Europe's Regulatory Approach to AI in the Insurance Industry

22 May 2025

The insurance industry has been an early adopter of AI systems, which are reshaping how insurers assess risk, underwrite policies, detect fraud, engage with customers, and conduct their internal business operations. Insurers are increasingly leveraging AI to streamline operations, reduce claims processing times, and gain deeper insights into consumer behaviour. Common AI use cases for insurers include: using advanced machine learning algorithms that analyse vast datasets to deliver more accurate pricing models, AI-enabled chatbots to enhance customer service, AI-enabled recruitment tools, and using AI to create first drafts of legal, business, and marketing documents.

As AI adoption accelerates, so does the associated regulatory scrutiny, both in the U.S. and Europe. While most regulators agree that AI-related risks in the insurance industry merit attention, EU authorities are taking a different approach to addressing them than UK and U.S. state regulators (such as the NYDFS's approach). For example, whereas the EU is adopting a risk-based, prescriptive regime, the UK continues to maintain a light-touch and principles-based approach focused on outcomes and economic growth.

The EU's Approach

The EU AI Act

The EU AI Act is the EU's flagship piece of AI regulation. It adopts a risk-based approach, imposing new regulatory requirements on AI systems that fall within four risk-based categories: (i) "prohibited" systems; (ii) "high-risk" systems; (iii) systems that trigger transparency obligations; and (iv) general-purpose AI systems. A number of these categories directly and indirectly capture insurance-related AI use cases.

- **Prohibited AI Systems That May Be Applicable to Insurers:**
  - **Social Scoring Using Data from Unrelated Contexts:** Using AI systems to evaluate or classify individuals over time based on their social behaviour and/or personality traits from an unrelated context, where the output of the evaluation

or classification results in detrimental or unfavourable treatment, is prohibited. Based on the European Commission's guidance, this prohibition could potentially capture the use of External Consumer Data and Information Sources (or ECDIS) in underwriting decisions where that data has been sourced from an "unrelated" context. This will require highly fact-specific analysis. For example, an insurer may not lawfully be able to use a person's grocery shopping data when assessing health insurance coverage.

- **Emotional Recognition in the Workplace:** This may be relevant where insurers use AI systems to evaluate the performance of their call centre handlers when responding to callers based on voice, tone and other emotional markers, rather than the text of the conversation, e.g., did the handler sound calm and friendly throughout the call.

These prohibitions came into effect on 2 February 2025, but the penalties for non-compliance do not come into force until 2 August 2025.

- **High-Risk AI Systems for Insurers:** Three high-risk categories that might be directly relevant to insurers are AI systems that are used: (1) for risk assessment and pricing of individuals' life and health insurance; (2) to evaluate individuals' creditworthiness or credit scores (except for financial fraud); and (3) for emotional recognition in non-prohibited situations (e.g. voice/tone analytics to assess the emotions of customers calling in so that angry or upset customers can be allocated to specialist handlers). Further, other high-risk categories also apply to general internal business AI uses, such as recruitment or employment-related use cases. High-risk AI systems are required to comply with a long list of onerous compliance requirements, the details of which will be fleshed out in secondary legislation and guidance over the next 12+ months before the requirements come into effect on 2 August 2026. While most of the requirements will attach to the AI system developers, a smaller list of requirements will apply to deployers and distributers. See our previous posts on the Act here and here.

- **Transparency Obligations:** To the extent insurers use AI chatbots or other consumer-facing AI systems, they must comply with light-touch transparency requirements. Specifically, (i) clearly identifying when a person is interacting with AI and not a human (unless obvious), (ii) informing individuals when they are subject to AI systems undertaking emotional recognition or biometric categorisation, and (iii) if they are the developer of the AI system, ensuring that the output is marked in a machine-readable format and detectable as artificially generated or manipulated. Again, these requirements apply from 2 August 2026.

While the EU AI Act provides a significant step toward harmonising AI regulation across Member States, its material scope remains relatively narrow in practice. Many AI use cases in insurance – particularly those involving internal process automation or lower-risk applications – likely fall outside the EU AI Act's risk classification framework, thus attracting minimal compliance obligations.

Further, as part of its broader regulatory simplification agenda, the European Commission is currently reviewing the coherence and administrative burden of existing legislative frameworks, including the EU AI Act, to help facilitate greater AI adoption. Consequently, there could be a further reduction in the Act's requirements in the near future, although the Commission has not yet committed to making any changes.

Other Regulatory Requirements

Given the limited scope of the EU AI Act – and with most obligations not applying until August 2026 – a more immediate focus for insurers is how their existing (technology-neutral) regulatory frameworks may apply to AI. For example, (1) Solvency II already sets expectations around governance, risk management, and model use, all of which are relevant to AI systems; (2) the EU Digital Operational Reliance Act ("DORA") introduces rules on ICT risk, incident reporting, and oversight of third-party providers that may apply to AI; and (3) the Insurance Distribution Directive (the "IDD") contains relevant requirements around fairness, transparency, and suitability, particularly where AI is used in pricing, product design, or customer interactions. These regimes provide an immediate compliance lens through which insurers should assess their AI use cases.

