AI & Data Protection Series

Marrying GDPR and AI Governance

October 2025

Christopher Götz, Partner, Digital Business

Jaap Tempelman, Partner, Digital Business

Our speakers

Christopher Götz
Partner
Munich, Germany

Jaap Tempelman
Partner
Amsterdam, Netherlands

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

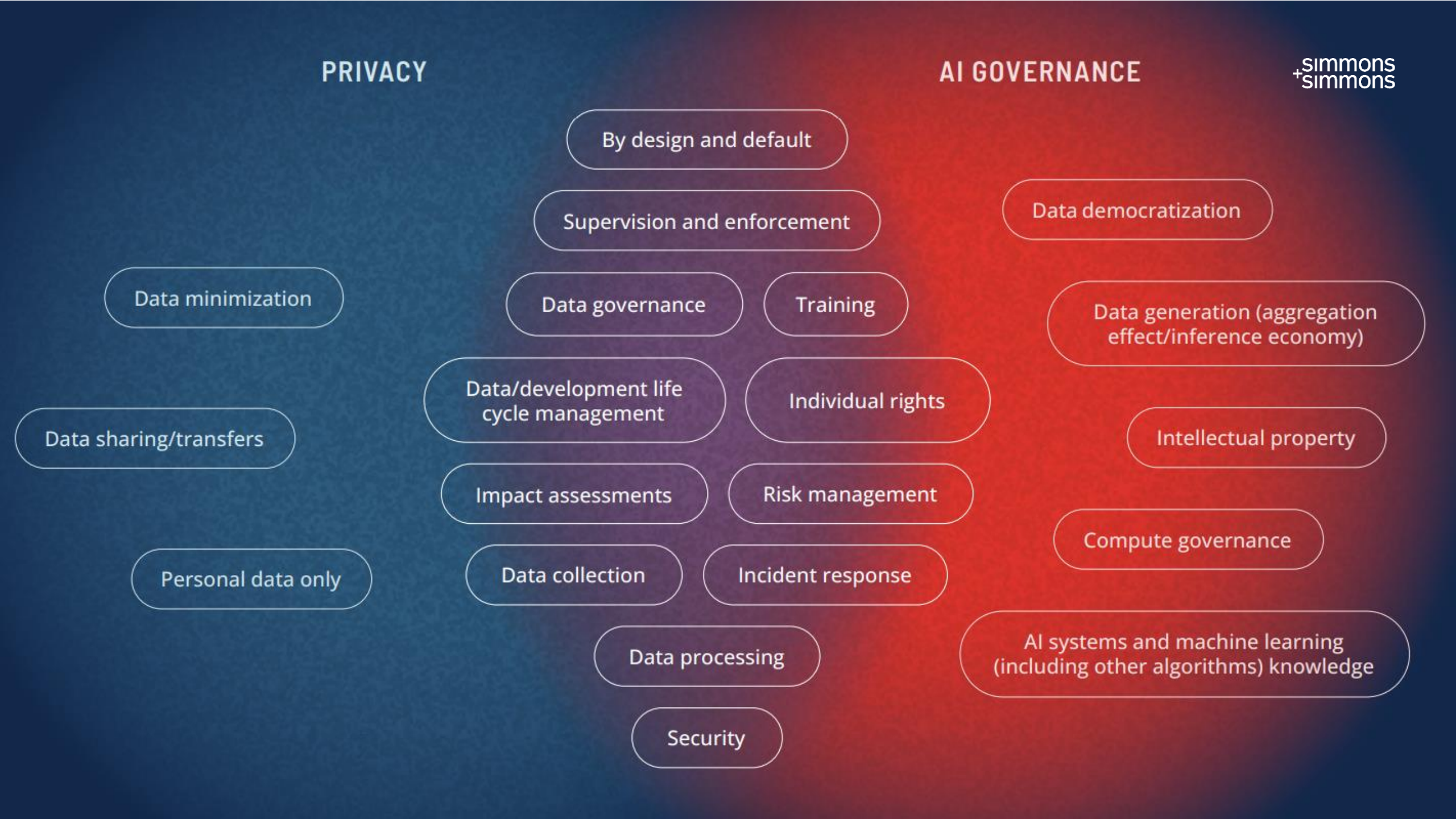
7 October: **Marrying GDPR and AI governance**

