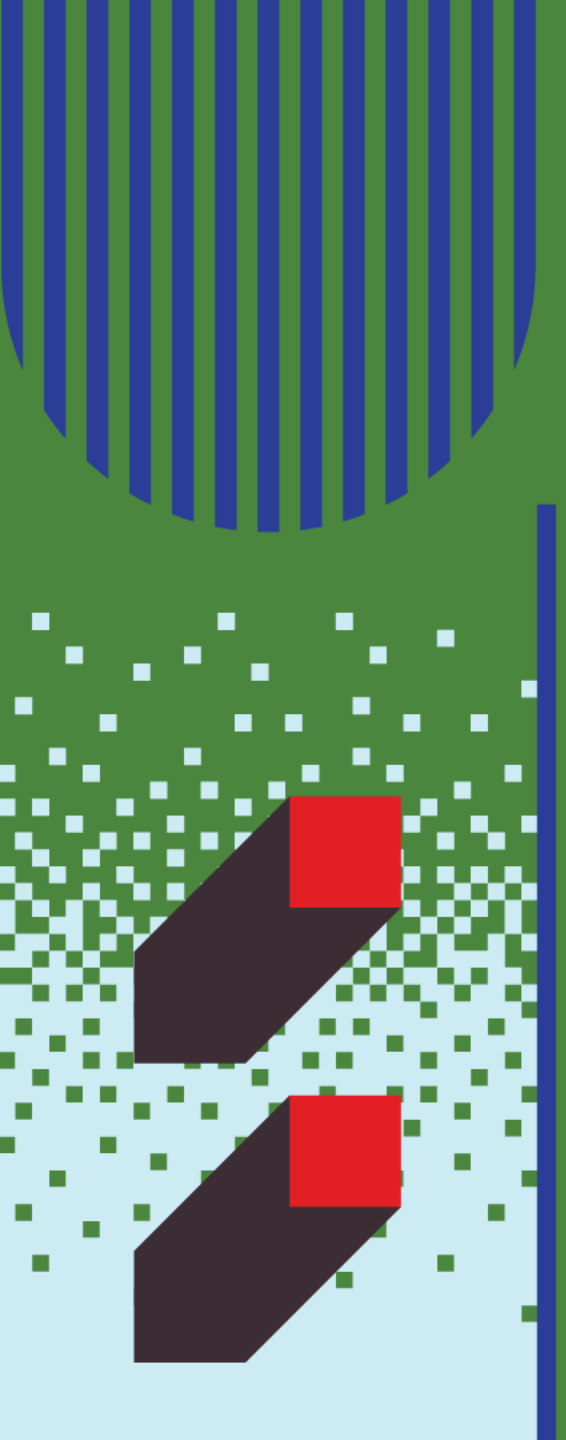


IAPP Global Summit 2026

Privacy | AI governance | Cybersecurity law

Conference 30-31 March

Workshops 1 April

Training 1-2 April

WASHINGTON, DC

#IAPPSummit26

How AI is Changing Data Protection

AI and Data Protection

Perspectives from U.S., UK, and EU

WELCOME AND INTRODUCTIONS

Edward McNicholas, JD,
Partner, Ropes & Gray LLP

Rohan Massey, PGDL, LPC
Partner, Ropes & Gray LLP

Frances Faircloth, JD,
Partner, Ropes & Gray LLP

Robert Silvers, JD,
Partner, Ropes & Gray LLP

AGENDA OUTLINE

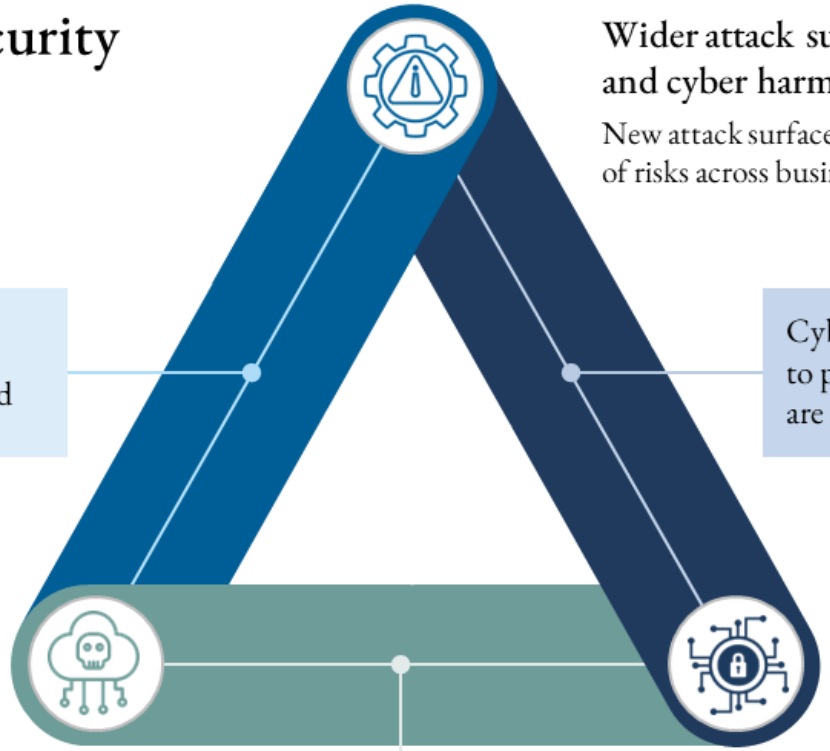
I. Session Outline
II. Welcome and Introductions
III. How AI is Changing the Data Protection Landscape
IV. AI & Data Protection in the U.S.
V. AI & Data Protection in the UK
VI. AI & Data Protection in the EU
VII. Questions and Answers
VIII. Closing Remarks

How AI is Changing Data Protection:
AI Enhancing Cybersecurity

- Real-time threat detection
- Fraud and anomaly detection
- Automated incident response
- Phishing detection
- Malware identification
- Vulnerability management
- Security analytics and prediction
- User behavior analytics (UBA)
- Data mining speed increasing to identify victims faster

How AI is Changing Data Protection:
AI & Cybersecurity Risk Surface Evolving

Impacts of AI on Cybersecurity



Wider attack surface and cyber harms to enterprise

New attack surface and propagation of risks across businesses

New attack surface offers new targets and attack vectors, which will need to be defended

Cybersecurity capabilities need to innovate to protect the business; consequences of attacks are tightly linked to business processes

More potent cyberattacks

Toxicity of cyberspace increases, targeting of victims more effective

Enhanced cyber defence tools

Better prevention and attack detection, and more effective incident response

Next-generation cyber arms race driven by threat interest and potential for collateral damage

Source: Artificial Intelligence and Cybersecurity: Balancing Risks and rewards (2025). World Economic Forum

