EU Privacy + Security Law Workshop

Nik Theodorakis
Wilson Sonsini

Privacy+ Security Forum

Agenda

Privacy+ Security Forum

1. EU AI Act
2. UK Approach to Regulating AI
3. Discussion

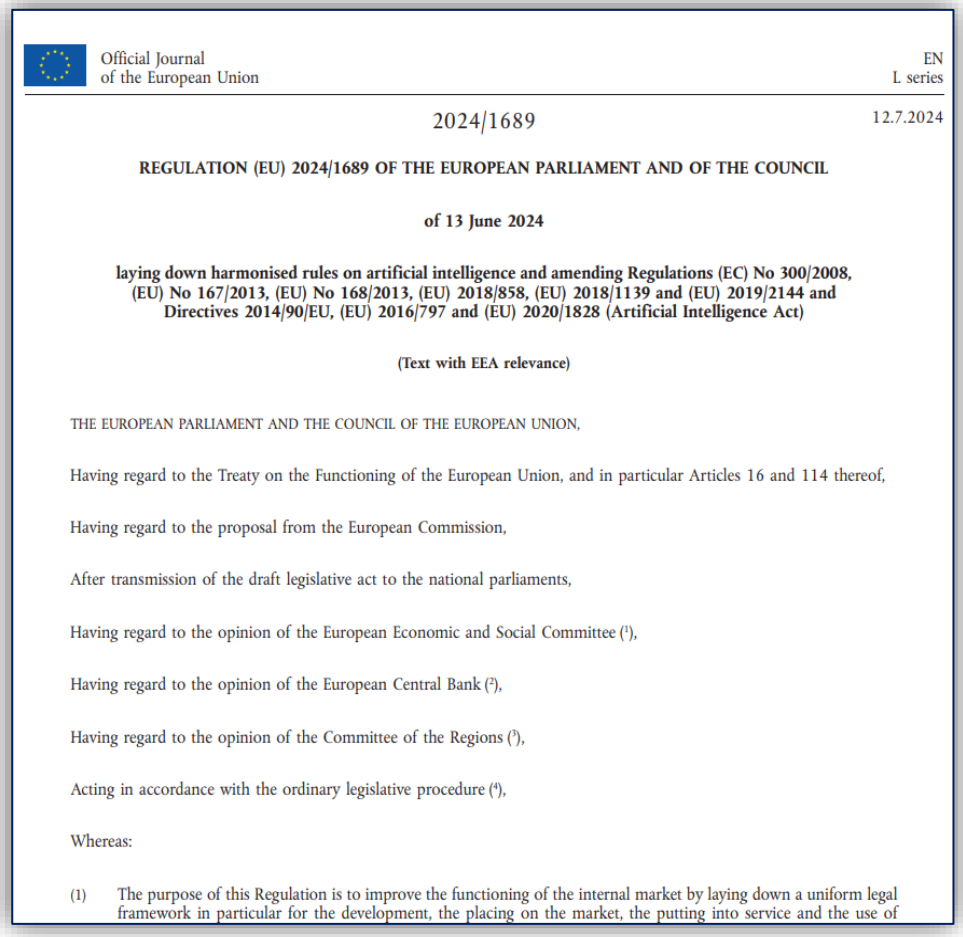
EU AI Act

Privacy+ Security Forum

What is the EU AI Act?

Privacy+ Security Forum

- The AI Act is a **regulation for artificial intelligence** in the EU.
- It is a **risk-based horizontal framework** and its scope. **encompasses all sectors**, and all types of AI.
- It has an **extra-territorial** scope of application.
- The requirements are modelled on **EU product safety law**.
- The AI Act entered into force on August 12, 2024. Requirements will start to apply in phases, primarily over the next 3 years.



Official Journal of the European Union — EN, L series

2024/1689 — 12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the European Central Bank ([2]),

Having regard to the opinion of the Committee of the Regions ([3]),

Acting in accordance with the ordinary legislative procedure ([4]),

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of

EU AI Act : 8 Key Points to Know

Privacy+ Security Forum

1. Broad, extra-territorial scope
2. Does not apply to areas outside of EU law
3. Applies to actors throughout the AI supply chain
4. Horizontal / cross-sector approach
5. Bans certain applications of AI
6. Majority of obligations focused on high-risk applications of AI
7. Transparency obligations for AI that poses specific risks
8. Separate obligations for providers of general purpose AI

What is an AI System?

