The Time to (AI) Act is Now: A Practical Guide to High-Risk AI Systems Under The AI Act

July 22, 2024

The AI Act establishes regulations for AI systems in the European Union, particularly those classified as high-risk due to their potential impact on health, safety, and fundamental rights.

This guide provides an overview of how high-risk AI systems are classified under the AI Act and outlines the necessary steps for compliance. It covers key requirements such as risk management, data governance, documentation, transparency, and cybersecurity, equipping legal practitioners with the knowledge needed to advise clients on compliance.

Overview of High-Risk AI Systems under the AI Act

Classification of High-Risk AI Systems

> The AI Act classifies high-risk AI systems based on their use and potential impact on safety and fundamental rights.

Article 6: Classification Rules for High-Risk AI Systems

High-risk AI systems are categorised under two main annexes:

Annex I High-Risk AI:

An AI system is considered high-risk if it is used as a safety component of a product, or is itself a product, covered by specific Union harmonisation legislation such as the Machinery Regulations and the Medical Devices Regulations. Additionally, these products or AI systems require a third-party conformity assessment before market placement or service initiation.

Annex III High-Risk AI:

This category encompasses AI systems in various domains including:

Biometrics: This includes remote biometric identification systems, biometric categorisation based on sensitive attributes, and emotion recognition systems, noting that emotion recognition systems are prohibited in the workplace or educational settings.

Critical Infrastructure: AI systems used as safety components in managing critical infrastructure like digital infrastructure, road traffic, water, gas, heating, and electricity.

Education and Vocational Training: AI systems determining access or admission to educational institutions, evaluating learning outcomes, or monitoring student behaviour during tests.

Employment and Work Management: AI systems used for recruitment or selection of personnel, making decisions on employment conditions, promotions, or terminations, and monitoring and evaluating employee performance and behaviour.

Access to Essential Services: This includes AI systems evaluating eligibility for public assistance, healthcare, or social services, used for creditworthiness assessment or insurance risk assessment, and for emergency response services.

Law Enforcement: AI systems assessing the risk of criminal offences, used as polygraphs or evaluating the reliability of evidence, assessing the risk of offending or re-offending, and used for profiling in criminal investigations.

Migration, Asylum, and Border Control: AI systems used as polygraphs or risk assessment tools for entry into Member States, evaluating applications for asylum, visas, or residence permits, and detecting or identifying individuals in migration contexts.

Administration of Justice and Democratic Processes: AI systems assisting judicial authorities in researching and interpreting facts and the law, and those influencing

election outcomes or voting behaviour.

Exceptions:

Certain AI systems listed in Annex III may not be classified as high-risk if they perform narrow procedural tasks, improve results of previously completed human activities, detect patterns without influencing decision-making, or perform preparatory tasks for assessments relevant to Annex III use cases. However, AI systems that perform profiling are always considered high-risk.

Provider Responsibilities:

Providers of high-risk AI systems have several responsibilities under the AI Act. They must clearly indicate their identification and contact information on the AI system or its packaging and accompanying documentation. They must implement a quality management system that includes regulatory compliance strategies, design and development procedures, data management, risk management, post-market monitoring, incident reporting, and communication with authorities.

Providers must also maintain comprehensive and up-to-date technical documentation demonstrating compliance with the AI Act's requirements, which should be available for review by national competent authorities and notified bodies. High-risk AI systems must have the capability to automatically record events throughout their lifecycle for traceability and monitoring purposes.

Before placing an AI system on the market or putting it into service, providers must ensure it undergoes the appropriate conformity assessment procedure. They must draw up an EU declaration of conformity and affix the CE marking to the AI system or its packaging to indicate compliance with the AI Act. Additionally, providers must comply with registration obligations, take necessary corrective actions to address non-compliance, withdraw, disable, or recall the AI system if it poses risks, and inform relevant parties and authorities. Cooperation with national competent authorities, including providing information and documentation upon request and granting access to logs and other necessary data for compliance verification, is mandatory. Providers must also ensure the AI system meets accessibility requirements in line with relevant EU directives.