How AI is Changing Data Protection: Different Approaches to AI Regulation

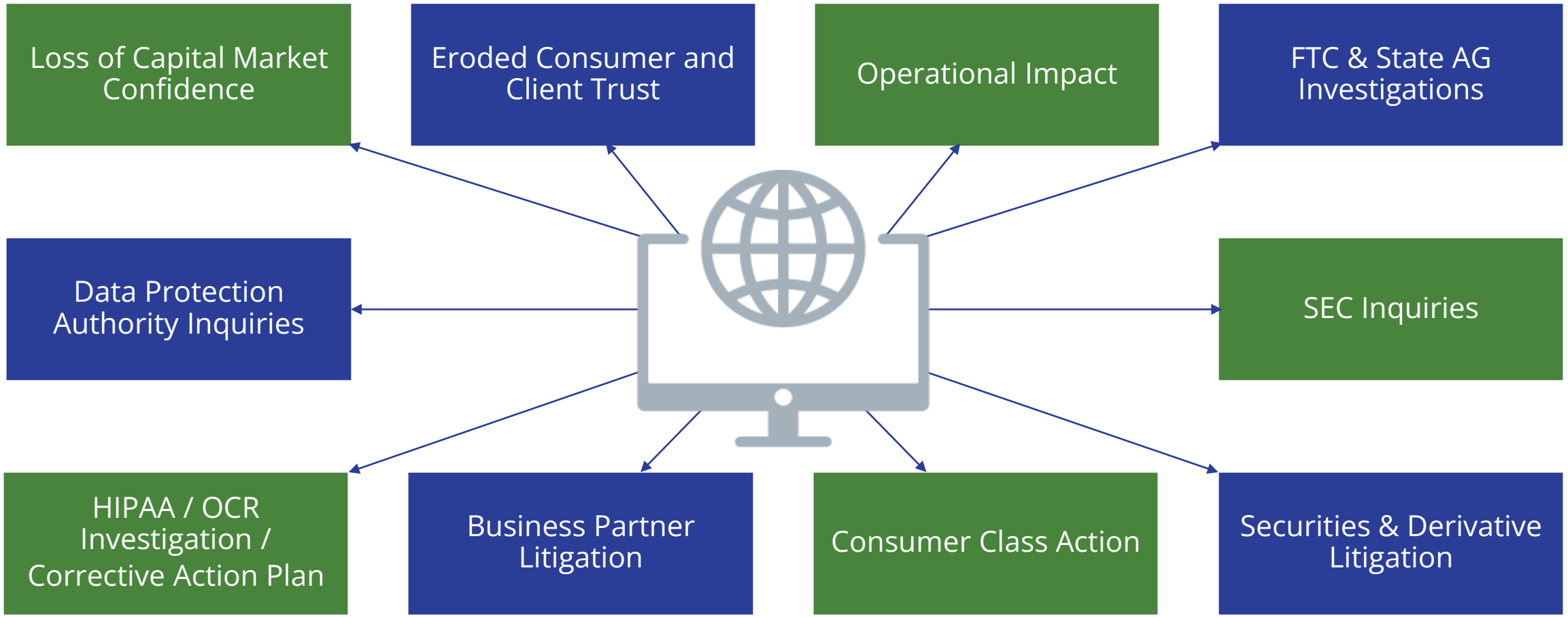
	EU	UK	US
Type of Regulation	Legislative (AI Act)	Non-statutory (existing regulators)	No federal law (executive orders + state laws)
Regulatory Approach	Prescriptive (detailed rules based on risk)	Principles-based, non-binding	Voluntary guidelines (federal vs state conflict)
Regulatory Bodies	National authorities + EU AI Board	No new regulators (existing bodies apply principles)	No AI regulator (agency coordination + litigation task force)
Penalties	Up to €35M or 7% of global turnover	No new penalties (existing penalties)	No federal AI penalties (state penalties under challenge)

AI & Data Protection in the U.S.: Substantive, Bipartisan, Federal Consensus

"Open, Interoperable, Reliable, and Secure Internet"

- Corporate and government information sharing
- Federal sectoral requirements (defense contractors, financial services, health, nuclear, communications, public companies, etc.)
- Federal and state laws against "unfair" or "deceptive" trade practices enforced by Federal Trade Commission and state Attorneys General
- State comprehensive and sectoral security laws
- Common law torts enforced through class actions
- Industry self-regulation, such as payment cards

AI & Data Protection in the U.S.: U.S. Implications of Data Breaches



AI & Data Protection in the U.S.: U.S. AI Regulation Overview

Currently a **patchwork of regulations**, many proposals

- **NIST AI Guidance**: broad, non-binding guidance focusing on reliability, safety, security, and accountability of AI systems
- **Biden Executive Order on AI** (Oct. 2023): principles to ensure a safe, reliable and unified approach to AI governance
- **Trump Executive Order on AI** (Jan. 23, 2025): revokes Biden's EO and rescinds actions taken under it; emphasizes deregulation and promotion of AI innovation to boost U.S.
- **Congress**: bipartisan legislative framework to "establish guardrails" for AI introduced in Sep. 2023 and tabled; proposed independent oversight body & registration of "high risk" models

