simmons+simmons

AI & Data Protection Series

Enforcement of AI issues under data privacy law

January 2026

Minesh Tanna, Partner, Disputes & Investigations; Global AI Lead
Alejandro Guerrero, Partner, Disputes Resolution
Emilie Danglades-Perez, Of Counsel, Dispute Resolution

Our speakers

Minesh Tanna
Partner &
Global AI
Lead
London

Alejandro Guerrero
Partner
Brussels

Emilie Danglades-Perez
Of Counsel
Paris

List of webinars and dates

27 May: Data privacy considerations in AI model training

12 June: AI and GDPR purpose limitation requirements

24 June: AI-related Data Protection Impact Assessments (DPIAs)

22 July: Data privacy considerations in APAC AI legal regime

9 September: AI and individuals' rights under the GDPR

23 September: Automated decision making and profiling

7 October: Marrying GDPR and AI governance

21 October: AI and biometric data/special category data

4 November: AI and data security

3 December: GDPR considerations in contracting for AI solutions

28 January: Enforcement of AI issues under data privacy law

18 March: Incident Response – GDPR vs EU AI Act

Agenda

- GDPR decisions on AI tools by European data protection authorities
- Future enforcement focus areas
- Interplay between enforcement under the EU AI Act and GDPR
- Questions?

GDPR decisions on AI tools by European data protection authorities

Enforcement actions – the €90M+ total fines against Clearview AI

Netherlands (2024), France (2022), Italy (2022), Greece (2022)

Monetary sanctions: €30.5M (NL) , €20M (FR) , €20M (IT) , €20M (GR).

The issue: mass scraping of open-source photos for biometric identification and profiling.

Key legal breaches: Art. 6 and 9 (biometric data) and Art. 5(1)(a) (fairness and transparency).

Precedent: public availability of data does not grant a license for automated re-use or AI training by third parties.

Aggravator: Massive scale ; sensitive biometric data ; lack of cooperation

Major AI sanctions – the €15M OpenAI (ChatGPT) decision

Italy (December 2024 ; updated March 2025)

Monetary sanction: €15,000,000

The issue: unlawful processing of personal data for training generative AI and lack of protection for minors.

Key legal breaches: Art. 6 & 9 GDPR: absence of a valid legal basis for massive data harvesting.

Art. 5(1)(d) GDPR: processing of inaccurate personal data (algorithmic "hallucinations").

Corrective measures:: Mandatory 6-month information campaign

Age verification: implementation of strict age-gates for users under 13.

Procedural status: the DPC (Ireland) is now the lead authority for ongoing compliance oversight.

Algorithmic moderation – transparency and "shadow banning"

Lithuania (2024)

- **Monetary sanction:** €2,385,276
- **The issue:** covert restriction of user accounts via automated moderation
- **Key legal breaches:** Art. 5(1)(a) (transparency and fairness)
- **The violation:** users were not informed of the logic behind AI-driven restrictions
- **Rights denied:** failure to process erasure requests under Art. 17

AI in employment – the "Frank" algorithm decision

Italy (2024)

- **Monetary sanction:** €2,500,000
- **The issue:** opaque AI-driven shift assignments and performance scoring
- **Key legal breaches:** Art. 22 (automated decision-making)
- **The violation:** lack of human oversight and failure to explain the "logic involved" (Art. 13)
- **Requirement**: technical transparency is mandatory for AI impacting worker rights

Regulatory freezes – X and the DeepSeek "App Store" block

Germany, Ireland, Italy, Greece (2024)

Monetary sanction: None (immediate service blocks and app store removals)

The X (Grok) case: Irish DPC used urgency powers to halt AI training on EU data.

The DeepSeek case (Italy, Jan 2025): Immediate block for lack of EU representative (Art. 27).

The DeepSeek case (Berlin, June 2025): App store removal requested for unlawful data transfers to China without adequate safeguards (Art. 46).

Key issue: Failure to comply with EU territorial anchoring and data transfer rules.

