DEEPLOY

WHITEPAPER

Decoding the EU AI Act

Implications for Financial Service Providers

Summary

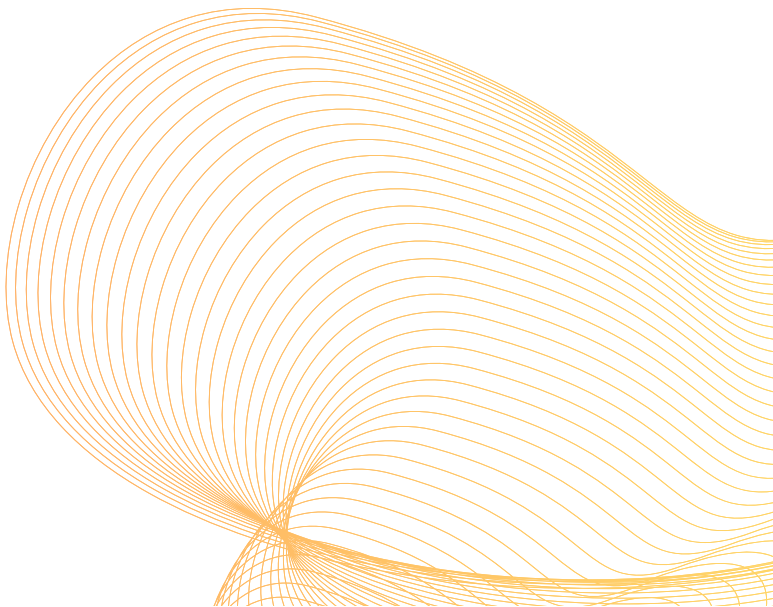
The EU AI Act is a comprehensive legal framework that regulates the use of AI in the European Union (EU). Financial service providers face significant challenges and risks in complying with the Act's requirements for high-risk AI use cases. Deeploy's responsible AI platform offers a solution to simplify deployment, ensure transparency, and enable real-time performance monitoring. By leveraging Deeploy, financial institutions can navigate the EU AI Act effectively, meet regulatory requirements, and build trust in the responsible use of AI while staying competitive in the financial services industry.