Deployer Responsibilities:

Deployers, or users, of high-risk AI systems must ensure proper use according to provided instructions. They must assign competent personnel for oversight and ensure they are adequately trained. Input data must be relevant and representative for the AI system's intended purpose. Continuous monitoring of the AI system's performance and compliance is essential, and use must be suspended and authorities informed if any risks or serious incidents are identified. Logs generated by the AI system must be maintained for a period appropriate to its purpose, typically at least six months.

Deployers must notify workers and representatives before deploying high-risk AI systems in the workplace and inform individuals when they are subject to decisions made by high-risk AI systems. Information provided under the AI Act should be used to comply with data protection impact assessments as required by GDPR. Deployers must also submit annual reports on the use of certain high-risk AI systems, such as post-remote biometric identification systems, to relevant authorities.

Key Dates:

12 July 2024: The AI Act is published in the Official Journal.

1 August 2024: The AI Act becomes law.

2 August 2026: Rules on Annex III AI systems come into effect.

2 August 2027: Rules on Annex I AI systems come into effect.

Enforcement and Penalties:

The AI Act imposes significant fines for non-compliance, especially for high-risk AI systems. Non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers, authorised representatives, importers, distributors, deployers, and requirements and obligations of notified bodies, as well as transparency obligations for providers and deployers.

Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7.5 million or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher. For small and medium-sized enterprises (SMEs), including start-ups, each fine is capped at the lower of the specified percentages or amounts.

Steps to Compliance:

Determine High-Risk Classification

To determine if an AI system falls within the high-risk categories specified in Annex III, providers must assess its applicability and verify if it requires third-party conformity assessments. If an AI system is not deemed high-risk, the assessment must be documented and ready for presentation to competent authorities.

Implement a Risk Management System

Providers must develop and implement a risk management system that includes continuous risk identification, analysis, and mitigation. Regular review and updates of risk management measures are essential, and mechanisms for effective human oversight and intervention must be integrated.

Ensure Data Quality and Governance

High-quality, relevant, representative, and bias-free datasets must be used for training, validation, and testing AI systems. Providers should implement data governance practices to maintain dataset quality and address data bias to ensure fairness and avoid discrimination.

Maintain Technical Documentation

Comprehensive and up-to-date technical documentation demonstrating compliance with the AI Act's requirements must be prepared. SMEs can use simplified forms provided by the Commission.

Establish Record-Keeping Practices

AI systems must have the capability to automatically log events for traceability and post-market monitoring. Logs should be maintained for a minimum of six months or as specified by applicable laws.

Provide Transparent Information and Instructions

Clear and accessible instructions for using the AI system must be developed, including information on its characteristics, limitations, and human oversight measures. Outputs of the AI system should be interpretable and actionable by deployers.

Ensure Robustness, Accuracy, and Cybersecurity

Measures to achieve and maintain high levels of accuracy and robustness throughout the AI system's lifecycle must be implemented. Appropriate technical and organisational measures to protect the AI system against cybersecurity threats are also necessary.

Conduct Conformity Assessment

The AI system must undergo the relevant conformity assessment procedure before being placed on the market, and the CE marking must be affixed to indicate conformity with the AI Act.

Monitor Post-Market Performance

Systems to monitor the AI system's performance and compliance after market placement

must be established. Serious incidents or non-compliance issues must be reported to competent authorities and relevant parties.

Ensure Continuous Compliance

Regular review and updates of risk management, data governance, and documentation practices are required to ensure ongoing compliance. Providers must also cooperate with competent authorities by providing necessary information, documentation, and access to logs.

Conclusion:

The AI Act sets strict regulations for high-risk AI systems to protect health, safety, and fundamental rights within the EU. Providers and deployers must comply with detailed obligations on risk management, data governance, transparency, and cybersecurity, with severe penalties for non-compliance. This guide offers essential insights for lawyers to help clients meet these requirements and ensure the safe, responsible use of AI technologies.

For further guidance and support on AI compliance, please contact Barry Scannell, Leo Moore, or any member of the William Fry Technology Department.