Data Protection: What you need to know

Tim Turner November 2017

What is Personal Data?

- Data about or relating to living, identified or identifiable individuals
- * CONCRETE: Name & Address, ID codes
- * SUBJECTIVE: behaviour, choices
- * SPECIAL: health, religion
- * Held anywhere at home, at synagogue
- * Even data online is personal data

What is Data Protection for?

- * Justify the use of personal data
- * Keep it safe and accessible only to those who need it
- * Limit the amount you hold, and keep it accurate,
- * Give it only to those who need it
- * Get rid of it when you don't need it
- Respect people's data like you would respect them

The role of the manager

- * Data quality is data accurate, adequate and professional?
- * Information handling
 - * Is access to data limited to those who need to see it?
 - * Is the process for sharing data with others properly managed?
- * Security of premises, equipment and records
 - * Where is your data? In the building, on a laptop, in someone's home?
 - * How do you dispose of equipment and data?

GDPR does not apply to:

Organisations that are investigating, detecting, preventing crime or criminal justice purposes

Use of data by individual for purely personal or household activities

Personal data of deceased persons

Synagogue = 'Data Controller'

Anyone who uses data on our behalf = 'data processor'

Individuals are NOT personally liable

Fines possible – BUT ICO's LAST RESORT

A5: Principles

a)
Lawfulness,
fairness and
transparency

b) Purpose limitation

c) Data minimisation

d) Accuracy

e) Purpose limitation f) Integrity and confidentiality

Controller is responsible for and shall be able to demonstrate compliance

JUSTIFYING DATA USE

Recording information

- * Accuracy do you ask right questions, and do forms / processes gather the right information?
- * Is data especially warnings clear, objective and helpful?
- * Is the tone professional?
- * Print only what you need
- * Do you have a clear retention policy for all of your data?

Article 6: Conditions

Consent

Necessary for contract

Legal obligation

Vital interests

Official authority / public interest

Legitimate interest

Article 9: Special categories

Racial / ethnic origin

Political opinions

Religious / philosophical beliefs

Trade union

Biometric & genetic data

Health

Sex life / sexual orientation

Article 9: Special categories conditions

Explicit consent

Employment law

Vital interests no consent

Special category group use

Made public by subject

Public interest underpinned by law

Establish / defend legal claims

Health / social care

Public health

Archiving / research with safeguards

RIGHTS

Rights rules

One month to respond (+ up to 2 more months if complex)

Requests generally free (limited ability to charge for unfounded / excessive requests)

Can check identity

What people need to know (even if you get their data from somewhere

WHO YOU ARE Contact of Data Protection Officer Why you process data and justification for doing so

Who will receive data

Transfers outside of Europe

How long data is kept for

Rights

Right to withdraw consent

Right to complain to ICO

Consequences of failure to supply data

Existence of profiling and other automated decision making

Where data came from

Rights

15

- Subject access
- Right to personal data and other contextual information (purposes, recipients, sources)

17

- Right to be forgotten
- Erasure of data where no longer required, consent withdrawn, successful objection

Rights

16

- Rectification
- Can add statement

18

- Restriction
- Quarantine on disputed data

20

- Portability
- Machine readable version of data provided by subject

Rights

21

- Objection to conditions
- Official authority, legit interest

22

- Objection to method
- Automated processing and profiling (some exemptions)