Privacy+ Security Forum

'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;
(Art. 3(1) AI Act)

Aligns with the OECD definition

Very broad, including many software applications in any sector

Narrow exemptions from certain obligations for AI systems released under free and open-source licenses

AI Act Risk-Based Approach

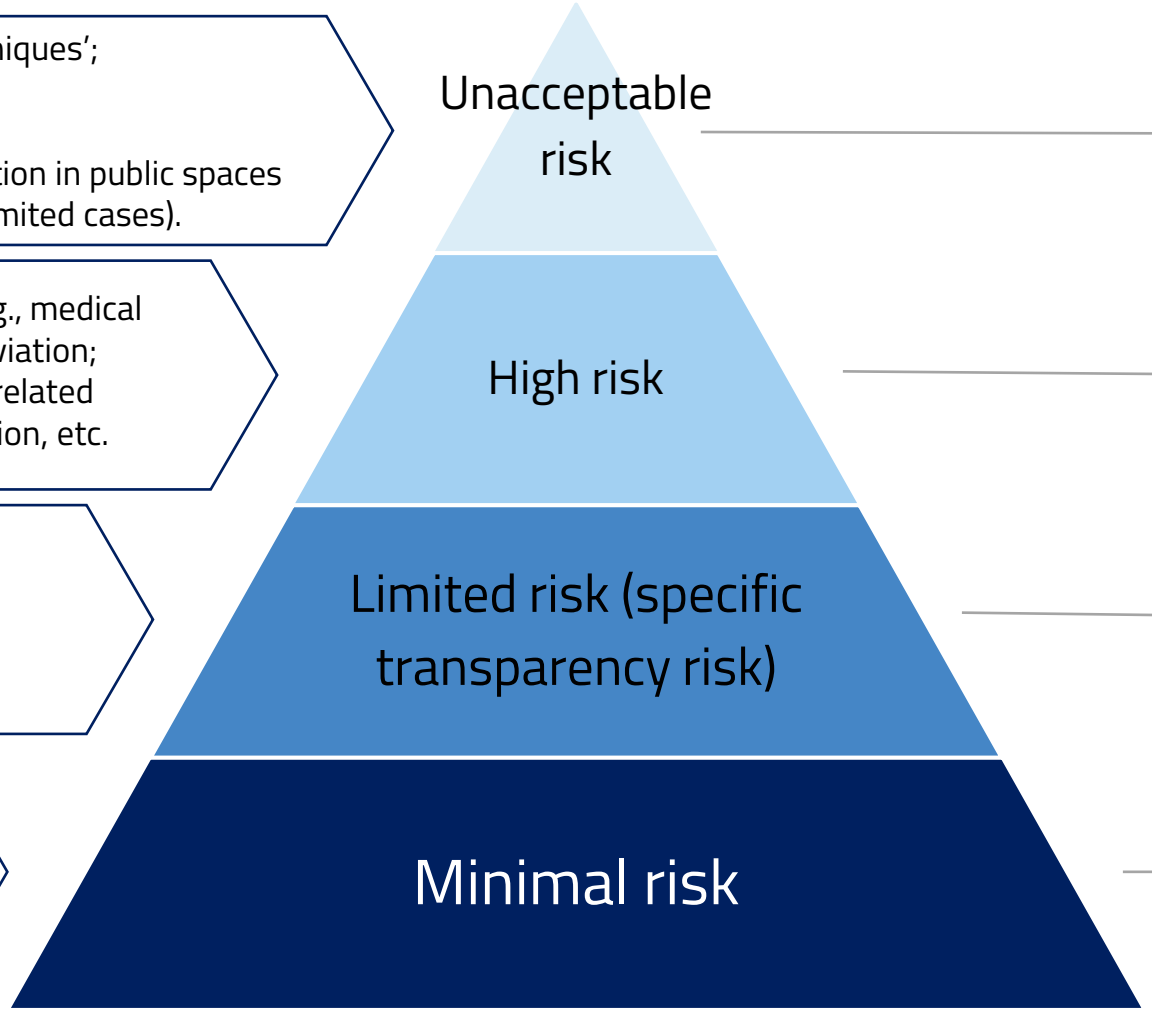
Privacy+ Security Forum

- Harmful manipulative 'subliminal techniques';
- Exploit specific vulnerable groups;
- Social scoring;
- Real-time' remote biometric identification in public spaces for law enforcement (allowed in very limited cases).