21 October: **AI and biometric data/special category data**

4 November: **AI and data security**

18 November: **GDPR considerations in contracting for AI solutions**

Overlaps between GDPR and EU AI Act Governance


PRIVACY
AI GOVERNANCE
simmons+simmons
By design and default
Supervision and enforcement
Data democratization
Data minimization
Data governance
Training
Data generation (aggregation effect/inference economy)
Data/development life cycle management
Individual rights
Data sharing/transfers
Intellectual property
Impact assessments
Risk management
Compute governance
Personal data only
Data collection
Incident response
Data processing
AI systems and machine learning (including other algorithms) knowledge
Security

By design and default

1. The use of large volumes of personal data underlies the development of many AI systems (e.g., LLMs like Chat GPT) and the processing of personal data is part of many business cases for the deployment of AI systems (e.g., workplace AI solutions).
2. Privacy and data protection are an integral element of the (by-design) requirements under the EU AI Act for AI systems.

Recital 69 of the EU AI Act

The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed.

Risk management and impact assessments

1. Article 9 of the AI Act requires setting up a risk management system in respect of high-risk AI systems that:

    - identifies and analyses the known and reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights;

    - mitigates or eliminates these risks through the development or design of the high-risk AI system.

2. Impact assessments (in the context of Article 9 and Article 27 AI Act) can be based on existing approaches taken for privacy impact assessments.

3. Privacy by design and impact assessments identify privacy concerns in different scenarios, relating those concerns to technical design choices, and embedding privacy principles throughout the data life cycle and in IT services and products. The same approach is appropriate for AI ethics by design and related impact assessments, which can be tied to existing privacy by design and impact assessment processes.

4. Privacy teams are familiar with navigating interdisciplinary challenges, working with other teams to balance policy, legal guidelines, business needs and technical requirements. A similar approach is required in AI governance.

Security and incident notification

Cybersecurity

- Article 15 of the AI Act requires high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity.
- Security measures and (privacy enhancing) technologies used in complying with security requirements under the GDPR may play a large role in the security measures to be deployed in developing and deploying AI systems.

Incident notification

- Article 73 AI Act requires providers of high-risk AI systems to notify serious incidents to the market surveillance authorities of the Member States where that incident occurred.
- Serious incidents may include notifiable personal data breaches and notification processes call for alignment in that context.

Training of AI models with personal data: Relevance of GDPR & AI Governance for the AI value chain

Data quality & data governance

AI Act & GDPR requirements overlap

High-risk AI systems that make use of techniques involving **training of AI models** with data

➡ Implementation of appropriate "**data** governance" with regard to training, validation, and test data sets and ensuring "data quality"

- **Data** sets must be relevant, sufficiently representative, and as **accurate** and complete -- in view of the **intended purpose** – to the best extent possible (Art. 10(3) AI Act).
    - Overlap with Art. 5 para. 1 GDPR
        - (d) (“Accuracy - principle”)
        - (b) (“Purpose limitation”)
- The processing of **sensitive personal data** is permitted if it is "absolutely necessary" for the purpose of monitoring and **preventing discrimination** and if additional conditions are met:

Data quality & data governance

AI Act & GDPR requirements overlap

Processing sensitive personal data to avoid bias – prerequisites:

- **Synthetic or anonymized data** cannot be used effectively for this purpose
- Technical restrictions on reuse and **state-of-the-art security** and **data protection** measures (including pseudonymization)
- Strict access **controls** and access documentation
- No data transfer to/access to data by **third parties**
- **Data minimization**/storage limitation
- **Records of processing** activities contain justification

Classic GDPR requirements -- set out in Art. 10 para 5 AI Act!

Processing personal data within AI models

Guidance by Data Protection Authorities

EDPB Guidance on certain data protection aspects related to processing of personal data in the context of AI models (Opinion 28/2024)

For an AI model to be considered **anonymous**, both the **likelihood of**

1. **direct extraction of personal data** regarding individuals whose personal data were used to develop the model and of
2. **Obtaining** (intentionally or not) such personal data **from queries**,

are **insignificant** -- taking into account "all the means reasonably likely to be used'" by the controller or another person.

Legitimate interest as an appropriate legal basis for processing conducted in the context of the development of AI models?

3-step test:

1. **Legitimate interest** pursued by the **controller or a third party;**
2. **Necessity of the processing for the purposes** of the legitimate interest(s) pursued ("necessity test"); and
3. Legitimate interest(s) not overridden by the **interests or fundamental rights/freedoms of data subjects** ("balancing test").

Processing personal data within AI models

Deployment of an AI model via 3rd party AI system

Scenario:

AI model was trained with personal data – in **breach of the GDPR.**

Does this **negatively effect the value chain,** particularly **does this taint the deployment** of the model by a third party **AI system** provider/deployer?

