **High-risk roadmap:** For systems falling within the relevant categories – particularly systems used to assess the creditworthiness of natural persons and systems used for risk assessment and pricing in life and health insurance – roles, classification and control requirements must be implemented on a robust basis by 2 December 2027.
- **Implementation priorities:** In the short term, financial entities should establish a complete AI inventory, clear responsibilities, role-based AI literacy programmes, transparency processes and risk-appropriate contractual standards for AI systems, and align these with DORA, MaRisk, the GDPR and their existing model risk management frameworks.
- **Immediate need for action:** The obligations relating to AI literacy and prohibited AI practices already apply; the transparency obligations under Article 50 of the AI Act have applied since 2 August 2026.

1. Background: A New Chapter in Financial Supervision

With the entry into force of the Act implementing Regulation (EU) 2024/1689—the German AI Market Surveillance and Innovation Promotion Act (KI-Marktüberwachungs- und Innovationsförderungsgesetz, KI-MIG) – the German legislature designated Bafin as the market surveillance authority for AI systems in the financial sector on 29 July 2026. Bafin supervises compliance with those obligations under the AI Act that already apply, insofar as the relevant AI systems are directly connected with a regulated financial activity; market surveillance of the requirements applicable to high-risk AI systems will commence on 2 December 2027. Alongside DORA, MiCAR, MaRisk and other sector-specific organisational requirements, the AI Act has therefore definitively become part of the core framework governing the practical supervision of credit institutions, insurance undertakings and other financial market participants.

In his accompanying statement, Bafin President Mark Branson made clear that full responsibility for the use of AI rests with supervised entities and their management bodies. For financial entities, this means that AI is no longer merely an innovation or IT matter; it is a matter of compliance, governance and management board responsibility.

2. Regulatory Frame-work and Delineation of Responsibilities

The AI Act is an EU regulation with direct effect that is conceptually rooted in product safety law. The Member States are required to designate market surveillance authorities for enforcement purposes. The KI-MIG establishes a hybrid supervisory model in Germany. Bafin does not replace the general AI supervisory regime but, for the financial sector, operates alongside the general market surveillance structure.

Accordingly, section 2(3) of the KI-MIG establishes Bafin's sector-specific remit. This remit covers in particular:

- credit institutions and financial services institutions, as well as branches established in Germany, supervised by Bafin or the European Central Bank under the Single Supervisory Mechanism Regulation;
- insurance and reinsurance undertakings and pension funds;
- asset management companies, investment firms and payment service providers;
- issuers of significant asset-referenced tokens within the meaning of Articles 43 et seq. of MiCAR; and
- the Federal and States Pension Institution (*Versorgungsanstalt des Bundes und der Länder*, VBL).

The distinction is important: Bafin will act only insofar as the AI system is directly connected with a regulated financial activity. According to Bafin's public communication, responsibility for horizontal applications – such as AI-supported recruitment, HR analytics or general internal administrative software – will remain with the Federal Network Agency as the central national market surveillance authority and coordinating body. In practice, this will result in responsibilities being divided within the same financial entity, and that division must be properly documented in the AI inventory. The AI Act does not assign any market surveillance responsibilities to the European Central Bank. As a general rule, those responsibilities are to be exercised by national authorities; see Article 70(1), first sentence, of the AI Act.

3. Phased Application – Relevant Dates

The obligations under the AI Act apply in stages. The following dates are particularly relevant for financial entities:

- **2 February 2025:** Application of the prohibited AI practices under Article 5 of the AI Act and of the AI literacy obligation under Article 4 of the AI Act.
- **2 August 2025:** Application of the provisions governing general-purpose AI models under Articles 51 et seq. and of the provisions on penalties.
- **2 August 2026:** Application of the transparency obligations under Article 50 of the AI Act—including those relating to chatbots, synthetic content, deepfakes and emotion recognition—and of most of the governance provisions.

- **2 December 2027:** Application of the requirements governing high-risk AI systems under Annex III, point 5(b) and (c), of the AI Act, covering the assessment of the creditworthiness and credit scoring of natural persons and risk assessment and pricing in relation to natural persons in the case of life and health insurance.