AI & Data Protection in the U.S.: States as Laboratories of Democracy

Colorado AI Act

- Regulates High Risk AI systems: systems that make a consequential decisions related to sensitive areas such as employment or insurance.
- Regulates algorithmic discrimination and prohibits disparate treatment by AI.
- Required disclosures: statement from companies who use or develop High Risk systems regarding the intended use cases and benefits of AI, analysis of risk, description of data inputted into the AI, post-deployment safeguards, and other required disclosures.
  - Transparency: even non-High Risk AI systems must disclose AI use to consumers.
  - Incident reporting obligations.
- AI deployment obligations: entities that use AI from third parties must have robust disclosure and compliance programs.

AI & Data Protection in the U.S.: The Current Political Picture

Significant shifts in norms in the second Trump Administration continue to impact cybersecurity

- Restructuring of civil service generally.
    - Democratic **FTC** Commissioners fired
    - Privacy & Civil Liberties Oversight Board firings
    - **CISA** staff cut / mission uncertain
    - Bulk personal data transfers to China restricted
- Shift away from multilateral engagement.

AI & Data Protection in the U.S.: AI in President Trump's Cyber Strategy

March 6, 2026

- "We will deploy the full suite of U.S. government defensive **and offensive** cyber operations. We will **unleash the private sector by creating incentives to identify and disrupt adversary networks** and scale our national capabilities."
- "We will work to adopt **AI-powered cybersecurity solutions** to defend federal networks and deter intrusions at scale."
- "And we will secure the AI technology stack—including our data centers—and promote innovation in AI security. We will swiftly implement AI-enabled cyber tools to detect, divert, and deceive threat actors."
- "We will **rapidly adopt and promote agentic AI** in ways that securely scale network defense and disruption."
- "Through **cyber diplomacy**, we will ensure that AI—particularly generative AI and agentic AI—advances innovation and global stability. We will secure the data, infrastructure, and models that underpin U.S. leadership in AI and we will call out and **frustrate the spread of foreign AI platforms that censor, surveil, and mislead** their users."

AI & Data Protection in the U.S.: AI in President Trump's Cyber Strategy

Encouraged by Colorado, other states like CA, CT, NY, TX, and UT have also enacted bills targeting AI governance, transparency, and responsibility.

On Dec. 11, 2025, President Trump signed a new **Executive Order** titled "Ensuring a National Policy Framework for Artificial Intelligence" after federal preemption efforts in Congress failed.

- The EO aims to establish a **national AI standard** and reduce the "patchwork" of state AI laws that the administration views as burdensome or conflicting with national policy.
- Directs the Attorney General to create an **AI Litigation Task Force** to challenge state AI laws deemed inconsistent with federal policy on preemption and interstate commerce grounds.
- Secretary of Commerce is ordered to evaluate state AI laws and consider making states with "onerous" AI rules ineligible for certain federal funds and discretionary grants.

The legal authority of an Executive Order to preempt state laws is uncertain at best.

AI & Data Protection in the U.K./EU: Seven Principles of Data Protection / Privacy (GDPR)

1 Transparency, Fairness & Lawfulness

Personal data should be processed lawfully, fairly and in a manner that is transparent to the data subject.

2 Purpose Limitation

Personal data should be collected for specified, explicit and legitimate purposes.
We should not further process personal data for other purposes.

3 Data Minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4 Accuracy

Personal data should be accurate and, where necessary, kept up to date.

Personal data that are inaccurate should be promptly erased or rectified.