EDPB Guidance (Opinion 28/2024): "Depends"

- If AI model considered "**anonymous**" (see above)
  - no issue

If „personal data is **retained** in the model"

- check that AI model was not developed by unlawfully processing personal data!
- Take into account source of data!

Hamburg DPA: Discussion Paper LLM & Personal Data (July 2024)

- LLM "does not store personal data"
- "potential violations during LLMs training phase do not affect the lawfulness of using such a model within an AI system."

GDPR & AI Governance

Manage AI Model risks in value chain

Checklist for AI system providers / deployers

- Conduct AI vendor due diligence
- Can AI model be considered “anonymous”?
- If not, in case **personal data** has been used for AI model training:
  - Did AI model provider conduct appropriate assessment (3-step legitimate interest - test)?
  - Did a supervisory authority / court determine GDPR-incompliance?
- In case sensitive personal data has been involved in training:
  - Check whether this has been necessary to avoid bias

AI Governance:
Role of DPOs

AI Governance: Role of a DPO?

Positive	Challenges
Existing expertise in risk and compliance – DPOs are already skilled in assessing data protection risks, documentation, and compliance frameworks.	**Limited mandate** – The DPO's legal role is defined by GDPR and focused on personal data; AI governance often extends beyond privacy.
Familiarity with data lifecycle – DPOs understand how data is collected, used, shared, and retained – core to responsible AI.	**Potential conflict of interest** – DPO independence requirements (Art. 38 GDPR) may clash with operational AI decision-making roles.
Established governance structures – Many organisations already have DPOs embedded in governance frameworks, offering a ready foundation for AI oversight.	**Insufficient technical depth** – AI governance may require expertise in model risk management, algorithmic transparency, or bias testing.
Cross-functional coordination experience – DPOs often liaise across IT, legal, and business units, aligning with the multidisciplinary nature of AI governance.	**Resource constraints** – Expanding the DPO's scope could overstretch limited capacity and dilute focus on core data protection obligations.
Regulatory **credibility – Authorities may view DPO involvement positively** as part of a robust accountability framework.	**Evolving regulatory landscape** – The EU AI Act is in essence a product safety law which is subject to an evolving regulatory landscape (national implementing laws, new technical standards) that may not fully align with the DPO's remit.

AI Governance: Role of a DPO?

Identified Challenge	Mitigation / Recommendation
Limited DPO mandate under GDPR	Define a **complementary AI Governance role** (e.g. AI Compliance Officer or Committee) to handle non-privacy aspects like model risk, safety, and transparency.
Potential conflict of interest	Clearly **separate advisory and decision-making functions**; the DPO should advise on AI data compliance but not approve or operate AI systems.
Insufficient technical expertise	Provide **targeted training** on AI risk assessment / the EU AI Act; establish cooperation with **IT team / data scientists / risk management teams.**
Resource constraints	Create a **cross-functional AI Governance Committee** to distribute workload; ensure DPO participation is focused on data-related AI risks.
Evolving regulatory roles (AI Act vs GDPR)	Map responsibilities between GDPR, AI Act, and complementing sectoral frameworks (e.g. DORA, Data Act); adopt a **matrix of accountability** to avoid overlaps or gaps.
Need for regulatory credibility and documentation	Embed AI considerations into existing **Data Protection Impact Assessments (DPIAs)** or create **combined AI + Data Protection Impact templates** for consistency.

National EU AI Act implementing laws: what role do DPAs play?

National AI Act implementing laws

Role of Data Protection Authorities (Examples)

Germany:

BNetzA = market surveillance authority

BaFin = for financial institutions if AI used to provide reg. financial service

National AI Act implementing laws

Role of Data Protection Authorities (Examples)

Netherlands:

Dutch Authority for Infrastructure and Data Protection Authority – coordinating authorities for general requirements (prohibited systems, transparency, GPAI)