- Products with health or safety risks e.g., medical devices, radio equipment, cars, toys, aviation;
- AI for assessing creditworthiness, HR related decisions, remote biometric identification, etc.

- Chatbots, deep fakes, emotion recognition (that is not prohibited).

- Video games, spam filters.



Banned

Documentation and internal processes

Transparency

No obligations under the AI Act

Tiered Rules for GPAI

Privacy+ Security Forum

General Purpose AI (GPAI)	*Systemic Risk GPAI*
Models trained with large amounts of data, that display significant generality (presumed if +1B parameters) which can be integrated in a variety of downstream systems.	GPAI models that have "high impact capabilities" (presumed if trained using a total computing power of more than 10^25 FLOPs). Unless there are no foreseeable risks to health, safety, security etc. The AI Office may specify other criteria for systemic risk GPAI. E.g., OpenAI's Chat GPT 4 or likely Google DeepMind's Gemini.

Transparency obligations apply to all GPAI (excl. open source) and systemic risk GPAI (inc. open source):

- Draw up technical documentation;
- Share documentation with companies who integrate the GPAI into their systems;
- Comply with EU copyright law;
- Publish detailed summaries of content used for training.

Example additional measures that only apply to systemic risk GPAI:

- Assess systemic risks at EU level;
- Incident reporting;
- Red-teaming;
- Cybersecurity requirements;
- Reporting on the model's energy consumption.

Prohibited AI Systems

Privacy+ Security Forum

AI systems that **manipulate or exploit individuals' vulnerabilities**

AI systems that perform **social scoring**

Untargeted scraping of facial images from the internet or CCTV footage

Emotion recognition systems used at the **workplace or in educational institutions** (excl. for medical or safety reasons)

Biometric systems that categorize people to infer sensitive data, such as sexual orientation or religious beliefs

Certain applications of **predictive policing**

Facial recognition for law enforcement purposes in publicly accessible areas (allowed in very narrow cases, e.g., to prevent terrorist attacks, subject to additional safeguards)

High-Risk AI Systems

Privacy+ Security Forum

Two ways for an AI system to qualify as "high-risk":

The **AI System is (integrated into) a safety product, that is subject to other EU safety legislation**, for example:

- Medical devices
- In vitro medical devices
- Components of lifts
- Radio equipment
- Civil aviation
- Agricultural and forestry equipment

The **AI system is intended to be used for a defined "high-risk application"**, such as:

- 'Real-time' and 'post' remote biometric identification systems e.g., airport security or fingerprint recognition for smartphone access
- Safety component in management and operation of critical infrastructure e.g., autonomous traffic management system for smart cities
- To determine access to education e.g., making decisions about university admission
- For recruitment e.g., placing targeted job ads
- Emotion recognition e.g., voice analysis
- Border control management e.g., assessing security risk of incoming travelers

Requirements for High-Risk AI Systems

Privacy+ Security Forum

Accuracy, Robustness and Cybersecurity

Implement reasonable accuracy, robustness and cybersecurity safeguards.

Human Oversight

Implement controls to ensure that humans can oversee the AI systems.

Transparency to Deployers

Ensure the AI system is designed and developed in a way that makes its functioning transparent and allows deployers to use it appropriately.

Registration

Register a high-risk AI system before it is released in the EU.

Risk Management System

Establish and maintain a comprehensive risk management system.

Technical Documentation

Draft technical documentation of the AI system before it is released and update it as necessary.

Data & Data Governance

Training data must comply with quality criteria in the AI Act. There must be a data governance and management approach to training data.

Record Keeping

Ensure that the AI system automatically records logs.

Obligations for Providers and Deployers of High-Risk AI Systems

Privacy+ Security Forum

Providers and deployers of AI must comply with certain obligations when developing or using high-risk AI.

Providers are individuals or entities that develop an AI system and place it on the market or into service under their own name or trademark.

- Obligations for providers include:
  - Establish and maintain quality management system;
  - Conduct conformity assessment;
  - Document retention;
  - Incident notification;
  - Post-market monitoring.