5 Storage Limitation

Personal data should be kept for no longer than is necessary for the purposes for which the personal data are processed.

6 Integrity & Confidentiality

Personal data must be processed securely, with appropriate technical and organisational measures to prevent unauthorised or unlawful processing and accidental loss or damage.

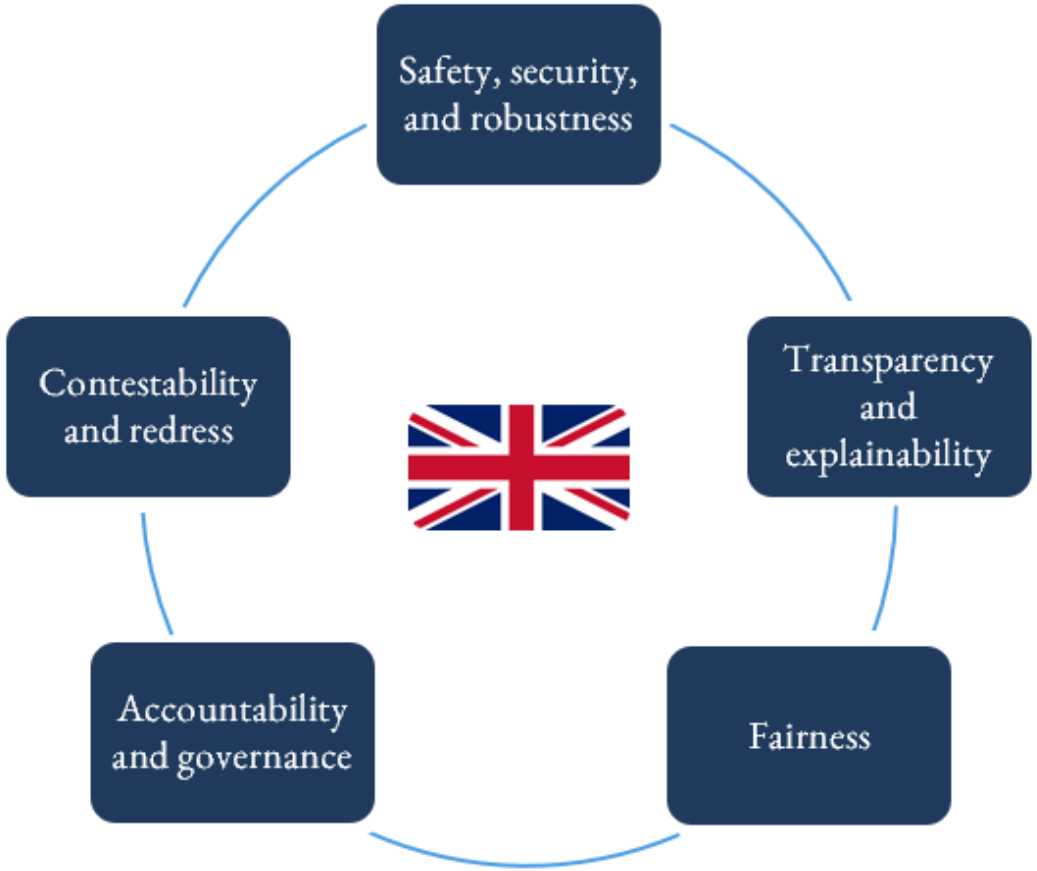
7 Accountability

We should be able to demonstrate, through ongoing recordkeeping and documentation of policies and practices, compliance with measures that give effect to these principles.

= GDPR Compliant

AI & Data Protection in the U.K.: The U.K. Approach to AI Regulation

- The UK's approach is technologically neutral, with a focus on context and sector-specific application to avoid stifling innovation or placing undue burden on businesses.
- However, the UK is carving out targeted rules for high-risk AI applications (particularly generative AI and deepfakes) through existing legislation.
- An **AI Bill** is proposed for late 2026 to (potentially) tackle frontier models, copyright issues, and possibly establish a statutory AI authority – but no firm legislation has been set, and further delays are expected.
- Until then, the UK will operate under a principles-based regime guided by **five** cross-sector principles:



AI & Data Protection in the U.K.: A Sectoral Approach to Regulation

The UK's pro-innovation approach avoids a single overarching AI law, instead allocating responsibility to existing sector regulators – each applying the five cross-sector principles within their own remit.