Some big requirements

Art 32 + 33: Security and breach notification

A35: Impact assessments

A37: Data Protection Officer

Data Protection Risks

Losing track of where data is stored

No clear justification for using data

Inaccurate data

Keeping data for too long

Working from home

Using data when on the move

Badly expressed data

Contractors

Big GDPR issues

Children

Pseudonymisation

Anonymisation

Profiling

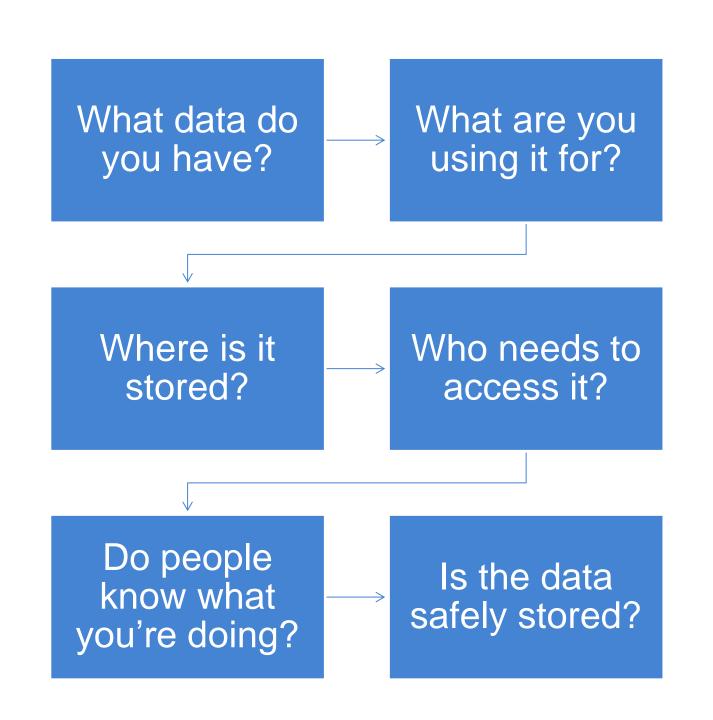
Automated decisions

Power imbalances

Data sharing

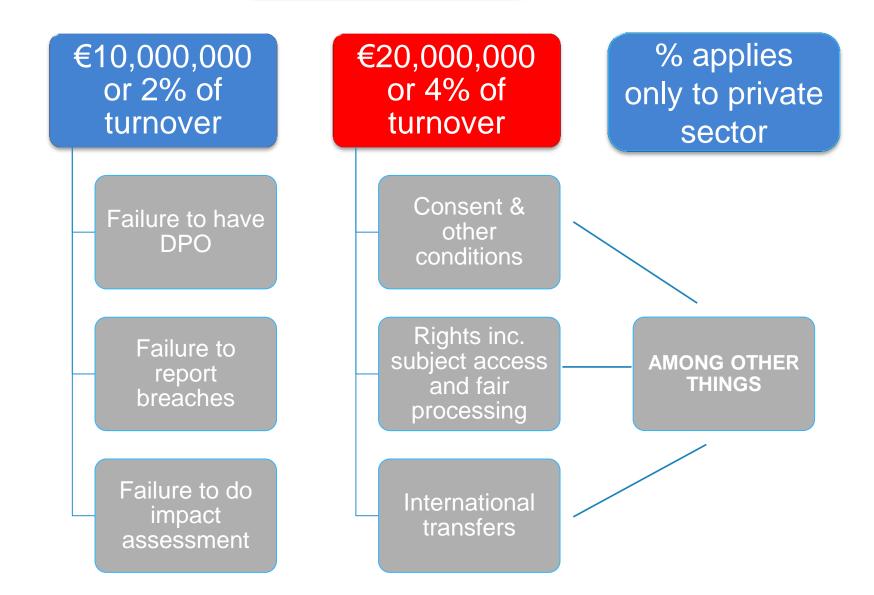
- * Why are you sharing?
- * Is there a clear justification e.g. consent, tenancy agreement, crime investigation, legal proceedings
- * Have you checked who you are sharing with?
- * Is this one-off sharing or do you need a data sharing agreement?

WHAT DO WE DO NOW?



FINES

Article 83



How fines work

- * The headline figures are for the biggest fines, against the biggest organisations
- * Small organisations very unlikely to be fined
- * Important to have control over your data, and make decisions about who uses it

What is a breach?

- * The breach is not the incident it is symptom that reveals a problem
- * Breach could be:
 - * No policies and procedures
 - * Inadequate or unclear policies and procedures
 - * Poorly communicated policies and procedures
 - * Staff who are not trained
 - Policies that are not enforced
 - * Lack of audit or management checks

How could you handle personal data better?

Office security?

Access to data?

Staff training?

Data quality?

Social media

Social Media

- * Control access to any organisational account
- * Train staff who use it to interact carefully and sensitively with the public

* ALSO: warn staff not to mention service users / colleagues on social media outside work

What to do now

- 1. Don't panic!
- 2. Find out what data you have, and where it is
- Weed out records, files and data that is irrelevant / out of data
- 4. Write a clear, straightforward privacy notice for your members
- 5. Make sure that data, records and equipment are safe
- 6. Write a simple process for rights and complaints

Contact 2040 for advice and training

www.2040training.co.uk

Email: tim@2040training.co.uk