Deployers are individuals or entities that use AI systems (exception for personal non-professional use).

- Obligations for deployers include:
  - Use the AI system in accordance with its instructions;
  - Notify serious incidents to providers;
  - Where the deployer controls data input, they must ensure that the data is relevant and sufficiently representative;
  - Monitor the functioning of the AI system.

Specific Transparency Risk Obligations

Privacy+ Security Forum

Deep fakes and other AI-generated content must be labelled as such.

Individuals must be informed when biometric categorization or emotion recognition is being used.

Synthetic audio, text, video and image content will need to be marked in a machine-readable format and be detectable as artificially generated or manipulated.

Transparency obligations for generative AI e.g., chatbots.

Conformity Assessments for High-Risk AI

Privacy+ Security Forum

What is it?

- The process of **demonstrating that a high-risk AI system fulfils the requirements** for high-risk AI systems in the AI Act.

Who is subject to it?

- **Providers of high-risk AI** i.e., individuals or companies that develop a high-risk AI system and place it on the market or into service in the EU under their own name or trademark.

When does it need to be performed?

- **Before the AI system is placed on the market or put it into service in the EU.**
- **Must be repeated before making a "substantial change"** to the AI system e.g., change of operating system or software architecture.

Who conducts the assessment?

- Depending on the context of the AI system:
  - The provider conducts the conformity assessment **internally**.
  - A **third-party body** designated by the national regulator.

What is being assessed?

- The **quality management system and technical documentation** for the AI system.

