GovLoX | Executive Briefing

EU AI Act:

What Organisations Need to Do Now

A practical guide for legal, compliance, and executive teams

Executive Summary

The EU AI Act is the world's first comprehensive legal framework for artificial intelligence. It entered into force on 1 August 2024, and its obligations are applying in phases - with the most significant requirements for high-risk AI systems taking effect from August 2026.

For organisations deploying or procuring AI systems in or affecting the European Union, compliance is not optional. The Act applies regardless of where an organisation is headquartered: if your AI system affects people in the EU, you are in scope.

This briefing explains what the EU AI Act requires, which organisations and systems are affected, what the key deadlines are, and what practical steps to take now.

> **Key finding**
> Most organisations are behind. The August 2026 deadline for high-risk AI system obligations is closer than it appears when set against the time required to complete conformity assessments, establish technical documentation, and implement human oversight mechanisms. The time to start is now.

What the EU AI Act Is - and Is Not

The EU AI Act is a regulation, not a directive. It applies directly in all EU member states without national implementation. It is also extraterritorial: it applies to AI systems placed on the EU market or used in the EU, regardless of where the developer or deployer is based.

The Act is risk-based. It does not prohibit AI broadly - it imposes obligations proportionate to the risk that an AI system poses to people's health, safety, and fundamental rights. Systems that pose unacceptable risk are banned outright. High-risk systems face the most stringent requirements. Limited and minimal risk systems have lighter obligations or none at all.

Important distinction

The EU AI Act distinguishes between providers (those who develop or place an AI system on the market) and deployers (those who use an AI system in a professional context). Both have obligations under the Act, though they differ. Most organisations are deployers - but organisations that customise, fine-tune, or significantly modify AI systems may also have provider obligations.

Key Dates and Deadlines

The EU AI Act applies in phases. Understanding which deadlines apply to your organisation is the first step in planning your compliance programme.

Date	Obligation	Status
1 Aug 2024	EU AI Act entered into force	**IN FORCE**
2 Feb 2025	Prohibited AI practices ban applies (Article 5)	**IN FORCE**
2 Aug 2025	GPAI model obligations apply; governance rules for providers	**IN FORCE**
2 Aug 2026	High-risk AI system obligations fully apply (Annex III)	**APPROACHING**
2 Aug 2027	High-risk AI systems under Annex I (product safety) obligations apply	**UPCOMING**

The Risk Tiers: Where Does Your AI Sit?

The Act's requirements depend on how an AI system is classified. Understanding your organisation's AI portfolio - and which systems fall into which tier - is the foundation of any compliance programme.

Risk tier	Examples	Obligations
Unacceptable	Social scoring by public authorities; real-time biometric surveillance in public spaces; manipulation of vulnerable groups	PROHIBITED - must not be deployed
High risk	CV screening; credit scoring; educational assessment; healthcare diagnostics; critical infrastructure management; law enforcement tools	Conformity assessment; technical documentation; human oversight; registration in EU database; ongoing monitoring
Limited risk	Chatbots; emotion recognition systems; deepfake generation	Transparency obligations - users must be informed they are

	tools	interacting with AI
Minimal risk	AI-enabled spam filters; recommendation systems; most productivity tools	No mandatory obligations - voluntary codes of practice encouraged

The high-risk categories most organisations encounter

Annex III of the Act lists the specific categories of high-risk AI system subject to the August 2026 obligations. Organisations should review their AI inventory against these categories immediately:

- **Employment and workers management:** AI used in recruitment, CV screening, promotion decisions, task allocation, or performance monitoring
- **Access to essential private services:** AI used in credit scoring, insurance risk assessment, or similar decisions affecting individuals' access to services
- **Education and vocational training:** AI used to assess students, allocate places, or monitor academic behaviour
- **Administration of justice:** AI used to support judicial decision-making or predict criminal behaviour
- **Critical infrastructure:** AI systems managing energy, water, transport, or digital infrastructure
- **Biometric identification:** AI systems used for remote biometric identification of individuals

What High-Risk Compliance Requires

For organisations deploying high-risk AI systems, the Act imposes a specific set of obligations. These are not tick-box requirements - they require genuine implementation and ongoing maintenance.