Meet Our Experts

Markus Heid
Chief of Staff
mheid@deeploy.ml

Anouk Wolters
Design & Implementation Engineer
awolters@deeploy.ml

Table of Contents

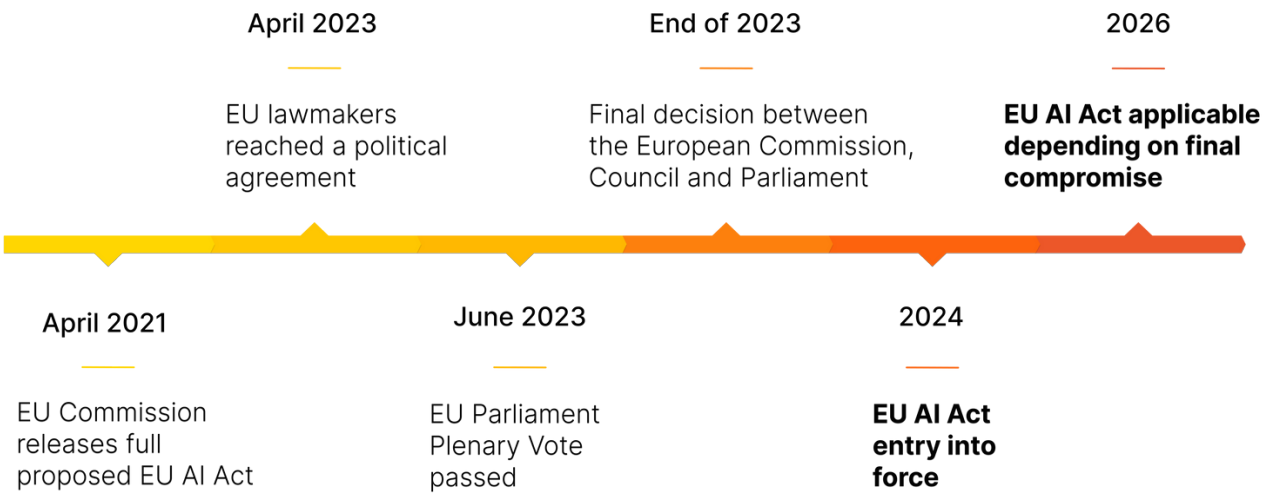


Introduction

The European Union's AI Act is a groundbreaking, comprehensive legal framework that will shape and regulate the use and deployment of artificial intelligence (AI) in the European region. It aims to ensure the safe and ethical use of AI while fostering innovation and protecting fundamental human rights. The AI Act categorizes AI systems into four risk tiers: unacceptable, high, limited, and minimal – and imposes regulatory requirements accordingly to limit the potential impact on individuals and society. The financial service sector, as one of the most impacted industries, must adapt to these new regulations to remain compliant and competitive.

Those so-called high-risk AI systems, which are prevalent in the financial service sector, are subject to stricter requirements around transparency, accountability, data quality, human oversight, and conformity assessment. To comply with the EU AI Act, financial institutions must address the new requirements in their AI applications, such as fraud detection and prevention, credit scoring and lending, risk assessment, algorithmic trading, and robo-advisory services.

Non-compliance with the AI Act can result in significant penalties, including fines up to 30 million euros or 6% of the annual global turnover, whichever is higher. As such, the financial service sector must take immediate steps to adapt to the new regulatory landscape which might involve investing in AI system improvements, adjusting internal policies, and conducting employee training on AI-related risks and responsibilities.



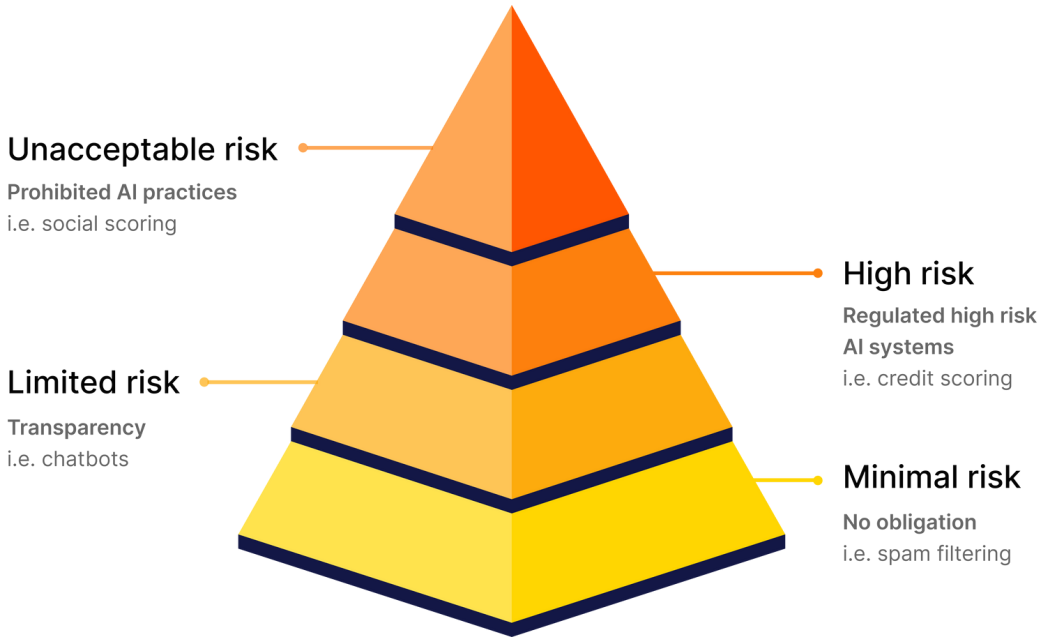
Timeline of the EU AI Act

1. High-Risk AI Use Cases in Financial Services

The cornerstone of the AI Act is a classification system that determines the level of risk an AI system could pose to the health and safety or fundamental rights of a person and/or society. The framework includes four tiers of risk: unacceptable, high, limited, and minimal. With High-Risk AI systems, the AI Act refers to the "significant" risk that an AI system poses to individuals' or organizations' health, safety, and fundamental rights. An AI system is classified "high-risk" according to the EU when it meets two conditions:

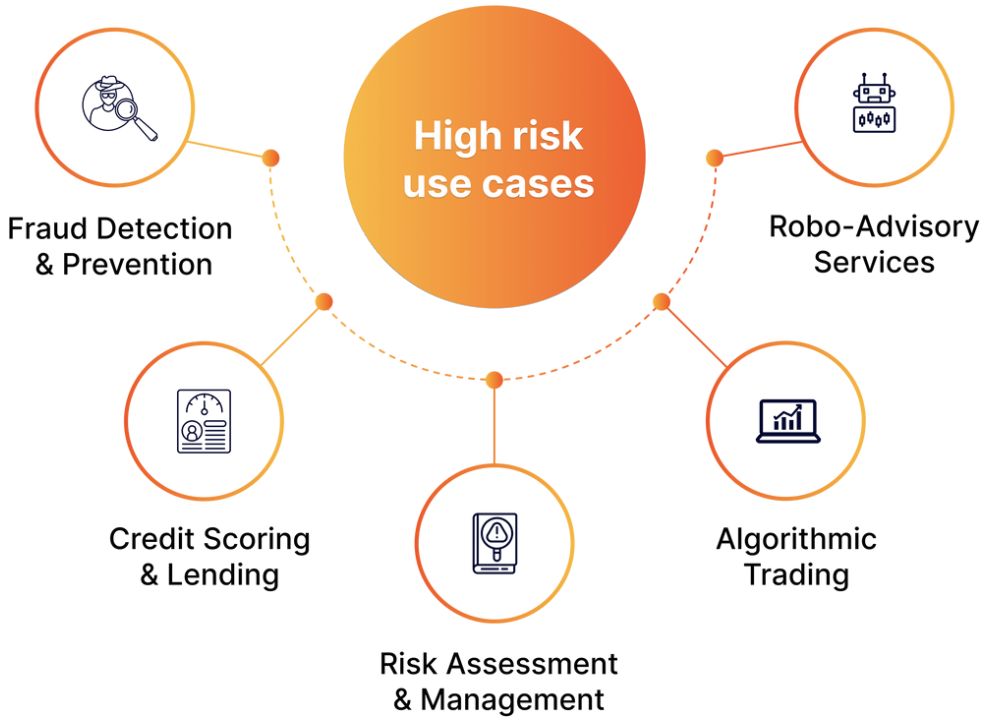
1. The system is used as a safety component of a product, or if the AI system is a product itself (covered by European legislation as in Annex II).
2. The product which uses the AI system as its safety component, or the AI system itself if it's a product, must undergo an independent assessment (by a third party) before it can be introduced to the market or put into use

Apart from the AI systems that fit the above description, there are also other AI systems that are considered high-risk, which are listed in Annex III.



EU AI Act Pyramid of Risks

The EU AI Act specifically targets high-risk AI systems and, while it does not provide an exhaustive list of affected use cases, several applications are likely to be affected due to their significant impact on users and organizations. This is in line with national regulations and guidelines on the usage of AI in critical decision-making processes by institutions such as BaFin (Germany) or DNB (The Netherlands). However, the decision of the regulating authorities - either authorities for personal data protection or financial supervisory - in each European country is still to be decided.