Key UK Regulators

ICO

- Regularly publishes guidance on data protection and AI (e.g., its AI and biometrics strategy *"Preventing Harm, Promoting Trust")*
- Regulatory sandboxes
- Voluntary audits
- Frequent enforcement (e.g., £7.5m Clearview AI fine)

FCA

- Self-labelled "technology-agnostic, principles-based and outcomes-focused regulator"
- Confirmed no bespoke AI-specific rules will be introduced
- Planning a Code of Practice on AI with the ICO
- Senior Managers & Certification Regime

Ofcom

- Oversees AI in online platforms primarily through the Online Safety Act 2023 (OSA)
- Issued its second OSA fine to an AI deepfake website in November 2025
- In January 2026, opened an investigation into Novi Ltd's AI chatbot and Grok AI on X

CMA

- Most active regulator; opened five merger control investigations into AI partnerships
- 80-person Data, Technology and Analytics unit
- New powers under the Digital Markets, Competition and Consumers Act (DMCCA)

AI & Data Protection in the E.U.: An Overview of The EU AI Act

The first attempt at a legislative framework for AI

- Classifies AI according to risk, with outright bans for AI that present the highest risk and the degree of regulation corresponding with the risk presented by a particular AI system.
- Imposes significant obligations on a range of parties involved with high-risk AI systems.
- Broad territorial scope with an extraterritorial effect, covering providers and users of AI systems within and outside the E.U.
- Enforcement options include fines of up to EUR 35 million or 7% of global revenue, as well as requests for information and powers to compel corrective measures or to recall the AI system from the market.

AI & Data Protection in the E.U.: An Overview of The EU AI Act

Key Timelines

- Staggered application of provisions between now and August 2027, with most provisions taking effect from 2 August 2026.

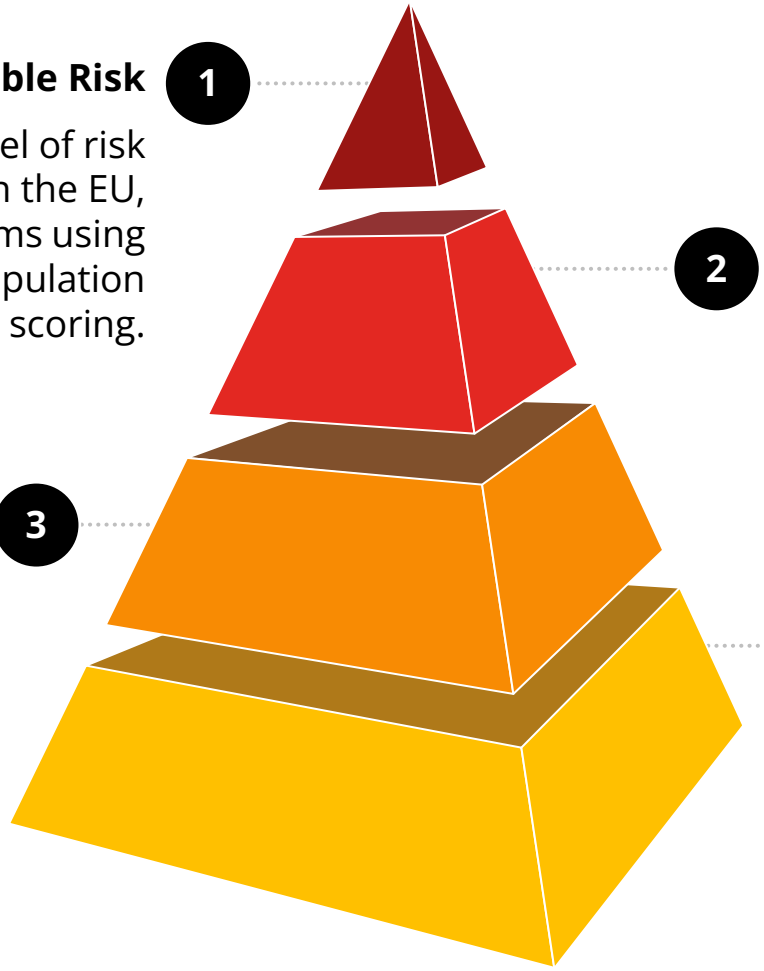
2024	2025	2026	2027
Published on 12 July 2024	Foundational provisions and guidance issued: AI literacy, GPAI governance, and model obligations	Most other provisions take effect: enforcement powers, regulatory sandboxes, role definitions, etc.	Fully operational on 2 August 2026 – but high-risk AI rules have an extended transition period until 2027

