# Data & Decisions

DPA, GDPR & personal data

Dr Peggy Gregory

# History of data protection law

- Data Protection Act (DPA) first passed in 1984 to protect personal data (PD) in paper-based filing systems and on computers
- DPA updated in 1998 in response to new EU law and advances in tech. More detailed, concerned with way PD were processed
- In 2002, DPA was supplemented with Privacy & Electronic Communications Regulations 2003, which focused on email marketing and website consent for cookies – known as cookie law
- In May 2018 EU enacted General Data Protection Regulation (GDPR) strengthening DP law across Europe. UK enacted DPA 2018 which is a UK supplement to GDPR
- UK left EU in 2020, kept GDPR with small changes enacted as UK GDPR. i.e. age of child consent 13 in UK, 16 in EU, changes to how PD about criminals handled, and how PD is used for automated decision making.
- Organisations have to comply with UK GDPR and DPA if working in UK, if they process data of EU residents they must comply with EU GDPR.

# UK data protection law

- **Data protection (DP)** legislation sets out rules for the handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects') by organisations ('data controllers')
- Applies to organisations in public and private sectors. It applies to electronic and most paper records. It doesn't apply to anonymous information or to information about the deceased
- Since 1 January 2021, the principal legislation has been:
  - The UK General Data Protection Regulation (the UK GDPR)
  - The Data Protection Act 2018 (DPA 2018) which supplements the UK GDPR

# Personal data

- *Information that relates to an identified or identifiable living individual*
- This means anything about a person: name, address, phone no., email address, bank account no, NI no, student id, library card
- Also, it's personal if it can be used to identify a person when pieced together with other data, i.e. IP address or username for website, data confirming physical presence somewhere, fingerprints, CCTV footage or GPS location

# Identifying individuals

- If you cannot directly identify an individual from that information, then you still need to consider whether the individual is identifiable.
- When considering whether information ‘relates to’ an individual, you need to take into account a range of factors, including the content, the purpose for which you are processing it and the likely impact or effect of that processing on the individual.
- Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.
- Information which is truly anonymous is not covered by the GDPR.
- If information that seems to relate to a particular individual is inaccurate it is still personal data, as it relates to that individual.

# Sensitive personal data

- Stronger protections for type of data that might used to discriminate about people sensitive personal data or special category data
- Need explicit permission OR a very good reason (protect public health)
  - Race
  - Ethnic background
  - Sexual orientation & sex life
  - Religious beliefs
  - Political opinions
  - Trade Union membership
  - Health data med history, including data by fitness apps
  - Biometric data if used for ID – face recognition iris and retina scans, ears etc
  - Genetic information

# 7 Data Protection principles

1. **Processed lawfully fairly and transparently** - only if 'legal basis', i.e. consent, contract, legal obligation, vital interests (i.e. GP), public interest (only public orgs), legitimate reason
2. **Processed only for specified, explicit and legitimate purposes** – tell people what will do, even if sharing or selling data with others
3. **Adequate, relevant and limited to only what is necessary** – minimum amount of data
4. **Accurate and, where necessary, kept up-to-date**
5. **Not kept for longer than necessary** – DC must establish time limits for keeping PD
6. **Must be kept securely – preserving confidentiality, integrity and availability** – this means keeping PD encrypted if stored. Employees also need to know this
7. **Data controllers must be accountable** – must keep detailed records as evidence of policies being followed Third parties must also follow principles

Full/partial exemptions in specific contexts i.e. for academic research, policing etc.

# Data Controllers

- The UK GDPR defines a **data controller (DC)** as:

***"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"***

- Controllers make decisions about processing activities
- They control the PD being processed and are responsible for it
- Can be a company or other legal entity (i.e. public authority), or an individual (i.e. sole trade, self-employed professional).
- Individuals processing PD for household activity NOT subject to DP law

# Data Processors

- The UK GDPR defines a **processor** as:

***"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"***

- **Act on behalf of a DC** and under the DC's authority. They serve the controller's interests not their own
- May make day-to-day decisions but should only process personal data in line with controller instructions
- If they act without the DC's instructions, they become a controller for that activity and have the same liability as a DC

# Information Commissioner's Office (ICO)

https://ico.org.uk/

- ICO is the UK's independent regulator for data protection and freedom of information. Their role is to:
- Uphold the UK GDPR and DPA 2018
- Uphold the Freedom of Information Act 2000
- Uphold information rights of individuals and organisations
- Monitor and investigate breaches
- Take enforcement action
- Promote good practice
- Support organisations