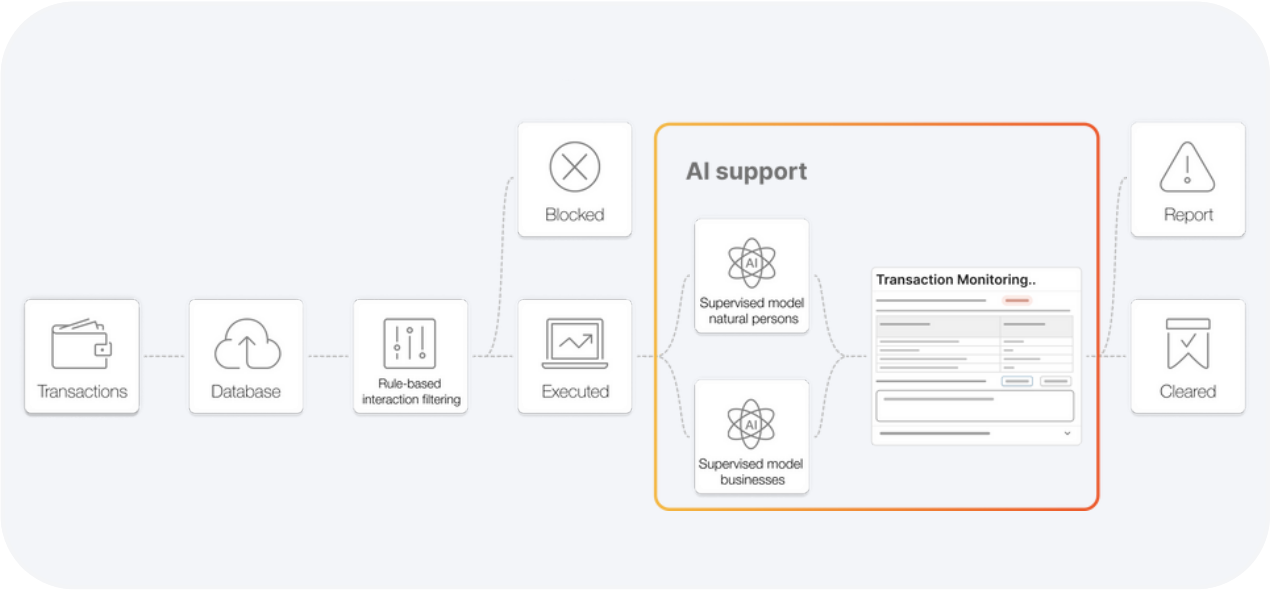


AI high risk use cases in the financial industry

a. Fraud Detection & Prevention

AI systems analyze financial transactions to identify and thwart fraudulent activities, including unauthorized credit card charges, identity theft, and money laundering. By harnessing machine learning algorithms and extensive datasets, artificial intelligence systems can spot suspicious patterns and behaviors better and more accurately than humans. These capabilities provide financial institutions with a powerful tool for detecting fraud, mitigating potential losses, and bolstering customer trust.

However, there are significant risks involved with these systems. Overblocking can occur due to excessive false positives, leading to unnecessary blocking of legitimate transactions. In addition, AI systems may unfairly target specific groups or individuals because of data biases: for example, an institution's AI system may decline transactions from customers who live in low-income areas because those customers have historically had higher rates of fraud; however, such blanket assumptions based on geography rather than individual behavior do not necessarily protect against fraud and may result in legal liabilities and damage to the institution's reputation if they are discovered. Fraudsters may also adapt their tactics to circumvent detection by artificial intelligence systems by developing new techniques that are not covered by existing rules or algorithms.



Implication of AI within transaction monitoring

b. Credit Scoring & Lending 

In the domain of credit scoring and lending, AI-driven models evaluate the creditworthiness of individuals and businesses by examining financial history, income, debt, and other factors. Utilising advanced algorithms offers companies more precise and efficient credit assessments while decreasing processing times and costs, benefiting both lenders and borrowers.

However, AI-enhanced credit scoring and lending can pose significant risks. First, biased data or algorithms can lead to discriminatory lending practices that exclude certain groups from accessing credit resulting in legal and regulatory challenges. Second, overestimation or underestimation of credit risk due to inaccurate credit assessments could lead to approving high-risk borrowers or rejecting creditworthy applicants, impacting the financial well-being of both parties. Finally, AI systems that depend on personal and/or sensitive data for credit assessments could potentially raise legal issues in regard to data protection in the case that privacy concerns emerge.

c. Risk Assessment & Management 

In financial risk management, AI helps institutions make informed decisions, safeguarding investments by assessing and managing various risks. These systems analyze huge volumes of data to expose patterns, correlations, and threats, guiding strategic adjustments, resource allocation, and loss prevention due to unexpected events or market volatility.

Like fraud detection and credit scoring, AI-based risk assessments bear risks like model risk, concentration risk, and non-transparency. Model risk arises from excessive reliance on AI models, potentially failing to capture financial market complexities or relying on outdated data. Concentration risk may happen when institutions widely adopt similar AI risk strategies, escalating industry-wide risk and potentially triggering systemic issues. The opaque nature of AI systems could limit risk management effectiveness if stakeholders can't fully understand system assumptions, limitations, and biases.