Complaints - AI outputs as a legal liability

Lithuania (2024)

Monetary sanction: pending (ongoing investigation)

The issue : AI-generated "reputation reports" containing inaccurate data

Key legal breaches: Art. 5(1)(d) (principle of accuracy)

The argument: GDPR violations through sale of inaccurate data and charges for access

Rights issue: no possibility to rectify inaccurate information (Art. 16)

Future enforcement focus areas

Key risk / enforcement areas

GDPR and AIA risk areas

GDPR

- Data protection principles
- Legal bases (focus on legit. interests vs consent)
- Transparency
- Data subjects rights (focus on right to object and ADM)
- DPIAs

AIA

AI systems

- Input
- Functioning
- Output

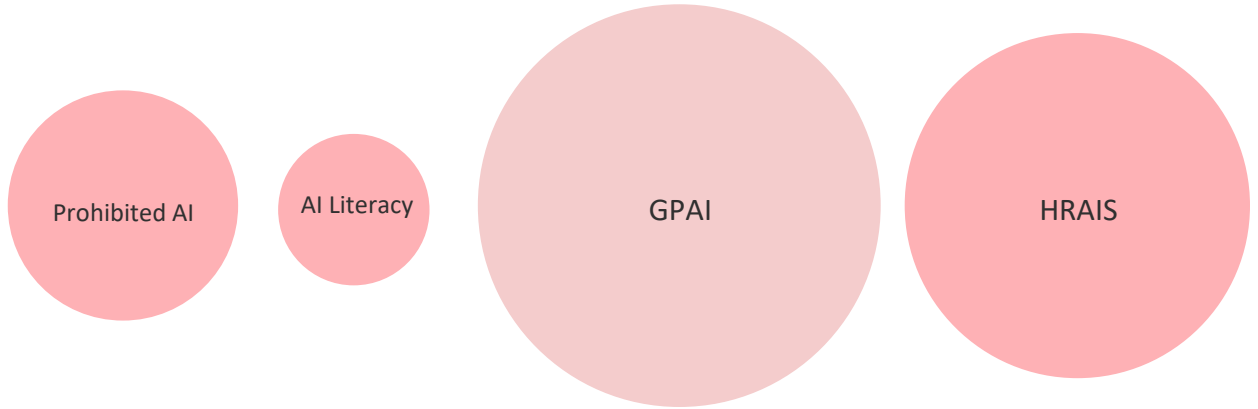
GPAI models

- Input
- Training

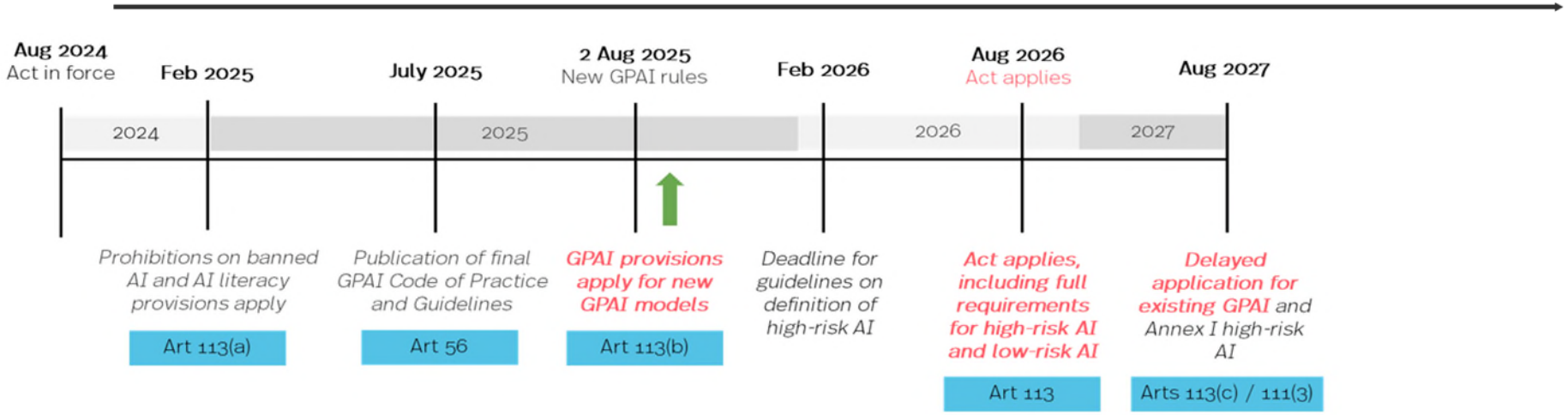
Key risk / enforcement areas

AIA enforcement risks and timeline

Risk areas



AIA application timeline



Key risk / enforcement areas

GDPR / AIA: Data collection and legal bases

- **Legal Bases**: Collecting data for AI model training observing legal bases under GDPR and other applicable regulations:
  - Collection of data used in prior processing for new purposes (AI model training).
  - Internet content processing/scrapping to collect data for model training.
  - AI-powered facial recognition and tracking systems for public/private space monitoring (e.g., right to object, preserve anonymity), including processing of data of non-target individuals (e.g., "bystanders" in facial recognition datasets).