# Data Access Rights of Individuals

- To be **informed** of how personal data are being used – **'privacy notices'**
- Of **access** to their personal data - known as making a **'subject access request'**
- To **rectification** of inaccurate personal data
- To **erasure** of personal data where appropriate - **right to be forgotten**
- To **restrict processing** of personal data pending its verification or correction.
- To **data portability** - to receive copies of their personal data in a machine-readable format
- To **not be subject to automated decision making** – profiling, direct marketing, for research (if not in public interest).
- To **object** to the way their personal data is being used

Response to a rights request normally should be sent within one month, but nearly all rights are qualified in various ways and there are exemptions

# Privacy notices

- An important aspect of complying with data protection law legislation is being **open and transparent** with individuals about how their personal data will be used.
- The supply of this information - through documents variously known as **'privacy notices', 'data protection statements', 'data collection notices', 'privacy policies'** is essential
- It takes places in numerous targeted ways depending on the context of the interaction with the individual
- It is the responsibility of the **Data Controller** to provide notices

# Subject Access Requests

- Right of access to a **copy of personal data** being held by a DC
- Ask in writing or
- Provide in a month, free of charge
- Easy to access and easy to understand.
- If complex can take up to 3 months and they may charge a small processing fee, but they must respond to the request within a month and explain why it will take time

# Data Portability

Individuals have rights:

- To receive a copy of your personal data in **a structured, commonly-used computer-readable format** so you can pass it on
- To ask a data controller to transmit your PD directly to another data controller – that means provide electronic data in an open format CSV, XML, JSON
- Only includes raw data that you gave, name and address etc, internet search history. DCs are NOT obliged to pass on data that they've inferred from your data, i.e. your likes and dislikes based on their activities

# Automated decision-making or profiling

- Automated decision-making is increasingly common
- Right not to be subject to a decision made by **purely** automated means
- Only allowed to do so with explicit consent, or authorised by law
- If using sensitive data MUST have explicit consent or for public interest
- **Good practice** for DC to tell you details of any profiling or automated decision-making they do, including where data comes from
- DC MUST explain how you can access data used to create your profile and simple ways to request human intervention or to challenge an automated decision

# Data security breaches & penalties

- Any DC who falls foul of DP rules will be held to account
- **Breaches** leading to disclosure, loss, destruction or alteration of PD that present a serious risk to anyone's rights and freedoms
  - Reported to ICO within 72 hours
  - The data subject involved will be notified as soon as possible
- Actions by ICO on organisations that fail to comply
  - Warning, temporary or permanent ban on data processing
  - If very serious: Fine up to 17.5%M or 4% of annual turnover in UK
  - i.e. In 2019 British Airways fined £183M hackers gained access to customers details including bank details

# DPA recent relevant cases

- **ICO v Clearview AI Inc** [2025] UKUT 319 (AAC) – CAI scraped public images from the internet, created a huge facial-recognition db, and offered its service (inc. to law enforcement). ICO **does have jurisdiction** over a US company under UK GDPR/DPA, & 'behavioural monitoring' is interpreted broadly (inc. passive collection, profiling)
- **ICO imposed a £14 million fine on Capita** for failures following a 2023 cyber-attack of highly sensitive personal data from ~6.6 million records. Key failures: privilege escalation allowed, lack of proper technical or organisational measures, and a very slow response to security alerts.
- **Jason Blake, director of Bridlington Lodge Care Home** was found guilty of obstructing a valid data subject access request for notes relating to the plaintiff's father – criminal charge upheld, fined.

# Data Use and Access Act 2025

- Modernises DPA/GDPR, reducing admin & enabling secure data sharing
- Govt can regulate access to business data – mandate ‘smart sharing’
- Digital Verification – framework for ‘trusted digital identity’ & certified providers, to prove identity without providing physical documents
- Expands automated decision-making – but still with safeguards
- Recognised legitimate interests – new lawful ground for processing
- Simplifies rules for transferring PD internationally
- Requires orgs to have a complaint handling system for PD
- Permits storage & access tech (cookies) without consent – low-risk sits
- Restructures ICO
- Strengthens enforcement powers with audits, inspections & higher fines