d. Algorithmic Trading 

AI-powered trading algorithms enable investment decisions to be automated by analyzing market data and executing trades based on pre-defined strategies. These systems can adapt to evolving market conditions, capitalize on short-term opportunities, and minimize human biases in trading decisions. By automating the trading process, algorithmic trading potentially boosts profits and lowers the risk of human errors, while also contributing to market liquidity and price discovery.
However, they also have drawbacks. Poor algorithms may amplify market volatility or be used for manipulation, causing market distortions. The widespread use of similar algorithms could lead to herding, resulting in asset bubbles, market inefficiencies, or systemic risks.

e. Robo-Advisory Services 

AI-based robo-advisors provide automated investment advice, considering user's financial goals, risk tolerance, and preferences. Using advanced algorithms and large datasets, they customize investment portfolios, helping users diversify investments and manage risks effectively. This democratizes access to financial advice, making it affordable and accessible to more investors. Despite the benefits, there are also risks associated with these AI systems. Robo-advisors may prioritize their interests, leading to conflicts of interest and unsuitable advice. Overconfidence in AI advice could cause excessive risk-taking or unsound investments. AI systems might also over-rely on historical data, failing to consider changing markets or unexpected events, potentially resulting in less than optimal investment decisions.

While the AI offers extensive benefits to the mentioned use cases, it is obvious that AI also opposes significant risks that need to be mitigated. Those risks associated with high-risk AI use cases in the financial service industry highlight the need for responsible AI development and deployment. By addressing these challenges through robust governance, transparency, data quality, and human oversight, financial institutions can harness the potential of AI while mitigating potential negative impacts on users and the market.

2. Key-Requirements to comply with the EU AI Act

As shown, utilising AI systems to support critical use cases across the financial industry can be highly beneficial but also poses significant challenges and risks, which must be addressed to maintain trust, ensure fairness, and protect users. The EU AI Act outlines key requirements for high-risk use cases and their providers to ensure the responsible development and deployment of AI. Let's explore these requirements and how they aim to mitigate risks associated with AI in the financial service sector.

Key requirements of the EU AI Act for high-risk use cases

a. Data & Data Governance 

Articles 10-12 of the EU AI Act guide data governance, technical documentation, and record-keeping for high-risk AI systems. Article 10 mandates quality training, validation, and testing data for these systems, which must be representative and error-free. It permits the processing of special categories of personal data for bias monitoring in specific situations.

Article 11 requires up-to-date technical documentation before market entry, demonstrating compliance with the Act and providing relevant information for conformity assessment.

According to Article 12, high-risk AI systems need logging capabilities for lifecycle traceability, enabling system operation monitoring and post-market scrutiny, especially in high-risk or majorly modified scenarios.

Providers must ensure data accuracy, currentness, and error-freeness in training and validation, conducting regular audits to tackle data quality issues impacting performance or fairness. It's vital that the data used corresponds with intended use cases, preventing biases leading to unfair outcomes.

In terms of data protection, providers must adhere to regulations like GDPR when processing personal data for AI system development and deployment, which includes obtaining necessary data subject consent and conducting data protection impact assessments for high-risk AI systems.

b. Transparency & Accountability 

The EU AI Act mandates transparency in high-risk AI systems (Article 13), ensuring users can interpret outputs and are provided with comprehensive instructions detailing performance limitations, maintenance, and human oversight. The Act demands full system documentation, from development to maintenance, explaining algorithms, data sources, training and testing procedures, performance metrics, and bias mitigation measures. AI providers must clearly inform users about the AI's presence, its purpose, and possible implications. Additionally, the Act imposes record-keeping regulations, necessitating logs of system inputs, outputs, and human interventions for a set time. This promotes accountability and enables evaluation of system performance over time.

c. Human Oversight

As one of its key elements, the EU AI Act requires human oversight for high-risk AI systems, demanding human-machine interfaces that allow humans to supervise AI use and quickly detect anomalies (Article 14). Proper human oversight helps minimize risks to health, safety, or fundamental rights, manages automation bias, and ensures accurate AI output interpretation. In certain situations, the Act requires at least two human verifications before action is taken on system identifications.