Key risk / enforcement areas

GDPR / AIA: Processing

- Re-identification: “De-anonymisation” of anonymous datasets by cross-referencing them with other available information.
- Sensitive Data Processing: AI capabilities to connect non-sensitive/anonymized data points to accurately infer personal traits, such as health conditions, political views, or sexual orientation.
- Data Processing Limitations: Reuse of information shared for one specific purpose to train models for entirely different purposes.
- Informed Processing: Lack of transparency regarding how personal data is being used to train a model or for the system to take a decision.

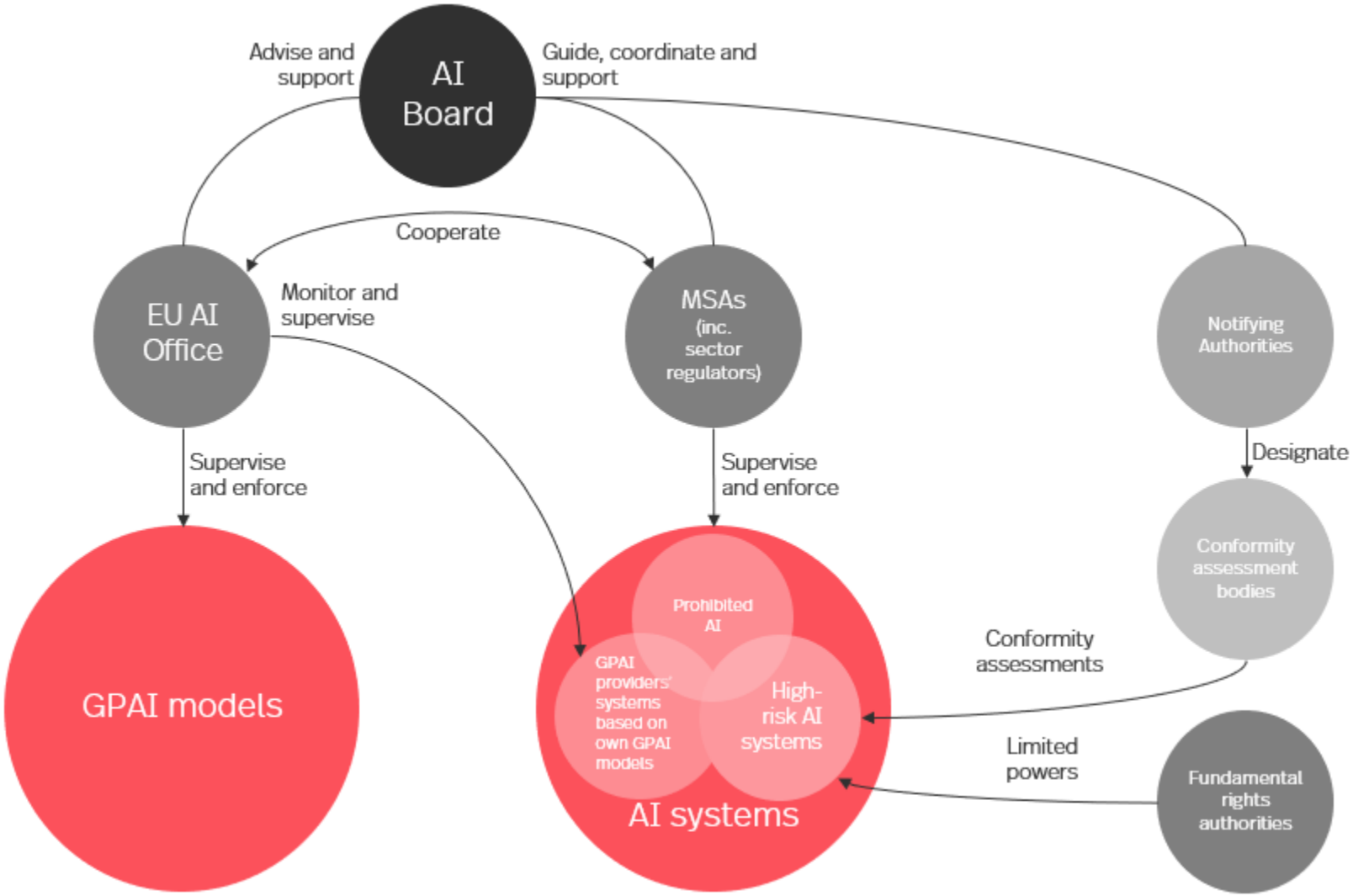
Key risk / enforcement areas

GDPR / AI substantive areas – Practical applications

Substantive Issue	GDPR relevance	AIA relevance
Deepfakes	Personal data definition (ressemblance) Legal bases (sensitive personal data, « biometric data)) Lawfulness of data processing	Harm of use of AI system/model « Deepfake » information Systemic risks
Nudity apps	Personal data definition (ressemblance) Legal bases (sensitive personal data, « biometric data)) Lawfulness of data processing	Harm of use of AI system/model « Deepfake » information Systemic risks
AI and children data	Legal bases (children consent) Lawfulness of data processing	Harm of use of AI system/model Systemic risks
Harm-inducing chatbots	Legal bases (legitimate interest, consent) Lawfulness of data processing	Harm of use of AI system/model Systemic risks
AI model training	Personal data definition (identification) Legal bases (legitimate interest, consent) Lawfulness of data processing	GPAI model training rules (policy for unlawful content removal)

Interplay between enforcement under the EU AI Act and GDPR

Enforcement under EU AI Act



EU AI Act - Main MSAs

Confirmed MSAs		Likely MSAs	
Member State	MSAs (* denotes where multiple)	Member State	Likely MSAs* (* denotes where multiple)
