Module	**ARTIFICIAL INTELLIGENCE SYSTEMS**
Jurisdictions	**EUROPEAN UNION (EU)**

Module Application

Is your organisation developing, deploying, or using third-party AI systems within the EU?

Does your organisation conduct regular risk assessments of AI systems to classify their risk level?

Does your organisation have transparency measures in place, such as informing users when interacting with AI systems?

Does your organisation conduct regular testing, impact assessments, and reporting for high-risk AI systems?

Does your organisation align its AI systems with relevant Environmental, Social, and Governance (ESG) requirements to ensure ethical and socially responsible AI deployment?

Module Scope

The EUROPEAN UNION – ARTIFICIAL INTELLIGENCE SYSTEMS module provides an organisation operating in the EU that develops, deploys, or uses third-party Artificial Intelligence (AI) systems actionable insights to comply with the EU Artificial Intelligence regulatory framework and an understanding of their legal obligations under the framework. The module provides the practical assistance and guidance to ensure these obligations are complied with by demonstrating the establishment and maintenance of best practice processes.

The EUROPEAN UNION – ARTIFICIAL INTELLIGENCE SYSTEMS module covers the regulatory system especially for the financial services sector in Europe that imposes obligations on organisations including:

- Financial entities;
- Developers/Deployers/Users of third-party AI systems; and
- Importers of AI systems

The primary piece of legislation regulating the development/deployment/use of AI systems in the EU is the Artificial Intelligence Act 2024 (2024/1689/EU).

In addition, there are other legislative sources of obligations for organisations including:

- Cybersecurity Act 2019 (2019/881/EU)
- Digital Services Act 2022 (2022/2065/EU)
- Digital Operations Resilience Act (DORA) 2022 (2022/2554/EU)
- General Data Protection Regulation (GDPR) 2016 (2019/679/EU)
- Charter for the Fundamental Rights of the European Union 2012
- OECD Guidelines on Responsible Business Conduct 2023

The primary regulatory bodies that regulate the development, deployment, or use of AI systems in the EU are the European Commission, European Artificial Intelligence Board (EAIB), European Union Agency for Cybersecurity (ENISA), and national supervisory authorities in each Member State.

An organisation using this module must ensure it complies with all obligations set out under the EU Artificial Intelligence regulatory framework, including:

- Classifying AI systems based on their risk profile (high-risk, limited risk, minimal risk)
- Implementing risk management and data governance practices
- Ensuring system integrity with technical and organisational controls (logging, cybersecurity, human oversight)
- Disclosing when AI systems interact with humans or use biometric data
- Conducting regular testing, impact assessments, and reporting for high-risk AI systems

There are also specific obligations for financial entities under the digital operational resilience regulatory framework for managing risks related to ICT- related incidents. Financial entities further have the obligation of notifying authorities of security breaches or lapses in their AI systems.

The EUROPEAN UNION – ARTIFICIAL INTELLIGENCE SYSTEMS module covers the requirement and practical guidance for organisations to establish a robust compliance framework to ensure they comply with their core regulatory obligations. The framework should include systems for ensuring that the institution:

- Is appropriately authorised to develop, deploy, or use AI systems, particularly those classified as high-risk in their operations.
- Conducts its business with integrity, ensuring that AI systems are used ethically and comply with legal requirements.
- Operates with due skill, care, and diligence in the management and oversight of AI systems to ensure they function safely and without causing harm.
- Has appointed qualified and trained representatives and employees, ensuring staff involved in AI operations are suitably equipped to handle related tasks.
- Operates efficiently, honestly, and fairly, ensuring that AI systems respect customer rights and improve business operations without creating undue risks.
- Manages conflicts of interest effectively, particularly in cases where AI-driven decisions may impact various stakeholders.
- Maintains adequate financial resources to support the safe and compliant operation of AI systems, with the ability to address potential risks or breaches.

- Implements effective risk management systems to identify, mitigate, and report risks associated with AI technologies, particularly high-risk AI systems.
- Observes proper standards of AI usage and market conduct, ensuring that AI systems align with relevant laws, ethical standards, and business practices.
- Maintains organisational competence by keeping up with regulatory changes and continuously improving AI systems and compliance procedures.
- Maintains risk management and breach reporting systems to address potential failures, ensuring timely reporting and resolution of any issues.
- Complies with disclosure requirements, including notifying individuals when they are interacting with AI systems or when AI-generated content is used.
- Ensures data quality and appropriate AI objectives, making reasonable inquiries into data sources and ensuring that AI systems function correctly and responsibly.
- Pays due regard to customer interests and treats them fairly, ensuring AI systems do not discriminate or cause undue harm to individuals.
- Takes reasonable care to ensure AI outputs and decisions are suitable for customers or any parties relying on AI-based results.
- Implements data protection and privacy practices, ensuring that personal data processed by AI systems is secure and complies with relevant data protection laws.
- Engages in lawful advertising and AI-driven communications, ensuring transparency and ethical standards in AI-generated content and interactions.
- Maintains required records related to the development, deployment, risk management, and compliance of AI systems.
- Maintains a functioning internal dispute resolution system, enabling concerns related to AI systems to be addressed efficiently and effectively.
- Engages with regulators in an open and cooperative manner, providing relevant information and disclosures as required by supervisory authorities.

Failure to meet these obligations could expose the organisation to significant penalties, including regulatory sanctions, fines, and reputational damage.

The EUROPEAN UNION – ARTIFICIAL INTELLIGENCE SYSTEMS module comprehensively covers the range of specific consequences that apply to different breaches or failures by organisations operating within the EU – developing, deploying, or using third-party AI systems.

The EUROPEAN UNION – ARTIFICIAL INTELLIGENCE SYSTEMS module provides comprehensive coverage of the legal obligations of organisations operating in the EU. This module does not cover obligations related to the creation or commercialisation of AI systems for resale, nor does it address requirements for managing hardware or facilities linked to AI systems.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.