# AI & Data Protection Series

## AI-related Data Protection Impact Assessments (DPIAs)

**June 2025**

Alex Brown, Partner, Digital Business

Minesh Tanna, Partner, Global AI Lead

# Our speakers

**Alex Brown**
Partner
London

**Minesh Tanna**
Partner
London

# 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

# AI-related DPIAs

## Today's topics

Focus on AI deployers and the DPIA related decisions and processes that they have to follow + compare / contract to AI Act risk assessments

- When is a DPIA required?
- What constitutes high-risk processing?
- What a DPIA has to cover
- The process for conducting a DPIA & who needs to be involved
- Outcomes from the DPIA process

# DPIAs

## Why have them?

- **GDPR accountability principle** – companies must be compliant and be able to demonstrate compliance
- **Data protection by design and default** – they enable early consideration of privacy considerations in system and process design
- **Risk assessment and mitigation** - technical safeguards, organisational policies, or changes to the processing activity
- **Transparency and trust** – particularly through consultation with affected individuals and / or publication of the DPIA
- **Regulatory engagement** – through consultation with the supervisory authority (if required)

# Where to start?

AI powered systems and tools come in all shapes and sizes and with a wide variety of use cases and capabilities – understanding the system and how it will be used is key.

# When is a DPIA required?

Where the processing

- in particular using **new technologies**, and
- taking into account the nature, scope, context and purposes of the processing

is likely to result in a **high risk** to the rights and freedoms of individuals.

DPIA required for:

- systematic and extensive evaluation of personal aspects based on automated processing, including profiling, on which decisions are made that produce **legal or similarly significant effects**
- large-scale processing of **special categories of personal data**
- systematic **monitoring of publicly-accessible areas** on a large scale.

## AI Examples

AI used for credit scoring or entitlement to benefits
AI powered recruitment systems
Smart city initiatives
AI monitoring traffic patterns with CCTV
Wearable health devices
Collecting and analyzing biometric data

# Lawful basis

## Why is personal data processing integral to AI model development?

- Effectiveness and accuracy
- Diverse data representation
- Contextual understanding
- Enhancing model robustness and safety
- Feedback and iterative improvement
- Real-world application

# Lawful basis

## Legitimate interest

1. Purpose Test: Identifying the legitimate interest
2. Necessity Test: Necessity of the processing
3. Balancing Test
4. Documentation and accountability

# Special category data

## Article 9 GDPR

- Explicit consent
- Substantial public interest
- Research and statistics
- Legal claims

# Special category data

## Special category data

- Limited conditions under which SCD can be processed:
  - Consent
  - Substantial public interest
  - Research and statistics
- EU case law (*GC and Others v CNIL*) and guidance – no processing of SCD until an individual rights request / verification of processing SCD

## Fairness

"*personal data is not processed by unfair methods, or by deception, or in a way that is 'unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject'. Considering the complexity of the technologies involved, information on the processing of personal data within AI models should therefore be provided in an accessible, understandable and user-friendly way*"

- European Data Protection Board (EDPB)

# Transparency

## Article 12-14 GDPR

- Provision of information
- Timing and method of information provision
- Transparency in training processes
- Challenges in AI transparency

**What happens in case of absence of transparency?**

- Investigations from data protection authorities in the EU/UK
- Temporary ban of the AI tool in one or several EU/UK countries
- Administrative fine

# Data minimisation

## Article 5 GDPR

1. Key aspects of data minimisation
    - Data collection must have clear, specific purposes
    - Use data that is adequate, relevant, and limited to the model's purpose
2. Techniques for data minimisation
    - Feature selection: Use only relevant data features
    - Perturbation: Add noise to reduce re-identification risk
    - Synthetic data: Use data that mimics real data without personal information
3. Challenges in AI Models

# Accountability

## Article 5.2. GDPR

- Understanding accountability
- Conducting data protection impact assessments (DPIAs)
- Documentation and governance
- Ongoing monitoring and review
- Transparency and communication

# Deployers

## Key considerations

1. Due diligence on AI model development and training
    - Data sources and basis for processing
    - Data minimisation methodology
    - Bias and fairness measures
2. Understanding the model's functionality and limitations
    - Explainability
    - Testing and validation
3. Risk management and accountability

# Useful resources

## CtrlTransfer

## Digital Regulation Tracker

## AI Literacy Programme

**Next session > 12 June:** AI and GDPR purpose limitation requirements