Cyprus	Commissioner of Electronic Communications*	Belgium	Belgian Institute for Postal Services and Telecommunications*
Denmark	Danish Agency for Digitisation*	Bulgaria	The Commission for the Protection of Personal Data*
Finland	The Finnish Transport and Communications Agency*	Czech Republic	Czech Telecommunications Office
Hungary	Minister responsible for Enterprise Development*	France	Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF)*
Ireland	National AI Office*	Germany	Federal Network Agency*
Italy	National Cybersecurity Agency (ACN)*	Luxembourg	National Commission for Data Protection (CNPD)*
Latvia	Consumer Rights Protection Centre*	Netherlands	Dutch Data Protection Authority*
Lithuania	The Communications Regulatory Authority	Poland	Artificial Intelligence Development and Security Commission*
Malta	Malta Digital Innovation Authority*	Portugal	National Communications Authority (ANACOM)
Slovenia	Agency for Communications Networks and Services	Slovakia	Ministry of Investment*
		Spain	Spanish Artificial Intelligence Supervisory Agency (AESIA)*
		Sweden	Swedish Post and Telecom Authority*

DPAs as MSAs under EU AI Act

DPAs as main MSA

- Member States might appoint DPA as main MSA e.g. CNIL, Dutch DPA
- Member State MSAs have exclusive competence to enforce prohibited AI, AI literacy, high-risk AI systems and low-risk AI systems under the AIA
- DPAs constrained by one-stop-shop likely to be more aggressive
- Potential jurisdictional challenges around overlap with GDPR (one-stop-shop issues)

DPAs as "secondary" MSA to enforce certain HRAIS

- DPAs to enforce AIA requirements for: remote biometric ID systems, biometric categorisation systems, emotion recognition systems and HRAIS for law enforcement, border management, and justice
- Potential jurisdictional challenges around intended purpose of AI systems (particularly GPAI systems) and overlap with GDPR (one-stop-shop issues)
- Potential conflict in interpretation of concepts relevant to both AIA and GDPR

