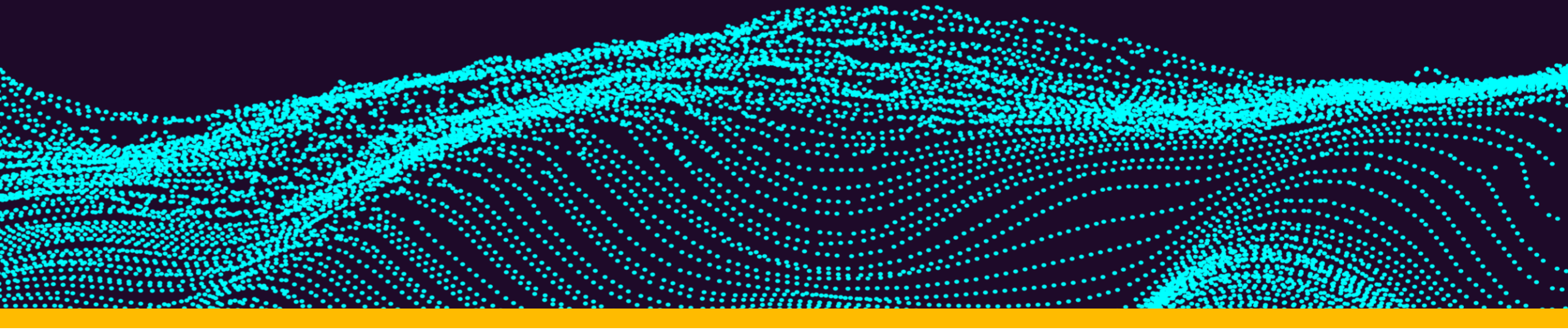
Data Analytics and Data Protection - Friends or Foes?



Alison Knight (PhD)
Senior Legal Adviser, University of Southampton

Seizing Opportunities And Preserving Values

Positive-Sum Model not Zero-Sum:
Replacing “Versus” with “And”

“There is no doubt the huge potential that creative use of data could have, but the price of innovation does not need to be the erosion of fundamental privacy rights.”

Elizabeth Denham
UK Information Commissioner

The above quote was used in announcing the decision by the ICO that the Royal Free NHS Foundation Trust violated data protection laws in providing 1.6 million patient details to Google DeepMind for analysis

Two Different Approaches to Data Protection:

1

Traditional EU Data Protection Laws (Directive)

- Static
- Absolute

2

General Data Protection Regulation (GDPR)

- Dynamic
- Adaptive

GDPR Dynamic/Adaptive Approach:

1

Much data relating to persons are – or may become in the future – personally identifiable data in this new era of expanded data discovery

2

Risk Assessment (Who, What, Why and & How of data access) must be combined with Risk Mitigation (Dynamic purpose preservation, Protection adaptation, & Data quality management)

3

Dynamic Pseudonymisation can facilitate data innovation via “Controlled Linkability” that ensures Fair & Lawful processing under GDPR Articles 5 & 6

The purpose for which personal data are processed in each case is crucial. Context is key!

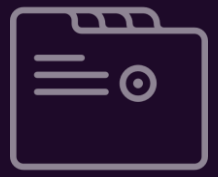
The Future of Analysis: Consent?

- Many organisations will find obtaining GDPR compliant ‘meaningful’ consent for data analytic purposes **impractical**
- If the initial legal basis for processing data is consent, it appears the only way to perform analysis on the data collected is via **re-consenting**
- Article 29 Working Party and commentators believe that alluding to data-driven generalised analysis will **not** satisfy Article 4(11) “specific” requirements for consent.

The Future of Analysis: Legitimate Interest!

Legitimate Interest

Must exist for data controller
and/or
3rd party



Necessity

The desired data must not be available via other sources

Balancing Test

Must show that the interests of both the data subject and the controller/3rd party have been carefully considered and that technical and organisational safeguards (like **pseudonymisation**, which is specifically mentioned) are put into place to balance the interests of the parties

Dynamic Data Governance for Analysis

Lawful Basis

Stage 1: Data Collection

- Must have lawful basis to collect data for analysis purposes **at the time of data collection**
- Legal Basis: **Legitimate Interest**

Stage 2: Data Analytics

- Must have lawful basis for processing analytics **at the time analysis is performed following data collection**
- Legal Basis: **Legitimate Interest**

Stage 3: Data Subject Impact

- Must have lawful basis **at the time when consequences from analysis are attached to data subjects**
- Legal Basis: **Legitimate Interest** or **Consent**

Data-Driven Analysis

The Purpose Limitation Principle:

1) Data must be collected for specified, explicit and legitimate purposes only ('purpose specification'); and
2) Data must not be further processed in a way that is incompatible with those purposes ('compatible re-use').

The purpose of data-driven general analysis can be specified (but need not be "specific"). However, it does require a description of the scope and consequences of the data analytics processes.

Repurposing personal data is deemed compatible with initial processing when it is carried out for the following purposes:

- Scientific research (Art.89 GDPR)

or

- Archiving in the public interest

or

- Statistical purposes

Dynamic Data Governance for Analysis
Impact Assessments

Stage 1: Data Collection

Stage 2: Data Analytics

- First impact assessment focused on data quality (source of data, accuracy of data), data minimisation (e.g., pseudonymisation) and data security (access restriction, encryption when data is transferred)

Stage 3: Data Subject Impact

- Second impact assessment focused on consequences to data subjects following analysis

The Future of Analysis:

Privacy respectful design solutions (**Data Protection by Design and Default, especially Dynamic Pseudonymisation**) can be **embedded into** operations.

The help ensure that **Purpose Limitation** and **Data Minimisation** are enforced as interdependent principles under Article 5 and 6 GDPR (its Fair & Lawful processing requirements)

Summary: Creating Trust and Transparency

- Data controllers can engage in GDPR compliant analytics via its enabling functions
- Legitimate Interest is the most likely legal basis for data collection and data analysis
- ‘By Design’ Dynamic Pseudonymisation proactively facilitates data innovation and helps ensure purpose preservation over time
- Consent should be reserved for those situations where it can be truly meaningful: empowering users to be in control
- The ‘key’ to GDPR compliance is robust data governance structures that control the way data is managed within and between organisations, and ensure data subjects’ reasonable expectations are managed and respected

Sophie Stalla-Bourdillon, and Alison Knight. “Data analytics and the GDPR: friends or foes? A plea for a dynamic and holistic approach to data protection law” (2018)

Alison Knight (PhD)
Senior Legal Adviser, University of Southampton

a.knight@soton.ac.uk