Following the requirements for human oversight, the Act promotes human-in-the-loop AI systems, necessitating manual review or override of AI decisions at key points. It emphasizes clear roles and responsibilities in AI management, including defined reporting lines and escalation procedures for AI issues. Further, the Act underscores training employees to understand AI functionality and limitations, facilitating knowledgeable interventions. This includes providing ongoing education about AI technologies, regulatory norms, and industry best practices.

d. Robustness, Accuracy & Security

Under Article 15, companies are required to maintain high accuracy, robustness, and cybersecurity standards, resisting errors, unauthorized exploits, and AI-specific vulnerabilities for their high-risk AI systems. The system's guidelines should define the required accuracy and robustness levels. Resilience is ensured through security measures like encryption, access controls, and safeguards against adversarial attacks. Continuous system monitoring using benchmarks, KPIs, and regular audits is necessary for detecting anomalies or breaches. The Act also necessitates incident response plans, outlining communication protocols and personnel responsibilities during system failures or security incidents.

e. Compliance & Auditing

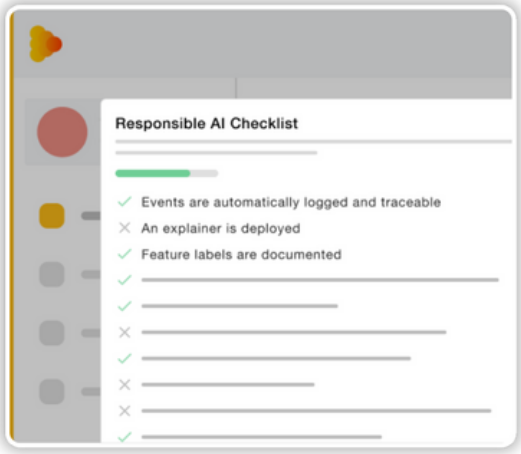
Per the EU AI Act, financial institutions must establish procedures for ongoing AI system compliance assessment and validation, including risk assessments, documentation scrutiny, and AI governance efficacy appraisals. Preparedness for external regulatory audits is essential, potentially requiring collaboration with third-party auditors or participation in self-assessment initiatives. Institutions must also regularly report to relevant authorities, providing detailed data on AI system performance, risk management, governance practices, and any incidents or breaches, demonstrating continued adherence to the AI Act and outlining remedial actions for detected issues.

3. How Deeploy supports Financial Service Providers

Deeploy's responsible AI platform offers a comprehensive solution for financial service providers to address the challenges associated with AI deployment, traceability, performance monitoring, and responsible use of models while ensuring compliance with the EU AI Act.

a. Simplified & Compliant Deployment

Deeploy does not only streamline the deployment process, making it easier to deploy models quickly and efficiently but also ensures adherence to the latest compliance standards through various features. This way of deploying AI safely and responsibly gives Data Science teams the space to concentrate their efforts on generating innovative and accurate insights.



Integrated compliance check before deployment

These features range from the integration of model cards to approval flows and model assessments - all with the aim to minimise risk of AI systems before putting them into production. Additionally, Deeploy's platform automatically generates and maintains comprehensive documentation for AI models, ensuring compliance with the EU AI Act's requirements for system documentation.

b. Complete Traceability & Accountability

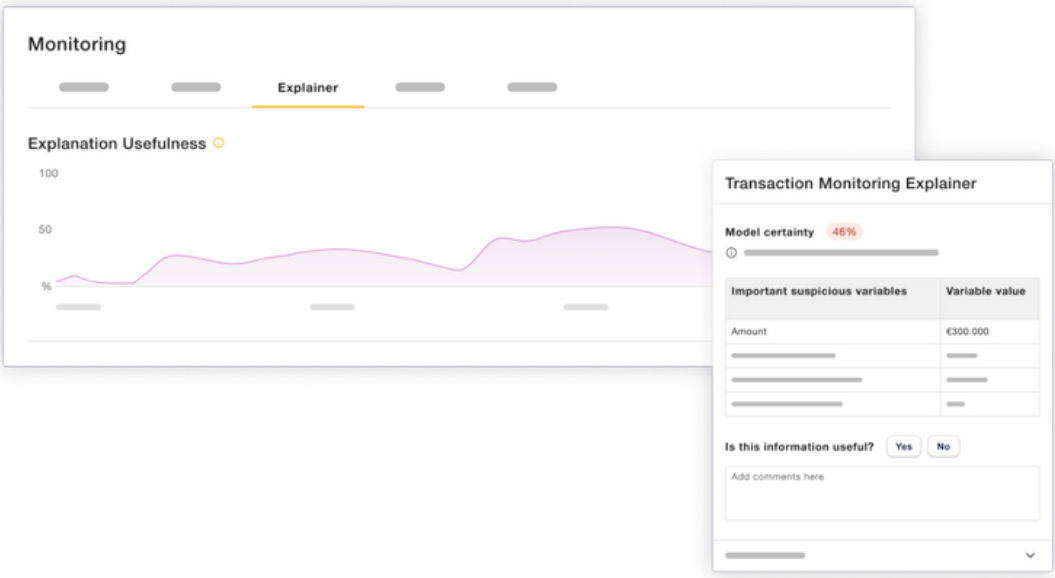
By providing end-to-end traceability for AI models, Deeploy enables transparency and auditability along the entire machine learning lifecycle, ultimately helping financial service providers demonstrate compliance with the EU AI Act's requirements for transparency and accountability. By tracking model development, validation, deployment, and performance, Deeploy enables institutions to maintain accountability for AI-driven decisions and respond effectively to any inquiries from regulatory authorities.