DPA indirect enforcement through GDPR

DPAs may issue RFIs / commence investigations under the GDPR relating to AIA

- Art. 5 AIA prohibitions cannot be enforced by AIA regulators until 2 August 2026, but are applicable and legally binding as from 2 February 2025
- If personal data is processed in course of an alleged prohibition, DPA may allege that:
  - No lawful basis under Art. 6 GDPR; and/or
  - Breach of requirement that personal data be processed "*lawfully, fairly and in a transparent manner in relation to the data subject*" under Art. 5(1)(a) GDPR
- Any action or finding by the DPA would need to be under, and confined to an alleged breach of, the GDPR
- DPA would need to establish that prohibition has occurred under AIA in the context of establishing GDPR violation (if the allegation was that processing was unlawful and in the absence of other, clearer, GDPR breaches)

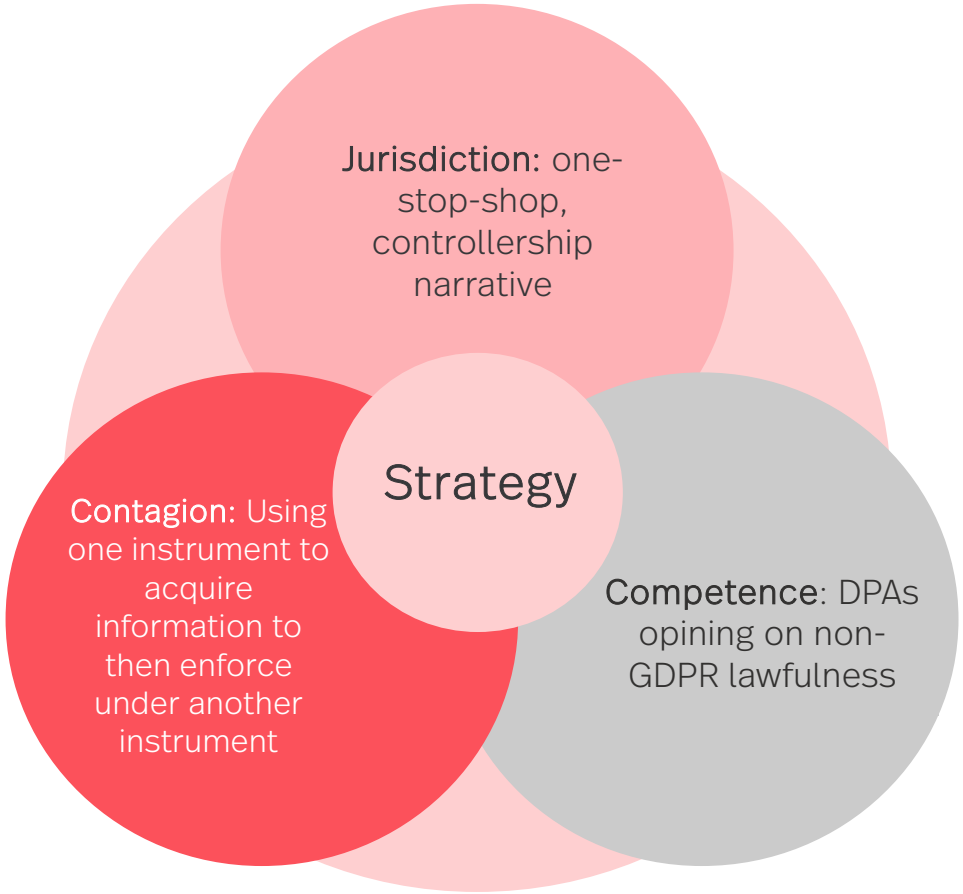
DPA indirect enforcement through GDPR: Spain

The Spanish Data Protection Agency (AEPD) published an Article on 15 July 2025:

However, it is important to note that the AEPD does not see its status as the **competent authority for the protection of personal data** altered, which includes, under its supervision and control tasks, those **processes carried out using artificial intelligence**. Therefore, although it is not a direct application of the AI Regulation, the AEPD can supervise and act against the processing of personal data carried out through prohibited systems, to the extent that they affect the right to data protection.

The Agency recommends that entities that implement or provide applications and services based on AI systems, as soon as they are bound by the future full application of the RIA, **be prepared to comply with their obligations by taking appropriate measures** to ensure their full compliance.

Strategic considerations



Any questions?

Useful resources

CtrlTransfer

Digital Regulation Tracker

AI Literacy Programme

Final session > 18 March: Incident Response – GDPR vs EU AI Act