In light of this, the European Insurance and Occupational Pensions Authority ("EIOPA") has published an opinion on how existing EU insurance regulatory requirements apply to AI systems that are not directly governed by the EU AI Act. For example:

- **Governance and Risk Management Systems:** Article 41 of Solvency II, Article 25 of the IDD, and Articles 5 and 6 of DORA each require insurers to maintain effective governance and risk management frameworks. These provisions provide a robust foundation for overseeing AI systems, covering areas such as accountability, oversight, and internal controls – many of the same good-governance requirements that also apply to AI systems.

- **Bias, Discrimination & Fairness:** One of the key regulatory risks associated with AI is the potential for algorithmic bias, particularly in areas such as underwriting, premium pricing, and fraud detection. Insurers must ensure that AI systems do not produce discriminatory outcomes based on protected characteristics like gender, race, age, or disability—obligations that are well established under the EU Charter of

Fundamental Rights and the GDPR. Article 17 of the IDD reinforces this by requiring insurers to act fairly and in customers' best interests, while EIOPA's 2023 Supervisory Statement on Differential Pricing highlights unfair pricing practices and sets expectations for governance and risk controls to manage such risks.

- **Transparency & Explainability:** Some higher-risk AI systems must be transparent and explainable because their decisions can significantly affect individuals (e.g., denial of coverage) or are used in the offering of insurance products (e.g. via chatbots). Under Article 8 of Regulation 2017/2358, insurance product manufacturers must regularly review products to ensure that they meet the needs of the target market and are distributed through appropriate channels for the target market, considering the insurance product's specific features. These obligations apply equally where AI is involved, and firms must be able to understand, monitor, and explain how AI systems influence product design and customer outcomes.

- **Cybersecurity & Operational Risk:** Insurers are subject to strict obligations around internal controls and ICT security. Solvency II requires insurers to maintain an effective internal control system, while Delegated Regulation 2015/35 mandates that information security measures reflect the sensitivity of the data involved. Similarly, DORA strengthens these expectations by introducing uniform ICT risk management requirements for covered entities, including the need for tested business continuity plans. These obligations are directly relevant to AI, which must be subject to the same standards of resilience, accuracy, and cybersecurity—whether developed in-house or sourced from third parties. Notably, managing AI-related cybersecurity risk is a key focal theme for other global insurance regulators. For example, the NYDFS has issued guidance on assessing AI cybersecurity risks under the existing 23 NYCRR Part 500 framework, which has thematic similarities to EIOPA's approach.

The UK's Approach

The UK has been a strong proponent of AI adoption. The UK AI Opportunities Action Plan – which was adopted in full by the Labour government – indicates that the UK will be taking a light-touch regulatory approach to help facilitate cross-economy AI adoption in all sectors.

In contrast to the EU, the UK government has not introduced, and currently does not plan to introduce, AI-specific legislation, aside from AI copyright laws and possible General Purpose AI Model regulation. Instead, the UK has published five AI principles that existing regulators must apply to govern the technology within their respective domains using their existing powers.

The Prudential Regulation Authority (the "PRA") and Financial Conduct Authority (the "FCA") have been amongst the forerunners in establishing what their AI regulatory approach may look like. Both the PRA and the FCA have stated that they will continue to adopt a technology-agnostic, principles-based and outcomes-focused approach to AI regulation . They are confident that their existing frameworks, including the FCA's Principles for Businesses and the PRA's expectations on operational resilience, outsourcing, and model risk management – plus similar governance, transparency, and fairness rules to those mentioned above for the EU – will ensure that the UK's AI principles are met. Further, the FCA and ICO have pledged to provide regulatory clarity and certainty around the use of AI within financial services.

Although the UK's approach to AI is more flexible than the EU's, it may not be universally lighter. For example, the UK is considering targeted reforms to the UK GDPR, including proposed changes to the rules on automated decision-making ("ADM"). These would require "material" human involvement to exclude a decision from being classified as ADM rather than the current test of more than minimal or token input. Given that many AI applications in insurance—such as automated underwriting, pricing, or claims decisions—may constitute ADM, insurers should ensure that their AI governance frameworks include meaningful human oversight to mitigate regulatory risk and help avoid triggering ADM requirements.

How to Respond

AI is increasingly used in insurance for automated underwriting, risk assessment, and claims processing – activities that directly impact individuals' financial security and access to coverage. These high-stakes outputs, combined with insurers' extensive use of personal data in their use of AI, make the industry a likely focus for AI regulation. This growing scrutiny, alongside varying regulatory approaches across jurisdictions, means insurers should consider developing responsive, risk-based AI governance programs.

Designing a governance framework around AI laws that are not yet in force is challenging. Many proposed rules are subject to change and are missing details. Inconsistencies also exist, both within and across regimes, and there is the potential for amendments and delays in implementation. Therefore, a practical starting point is to focus on reducing operational AI risks, ensuring that AI tools deliver value, function as intended, and avoid unnecessary harms.

Insurers already operate under robust regulatory systems that require strong governance, fairness, transparency, and resilience – core requirements under Solvency II, the IDD, DORA, and UK frameworks offer a solid base for managing AI risks. With

this foundation in place, insurers can monitor the progress of AI-specific regulations and make targeted adjustments once the final shape of AI-specific regulations becomes clearer.

* * *

Please do not hesitate to contact us with any questions.

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Dr. Clare Swirski
International Consultant, London
+ 44 20 7786 3017
cswirski@debevoise.com

Martha Hirst
Associate, London
+ 44 20 7786 5425
mhirst@debevoise.com

Dominic O'Leary
Trainee Associate, London
+44 20 7786 5402
doleary@debevoise.com