

EU AI Act

The first broad law for artificial intelligence is here and applying in stages. What it asks of your organisation and the one habit that keeps you on the right side of it.

WHAT IT IS

The EU AI Act (Regulation (EU) 2024/1689) governs how AI is built and used. It sorts systems by risk, bans a few uses, sets strict duties for high-risk systems and requires transparency for AI people interact with. It came into force on 1 August 2024 and applies in phases.

WHY IT MATTERS

€35M / 7%

Maximum fine for a banned AI practice, whichever is higher

EU AI Act, Article 99

2 Dec 2027

When the high-risk cybersecurity duties in Article 15 start to apply

Digital Omnibus, Reg (EU) 2026/1744

10²⁵ FLOPs

Compute above which a general-purpose model is presumed a systemic risk

EU AI Act, Article 51

WHAT HAPPENED

In September 2024 the Dutch Data Protection Authority fined Clearview AI €30.5 million for scraping billions of facial images without consent. The AI Act now bans that untargeted scraping outright, so consent is beside the point. Source: Dutch Data Protection Authority.

RED FLAGS TO WATCH FOR

Signs your AI use may be in scope or exposed.

- Using AI to decide on hiring, credit or access to a service
- A chatbot or AI-generated content with no disclosure that it is AI
- No inventory of where AI is used across the business
- No human able to understand and overturn an AI decision
- Pulling in models with no check on who published them

THE ONE RULE THAT STOPS IT

Know every place AI touches a decision about a person, and keep a human able to understand and overturn that decision.

THEN BUILD THE HABIT AROUND IT

- Inventory every AI system and classify its risk tier

- Give staff the AI-literacy training Article 4 requires
- Add the Article 15 controls to high-risk AI (data governance, adversarial testing, model provenance and monitoring)
- Map AI incident reporting onto your NIS2, GDPR and DORA duties

MYTHS AND FACTS

MYTH

The high-risk rules were delayed, so there is nothing to do.

FACT

Only the high-risk deadlines moved. The bans, AI literacy, the general-purpose AI rules and transparency already apply.

MYTH

If we follow GDPR we already meet the AI Act.

FACT

They are separate laws. The Act adds risk classification, human oversight and the Article 15 security duties on top.

MYTH

AI security is just normal IT security.

FACT

Article 15 names attacks a firewall does not stop, data poisoning, model poisoning and adversarial examples.

THE LEGAL DUTY

In Sweden the Act is supervised by PTS as coordinator, with IMY, Finansinspektionen, Läkemedelsverket and Swedac. It stacks on NIS2 (Cybersäkerhetslagen), GDPR and DORA rather than replacing them.

GET HELP

Map your AI use to the Act and to NIS2, GDPR and DORA with a Sweden-based team.

[Read the Full Article →](#)