



TOPICS:

Insurance

SOURCE

European Insurance and Occupational Pensions Authority

EIOPA Publishes Opinion on AI Governance and Risk Management

- The EIOPA published its **Opinion on the governance and risk management of Artificial Intelligence (AI) systems used by insurance undertakings and intermediaries**. The Opinion aims to clarify how existing insurance sector legislation - particularly Solvency II, the Insurance Distribution Directive (IDD), and the Digital Operational Resilience Act (DORA) - should be interpreted considering AI developments, focusing on non-high-risk AI applications under the EU Artificial Intelligence Act (AI Act).
- EIOPA adopts **a principle-based, risk- and proportionate approach**, acknowledging the diverse impact and complexity of AI use across the insurance value chain. While recognizing **AI's potential** - e.g., in pricing, underwriting, claims handling, and fraud detection - the Opinion stresses the importance of managing **associated risks**, including data bias, opacity, and ethical concerns.
- **Key governance and risk management principles** include: **Risk-Based Governance** - Undertakings must assess the potential impact of each AI system

and adopt proportionate controls based on data sensitivity, customer exposure, business continuity implications, and legal risks; **Fairness and Ethics** - Firms must ensure AI use aligns with customer interests, avoids discriminatory practices, and embeds ethical values into corporate culture and decision-making; **Data Governance** - Data used for AI training and testing must be complete, accurate, and appropriate, with strong controls to mitigate bias, particularly in proxy variables; **Transparency and Explainability** - Outputs from AI systems should be explainable to different stakeholders, including regulators and customers, with additional safeguards for complex, opaque models; **Human Oversight** - Clear internal accountability structures must be in place, including defined responsibilities for governance bodies, compliance, actuarial, and data protection functions; **Cybersecurity and Robustness** - Systems must be resilient against adversarial threats, with ongoing monitoring, fallback plans, and business continuity measures.

FOLLOW US!

