THE EU AI ACT

9 KEY TAKEAWAYS

8 Dec 2023	9 Dec 2023	Next months	6m to 2 yrs
Provisional agreement on the EU AI Act	Press releases by European Parliament & Council of Europe	Finalise wording & entry into law	Transition period

1 DEFINITION

Definition of AI system aligned with the OECD definition to ensure *'sufficiently clear criteria for distinguishing AI from simpler software systems'*.

2 SCOPE

No application to national security or systems used exclusively for military / defence purposes or research and innovation, or those using AI for non-professional reasons.

3 FINES

Like GDPR, tiered approach: €**35m** or 7% for violations of banned AI applications, **€15m** or 3% for violations of certain obligations, **€7.5m** or 1.5% for supply of incorrect information, p**roportionate caps** on fines for SMEs and start-ups.

4 RISK-BASED

'AI systems presenting only limited risk would be subject to very light transparency obligations, for example disclosing that the content was AI-generated so users can make informed decisions on further use.'

5 HIGH-RISK AI SYSTEMS

Those with '*significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law*' and those 'used to influence the outcome of elections and voter behaviour'. Mandatory fundamental rights impact assessment (FRIA).

6 FOUNDATION MODELS / GPAI

Transparency requirements: technical documentation, detailed summaries on training content. Comply with EU copyright law. **High-impact GPAI models with 'systemic risk'**: conduct model evaluations, assess and mitigate systemic risks, conduct adversarial testing, ensure cybersecurity and report serious incidents to the EC, and report on energy efficiency.

7 BANNED APPLICATIONS

Includes: biometric categorisation using sensitive characteristics; untargeted scraping of facial images for FR databases; emotion recognition in the workplace; certain social scoring; AI systems that manipulate human behaviour to circumvent free will or exploit people's vulnerabilities; and some cases of predictive policing.

8 LAW ENFORCEMENT EXEMPTIONS

Safeguards / 'narrow exceptions' for biometric identification systems (RBI) in publicly accessible spaces: prior judicial authorisation, strictly defined crimes. "Post-remote" RBI: targeted search of person convicted / suspected of serious crime. "Real-time" RBI: use limited in time / location, listed purposes.

9 GOVERNANCE

AI Office within EC to oversee advanced models, foster standards and testing practices, enforce common rules. **Scientific Panel** of independent experts to advise AI Office. **AI Board** of MS representatives to advise EC, coordinate implementation, design codes of practice. **Advisory Forum** to provide technical expertise to AI Board.

Subscribe to Keepabl's newsletter at keepabl.com and our YouTube channel @PricacyKitchen to stay uptodate on all things Privacy and AI