Note: Some public communications concerning the KI-MIG have referred to 2 December 2026 as the relevant date for high-risk systems. The controlling date, however, is 2 December 2027, as stated by Bafin. The postponement results from Regulation (EU) 2026/1744, the Digital Omnibus Regulation on AI, which amended Regulation (EU) 2024/1689 and extended the transitional period for the relevant high-risk AI systems listed in Annex III.

4. Core Substantive Obligations and Their Practical Significance

4.1 AI Literacy – Article 4 of the AI Act

Providers and deployers must take measures to ensure, to their best extent, a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems on their behalf. In doing so, they must take account of those persons' technical knowledge, experience, education and training, as well as the context in which the AI systems are to be used.

According to Bafin's supervisory communication, there is no obligation to guarantee a specified level of competence for every individual. Existing training concepts should nevertheless be expanded on a risk-based and target-group-specific basis. They should cover all functions whose responsibilities are affected by the development, procurement, approval, use, control or audit of AI systems.

4.2 Prohibited AI Practices – Article 5 of the AI Act

Article 5 of the AI Act contains an exhaustive list of prohibited AI practices. Of particular relevance to the financial sector are the prohibitions relating to manipulative or deceptive techniques, the exploitation of certain vulnerabilities and social scoring.

By contrast, the prohibitions concerning certain forms of emotion recognition and biometric categorisation depend on specific methods and contexts of use. Conventional fraud detection does not automatically fall within those prohibitions.

Infringements may be subject to administrative fines of up to EUR 35 million or, where the offender is an undertaking, up to 7% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

4.3 Transparency Obligations – Article 50 of the AI Act

The role- and application-specific transparency obligations under Article 50 of the AI Act apply from 2 August 2026.

Providers of AI systems intended to interact directly with natural persons must, as a general rule, ensure that the persons concerned are informed that they are interacting with an AI system. This does not apply where the fact that the person is interacting with an AI system is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and context of use.

Further obligations relate in particular to synthetic audio, image, video or text content and to deepfakes, and distinguish between obligations imposed on providers and those imposed on deployers. For financial entities, the principal areas of relevance include chatbots and voicebots used in customer communications, as well as AI-generated marketing and customer-facing content, for example through notices in AI-supported customer communications and the labelling of certain AI-generated marketing content.

4.4 High-Risk AI Systems – Articles 6 et seq. of the AI Act

The extensive substantive requirements governing the relevant high-risk AI systems will apply from 2 December 2027.

The obligations applicable to a financial entity initially depend on its role. Requirements concerning risk management, data and data governance, technical documentation, record-keeping, transparency and the provision of information to deployers, human oversight, accuracy, robustness, cybersecurity and quality management are largely addressed to providers. Deployers are subject in particular to the obligations laid down in Article 26 of the AI Act.

A financial entity may, however, itself become a provider – for example, where it develops an AI system in-house, makes a substantial

modification to an existing AI system or changes the intended purpose of a system.

The AI systems expressly covered include systems intended to evaluate the creditworthiness of natural persons or establish their credit score, other than AI systems used for the purpose of detecting financial fraud, and systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

Motor insurance pricing, property insurance and commercial lending are not covered by Annex III, point 5(b) and (c). Whether they qualify as high-risk under another provision of Article 6 or another part of the annexes must be assessed separately on a case-by-case basis.

5. Implications for Supervised Entities

The AI Act does not operate in a regulatory vacuum. It supplements existing requirements arising in particular from MaRisk – including AT 4.3.4 on the use of models and AT 9 on outsourcing arrangements – DORA, the GDPR and, in the context of lending, the EBA Guidelines on loan origination and monitoring (EBA/GL/2020/06).

The VAIT, KAIT and ZAIT were repealed with effect from the end of 16 January 2025. Since 17 January 2025, the BAIT have continued to apply only to a limited residual group of addressees and will be repealed in full with effect from the end of 31 December 2026.