- The Digital Omnibus Proposal – a package of simplifications to EU digital regulations – is progressing through the legislative process and would amend the AI Act by extending compliance timelines for high-risk systems, easing the use of sensitive personal data for AI training, and centralizing enforcement of GPAI models under the AI office.

AI & Data Protection in the E.U.: EU AI Act: Classification of Risk

Unacceptable Risk 1

Highest level of risk prohibited in the EU, e.g., AI systems using subliminal manipulation or general social scoring.



High Risk 2

Most regulated AI systems, as these have the potential to cause significant harm if they fail or are misused, e.g., if used in law enforcement or recruiting.

Limited Risk 3

Includes AI systems with a risk or manipulation or deceit, e.g., chatbots or emotion recognition systems. Humans must be informed about their interaction with the AI.

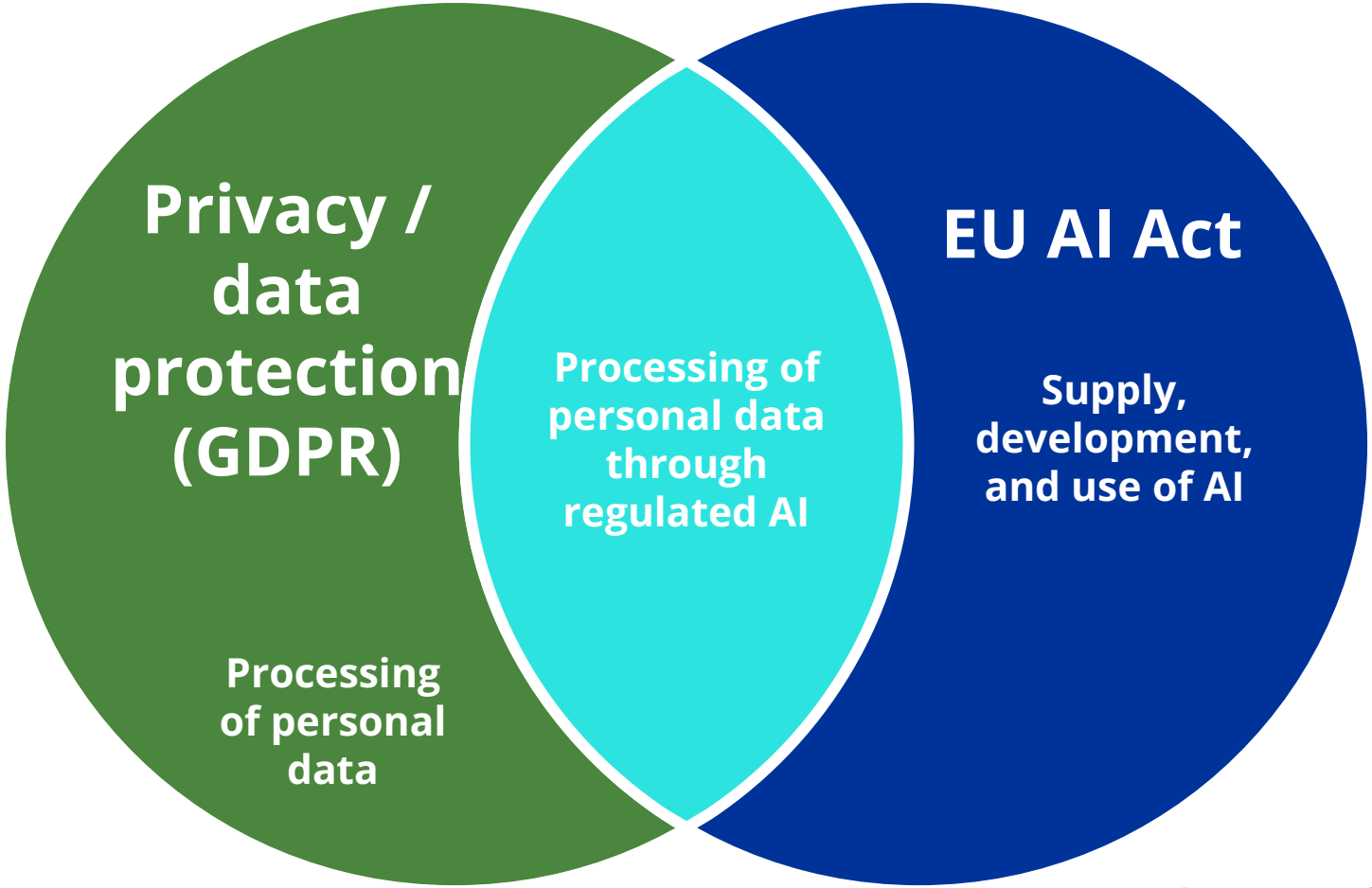
Minimal Risk 4

All other AI systems, e.g., a spam filter, which can be deployed without additional restrictions.

As well as intended use, the Act allows the Commission to take into account the **"extent to which the AI system acts autonomously"** when assessing whether a system results in an adverse impact on fundamental rights.

AI & Data Protection in the E.U.:
EU AI Act & Privacy Overlap

While the EU AI Act focuses primarily on the **technical security and risk classification** of systems, the GDPR still sets the framework for processing of personal data and managing data subject rights.



AI & Data Protection in the E.U.: Key Regulatory Issues