Existing sectoral authorities – for sector-specific AI system applications

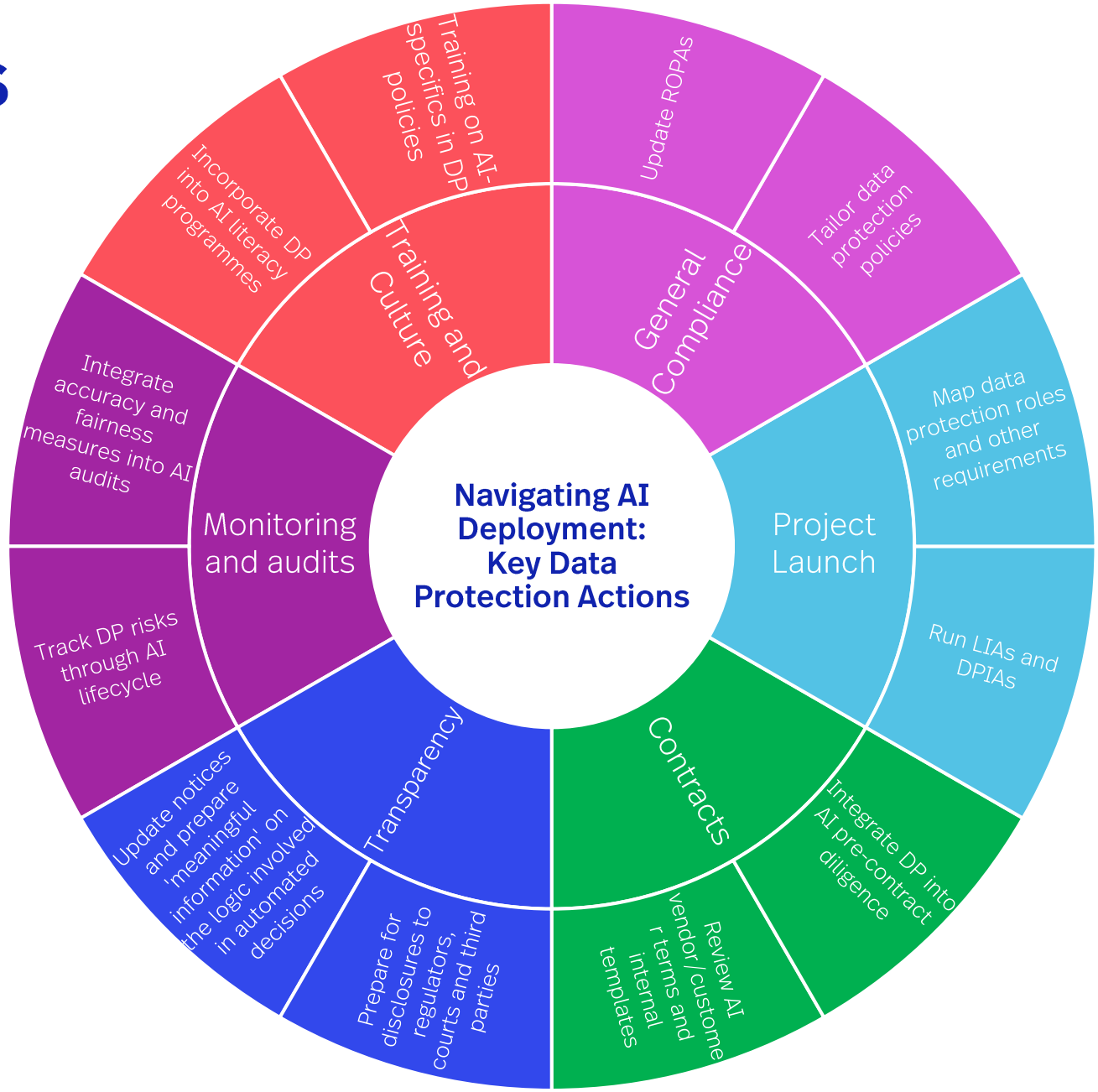
Key takeaways

Intersection between AI and DP

Key takeaways

- There are many overlaps between the EU AI Act and GDPR.
- Most AI systems interact with personal data – and AI technology has unique features that increase data protection compliance risks
- To ensure compliance and avoid delays in deployment, organisations looking to deploy AI responsibly and in line with data protection laws will need to ensure their compliance framework reflects this – regardless of whether the EU AI Act applies

Key actions


Navigating AI Deployment: Key Data Protection Actions
General Compliance
Update ROPAs
Tailor data protection policies
Project Launch
Map data protection roles and other requirements
Run LIAs and DPIAs
Contracts
Integrate DP into AI pre-contract diligence
Review AI vendor/customer terms and internal templates
Transparency
Update notices and prepare 'meaningful information' on the logic involved in automated decisions
Prepare for disclosures to regulators, courts and third parties
Monitoring and audits
Track DP risks through AI lifecycle
Integrate accuracy and fairness measures into AI audits
Training and Culture
Training on AI-specifics in DP policies
Incorporate DP into AI literacy programmes

Useful resources

CtrlTransfer

Digital Regulation Tracker

AI Literacy Programme

Next session > 21 October: AI and biometric data/special category data