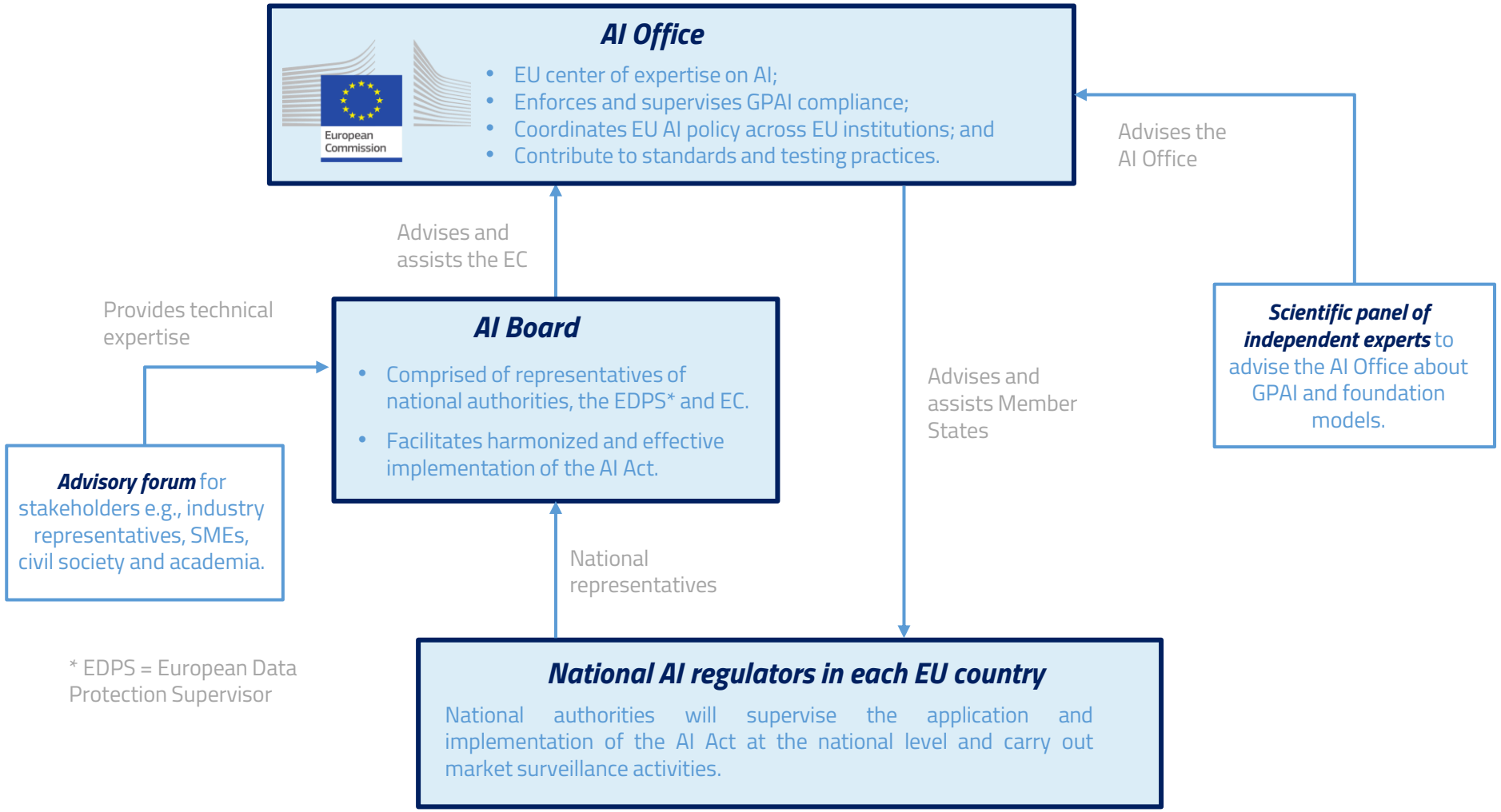
Conformity Assessments for High-Risk AI

Privacy+ Security Forum

High Penalties

Up to **EUR 35 mil. or 7% total worldwide annual turnover** for preceding financial year (for violations of banned AI provisions).

Up to **EUR 15 mil. or 3% total worldwide annual turnover** for preceding financial year (for violations of all other AI provisions).



Timeline for Phased Application of the AI Act

Privacy+ Security Forum

AUGUST 1 2024	FEBRUARY 2 2025	AUGUST 2 2025	AUGUST 2 2026	AUGUST 2 2027	AUGUST 2 2030
EU AI Act entered into force	Prohibition of certain AI systems + AI literacy requirements	Requirements for new GPAI models	Requirements for some high-risk AI systems + Requirements for AI systems with specific transparency risk	Requirements for existing GPAI models and high-risk AI systems subject to EU health and safety laws	Requirements for existing high-risk AI systems intended to be used by public authorities

UK Approach to AI

Privacy+ Security Forum

UK Approach to AI Regulation: 4 Key Points

Privacy+ Security Forum

Flexible, non-legislative approach	Key regulators have published their strategic approach to AI
In 2023, the UK Government published its AI Regulation White Paper which outlined a **principles-based and non-legislative approach to regulating AI**.	In April 2024, **key sectoral regulators** including the data protection regulator (ICO), Financial Conduct Authority (FCA) and the Medicines and Healthcare products and Regulatory Agency, were **tasked to present their own strategic approach to AI**.

Cross-sector collaboration between regulators is central	Potential for AI legislation in the future
The **Digital Regulation Cooperation forum brings together the ICO, Ofcom (online safety), FCA and the Competition Markets Authority**. AI is one of its focus areas for collaboration.	The **UK Government is monitoring the landscape, and may will introduce legislation** to regulate the largest AI models. To date no firm proposals or draft legislation has been introduced.

EU and UK: Comparing Approaches

Privacy+ Security Forum

	EU	UK
Legally binding?	Legally binding, **legislative** approach	Non-binding, and **principles based** – regulators are expected to develop non-binding guidance
Horizontal or vertical?	Horizontal, **cross-sectoral** application	Vertical, **sectoral** guidelines with cross-sector collaboration between regulators
Focus of the regulation	**Risk-based** and focused on the highest-risk applications of AI and development AI models	Focused on **proportionate** requirements that do **not inhibit innovation**
Institution responsible for AI safety and international cooperation	**EU AI Office** is responsible for monitoring the most advanced AI models and international cooperation for AI safety. Many national-level regulators are involved	**AI Safety Institute** established to focus on systemic risks posed by AI and international cooperation

Discussion

Privacy+ Security Forum

Questions for Discussion

Privacy+ Security Forum

- How can companies build on existing AI governance programs to comply with the AI Act?
- What are the first steps companies should take to approach complying with a new law with no existing guidance or precedent?
- Which requirements stand out as potentially the most challenging to comply with? How can companies approach these requirements?

Thank you!

Privacy+ Security Forum