Risk Classification under EU AI Act

Many common AI uses (hiring, credit scoring, fraud detection) – may fall within the high-risk category of the EU AI Act, triggering strict compliance duties.

Transparency and Explainability

AI makes transparency difficult; its decision paths are complex and changing, making it harder to provide clear and meaningful explanations.

Human Oversight

AI (and agentic AI) complicates oversight requirements: these systems are designed to reduce human involvement. The task of balancing the right level of human involvement with the increased autonomy of these models will be a key challenge for early adopters of AI.

Accountability

AI systems may involve multiple actors; model providers, system providers, and deployers, each with different expertise, resources, and information. This diffusion of responsibility makes it difficult to assign clear accountability for risk management and compliance.

Individual Data Rights under GDPR

Responding to data rights requests can be especially difficult with AI, given its use of memory, logs, and complex decision paths.

QUESTIONS

CONTACT LIST

Edward McNicholas, JD,
Partner, Ropes & Gray LLP
edward.mcnicholas@ropesgray.com

Rohan Massey, PGDL, LPC
Partner, Ropes & Gray LLP
rohan.massey@ropesgray.com

Frances Faircloth, JD,
Partner, Ropes & Gray LLP
fran.faircloth@ropesgray.com

Robert Silvers, JD,
Partner, Ropes & Gray LLP
robert.silvers@ropesgray.com

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Summit 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!