c. Real-Time Performance Monitoring & Robustness

With Deeploy, financial service providers can monitor their AI models' performance in real-time, addressing the requirements and needs for robustness and security. The platform's customizable alerts feature ensures that relevant stakeholders are notified of potential problems, enabling swift action to mitigate risks and prevent negative impacts on the business. Real-time monitoring also helps institutions to maintain system resilience and detect any deviations from expected performance.

d. Transparent & Responsible Use of Models for Non-discrimination & Fairness

Deeploy's explainability capabilities (XAI) facilitate transparency and trust in AI-driven decisions by offering standardized or customized explanations for models and model outputs and thus supporting financial service providers directly supporting transparency, non-discrimination, and fairness. By making it easier for internal business and compliance teams, external regulators, and customers to interpret and evaluate AI-driven outputs, Deeploy fosters trust and ensures the responsible use of AI models in compliance with the Act's provisions.



(Tailored) Explainable AI and monitoring of human feedback

e. Human-Centred Approach & Human Oversight

The key element of Deeploy is to support a human-centric approach to AI. By providing in-depth explanations for models and single model predictions, different stakeholders can easily understand and interpret model decisions. Using those explanations, users can provide direct feedback and overrule model decisions when necessary, ensuring that human judgment remains a critical part of AI-supported decision-making processes. Thereby, Deeploy enables and creates a consistent human feedback loop that can be used to control and improve AI systems. This promotes the responsible use of AI models in line with regulatory requirements and helps institutions maintain a balance between AI-driven automation and human decision-making.

By incorporating Deeploy's responsible AI platform into their operations, financial service providers can effectively address the challenges associated with AI adoption and ensure compliance with the EU AI Act. This not only helps institutions build trust and maintain a strong reputation but also enables the responsible and sustainable use of AI in the financial services sector.

Conclusion

The EU AI Act is a groundbreaking legal framework that aims to regulate the use and deployment of artificial intelligence in the European region. The financial world, as one of the most impacted industries, must adapt to these new regulations to remain compliant and competitive. High-risk AI systems in the financial service sector, such as fraud detection and prevention, credit scoring and lending, risk assessment, algorithmic trading, and robo-advisory services, are subject to stricter requirements to ensure transparency, accountability, data quality, human oversight, and conformity assessment.

Institutions failing to comply with the AI Act can face significant penalties, highlighting the importance of immediate action to adapt to the new regulatory landscape. Deeploy's responsible AI platform offers a comprehensive solution for financial service providers, incorporating compliance features already in the deployment process, ensuring traceability and accountability, enabling real-time performance monitoring, promoting transparency and responsible use of models, and supporting a human-centered approach with human oversight.

By leveraging Deeploy, financial service providers can effectively address the challenges associated with AI adoption and meet the requirements of the EU AI Act. This not only helps institutions build trust and maintain a strong reputation but also enables the responsible and sustainable use of AI in the financial services sector. Ultimately, the EU AI Act and Deeploy's platform provide a pathway for financial institutions to navigate the complexities of AI compliance, protect users' rights, and foster innovation in a rapidly evolving technological landscape.

TALK TO US:

(0031) 6 344 711 54
marketing@deeploy.ml