For deployers of high-risk AI systems

- **Human oversight:** High-risk AI systems must have meaningful human oversight mechanisms. The human must be able to understand, monitor, and where necessary intervene in or override the system's outputs.
- **Technical and organisational measures:** Deployers must implement appropriate measures to ensure the AI system is used in accordance with its instructions for use and the Act's requirements.
- **Data governance:** Input data used by high-risk AI systems must be relevant, representative, and free from significant errors. Data governance processes must be documented.
- **Logging and record-keeping:** Deployers must ensure high-risk AI systems generate logs that enable post-hoc monitoring and investigation of outputs.

- **Fundamental rights impact assessment:** For certain high-risk deployments - particularly by public bodies or private bodies performing public functions - a fundamental rights impact assessment is required before deployment.
- **Registration:** High-risk AI systems must be registered in the EU AI systems database before deployment (where the provider has not already done so).
- **Incident reporting:** Serious incidents and malfunctions must be reported to the relevant national authority.

> **Important for deployers**
> If you are using a third-party AI system classified as high-risk, you still have deployer obligations under the Act. You cannot outsource compliance to your vendor. You must verify that the system meets the Act's requirements, maintain your own records, and implement human oversight - regardless of what the vendor's documentation says.

General Purpose AI Models

The Act also regulates general purpose AI (GPAI) models - AI systems trained on broad data that can perform a wide range of tasks. This category includes large language models and foundation models.

GPAI providers must produce technical documentation, comply with EU copyright law, and publish a summary of training data. GPAI models that pose systemic risk - broadly, those trained with computing power above 10^25 FLOPs - face additional obligations including adversarial testing, incident reporting, and cybersecurity measures.

For most organisations, GPAI obligations apply to providers, not deployers. However, organisations that fine-tune GPAI models for specific purposes, or that integrate GPAI capabilities into their own products, should assess whether this creates provider obligations.

Penalties for Non-Compliance

The Act's enforcement regime is significant. Penalties are tiered by the severity of the violation:

Violation	Maximum fine
Deploying a prohibited AI system (Article 5)	**€35 million or 7% of global annual turnover**
Non-compliance with high-risk AI obligations	**€15 million or 3% of global annual turnover**
Supplying incorrect or misleading information to authorities	€7.5 million or 1% of global annual turnover

What to Do Now: A Practical Action Plan

The following actions are ordered by urgency. Organisations that have not yet started their EU AI Act compliance programme should treat steps 1 to 4 as immediate priorities.

#	Action	Owner	Priority
1	Build a complete inventory of all AI systems in use	IT / AI Governance Officer	**Immediate**
2	Classify each system against the EU AI Act risk tiers	Legal / Compliance	**Immediate**
3	Identify all high-risk AI systems and map to Annex III categories	Legal / AI Governance Officer	**Immediate**
4	Confirm whether prohibited AI practices (Article 5) are in use anywhere in the organisation	Legal	**Immediate**
5	Conduct conformity assessments for each high-risk system	AI Governance Officer / Legal	**This quarter**
6	Establish technical documentation for high-risk systems	IT / AI System Owners	**This quarter**
7	Implement human oversight mechanisms for high-risk systems	Operations / IT	**This quarter**
8	Review vendor agreements for high-risk AI tools - confirm compliance documentation	Procurement / Legal	**This quarter**
9	Establish incident reporting process for AI system malfunctions	Compliance / IT	**This half**
10	Register high-risk AI systems in the EU AI systems database (where required)	Compliance	**Before Aug 2026**
11	Train relevant staff on EU AI Act obligations and internal AI policy	HR / Compliance	**Ongoing**
12	Establish ongoing monitoring and annual review cycle	AI Governance Officer	**Ongoing**

The Governance Foundation

EU AI Act compliance does not exist in isolation. The obligations it imposes - inventory, risk classification, documentation, oversight, monitoring - are the same obligations that sound AI governance requires for any reason: risk management, stakeholder trust, operational resilience.

Organisations that treat EU AI Act compliance as the starting point for a broader AI governance programme will build something durable. Those that treat it as a one-

time legal exercise will find themselves repeating the work as regulations evolve and their AI portfolio grows.

The governance connection

ISO 42001 - the international standard for AI management systems - provides a complementary framework to the EU AI Act. Organisations certified against ISO 42001 are well positioned to demonstrate EU AI Act compliance, as the standard's requirements map closely to the Act's documentation, risk assessment, and oversight obligations.

Get started

GovLoX helps organisations build EU AI Act-ready governance programmes - from AI system discovery and risk classification through to conformity assessment documentation, human oversight workflows, and ongoing compliance monitoring.

govlox.ai