This produces three principal effects:

- **Dual supervisory perspective:** The same AI application may simultaneously be subject to ongoing prudential supervision – for example under section 25a of the German Banking Act or section 23 of the German Insurance Supervision Act – and to the new market surveillance regime. Bafin has announced that it will closely coordinate the two perspectives at organisational level.
- **Third-party provider and outsourcing perspective:** Depending on their function, contractual scope and integration into the entity's processes, external AI services may constitute an outsourcing arrangement within the meaning of AT 9 MaRisk or the use of ICT services within the meaning of DORA. Contracts should therefore contain risk-appropriate information, documentation, audit, logging, cooperation and change-management rights, as well as requirements relating to evidence of conformity and ongoing monitoring where appropriate.
- **More stringent sanctions architecture:** In addition to the administrative fines available under the AI Act – up to EUR 35 million

or 7% of total worldwide annual turnover – Bafin may take accompanying supervisory measures under the German Banking Act or the German Insurance Supervision Act. These may include prohibiting the use of an AI system and ordering the management body to implement remedial measures.

6. Practical Recommendations

Based on our advisory experience, six priorities emerge for the coming 12 to 18 months:

- **Establish or expand an AI inventory:** The AI inventory should be structurally aligned or technically linked with the inventory of information and ICT assets maintained under DORA, without losing its independent regulatory function. Each AI system should be classified by reference to the relevant risk category, the entity's role – such as provider, deployer or downstream provider – and the competent market surveillance authority.
- **Embed an AI governance framework and leverage compliance synergies:** Responsibilities should be clearly allocated across the three lines of defence, connected with model risk and ICT risk management, and supported by a risk-appropriate approval process for new AI systems and use cases. A specialised AI risk function may be a useful organisational option but is not expressly required by law.
- **Roll out an AI literacy programme:** Role-based curricula should be provided for the management body, including the administrative or supervisory body, business functions, development teams, compliance, data protection and internal audit. The measures, target groups, content and review cycles should be documented in a traceable manner and calibrated to the relevant risks.
- **Apply transparency processes from 2 August 2026:** For each use case, the entity should assess whether, and to what extent, provider or deployer obligations under Article 50 of the AI Act apply. Any required user notices, machine-readable markings or disclosures relating to synthetic content and deepfakes must be implemented by reference to the relevant role and medium. There is no general requirement to apply a watermark to every form of AI-supported communication.
- **Implement a high-risk roadmap by 2 December 2027:** The entity should first determine its role and the risk classification of each system and should then analyse the applicable provider and deployer obligations. Where the entity acts as a provider, it must establish, in particular, risk management, data governance, technical documentation, quality management and, where applicable, post-

market monitoring and serious-incident reporting. Deployers must address, in particular, the requirements relating to proper use, human oversight, logs and monitoring.

- **Review supplier and outsourcing contracts on a risk-appropriate basis:** Depending on the entity's role, the risk class and the service model, contracts should include appropriate information, documentation, audit, logging, change-management and cooperation rights. For proprietary models, proportionate evidence requirements and appropriate access rights should be agreed. Unrestricted access to model data or training data is neither invariably necessary nor invariably feasible in practice.

7. Conclusion

Bafin's designation as a market surveillance authority is more than a reallocation of regulatory responsibilities. It marks the transition from an approach to AI supervision that has so far been predominantly principles-based to a distinct market surveillance regime with specific intervention powers and sanctions.

Entities that already align their AI governance consistently with DORA, MaRisk and the relevant sector-specific organisational requirements have a sound foundation. They must, however, supplement those arrangements by implementing the role- and risk-specific obligations under the AI Act and should identify and realise synergies with related existing obligations and processes.

The requirements concerning AI literacy and prohibited AI practices, which already apply, and the transparency obligations applicable from 2 August 2026 require robust processes in the short term. For high-risk AI systems, entities have until 2 December 2027 to implement roles, classification processes and control frameworks systematically.

The applicable standard of responsibility was summarised by Bafin President Mark Branson as follows: "Responsibility for the use of AI lies with the supervised entities and their management bodies."

Reach out

Felix Brandes

Partner | Banking & Finance

fbrandes@deloitte.de
+49 511 30755 9316

Dr. Söntje J. Hilberg

Partner | Co-Lead Digital Law

shilberg@deloitte.de
+49 170 766 3353

Deloitte.
Legal

"Deloitte Legal" means the legal practices of Deloitte Touche Tohmatsu Limited member firm affiliates that provide legal services.

For legal and regulatory reasons, not all member firms provide legal services. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 460,000 people worldwide make an impact that matters at www.deloitte.com/de.

MAKING AN IMPACT THAT MATTERS since 1845