Data Protection 2018

Susi Calder
www.susify.com

Disclaimer!

- I am NOT a lawyer!
- This presentation is not legal advice
- This presentation is intended to give practical guidance
- Not suitable for statutory services (local government, parish & town councils etc.)
- Do not have time to cover everything!

What's all the fuss?

- GDPR coming into force 25th May 2018
  - EU legislation
  - Hefty fines for breaches
- New Data Protection Bill – repealing DPA 1998

New Data Protection Bill

From UK Government Factsheet:

- Implement the GDPR standards across all general data processing.
- Provide clarity on the definitions used in the GDPR in the UK context.
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained.
- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Set the age from which parental consent is not needed to process data online at age 13.

Still going through Parliament

GDPR – what is it?

- General Data Protection Regulations
- Strengthen and unify data protection for all individuals within the EU
- Addresses the export of personal data outside the EU
- Better reflect data processing that is carried out in an increasingly digital world
- Requires you to be more transparent
- Provides individuals with more rights

Who does it apply to?

- ‘controllers’ **and** ‘processors’.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.

What information does it apply to?

- Personal data
  - any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier
  - pseudonymised data, depending on how difficult it is to attribute the pseudonym to a particular individual.
- Sensitive data
  - ‘special categories of personal data’

Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

Key Measures

- Lawful processing
  - Necessary
  - Determine before processing
  - Include in privacy notice
  - Changing purposes
  - Special category data & criminal convictions
  - Affects which rights are available to individuals.

Key Measures

- Individual rights
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erase
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling.

Right to be informed	Individuals should be informed of how their data is collected, stored and processed in a clear, accessible way	You should provide this in your Privacy Statements and by request
Right of access	Individuals can request access to a copy of their data in electronic form and details of how it is processed	You must provide this, for free, within one month
Right to rectification	Individuals are entitled to have their data corrected if it is inaccurate or incomplete	You should do this within one month, two if it is a particularly complex task
Right to erasure	Also known as 'the right to be forgotten', this permits individuals to request the deletion of their data	You must do this within one month, unless you have a strong, valid reason
Right to restrict processing	Individuals can request a halt on processing if they object to accuracy or purpose but you can still hold the data until resolved	This should be an immediate, and often temporary, stop
Right to data portability	Individuals can request their data in a suitable digital format, sent either directly to them or to a third party	You should do this within one month, two if it is a particularly complex task
Right to object	Individuals can, in certain cases, object to the processing of their data, eg. in direct marketing	You should provide reasonable means to object and act on this within one month
Rights in relation to automated decision making	Individuals can object to potentially damaging decisions being taken against them based only on automated data processing	You should allow the individual to challenge and request human intervention

Key Measures

- Accountability and Governance
  - implement appropriate technical and organisational measures (e.g. internal data protection policies, staff training, internal audits of processing activities, and reviews of internal HR policies)
  - implement measures that meet the principles of data protection by design and default
  - where appropriate, appoint a data protection officer;
  - maintain relevant documentation on processing activities
  - use data protection impact assessments where appropriate

Key Measures

- Personal data breaches
  - Robust procedures to help with decision-making
  - Report to ICO within 72 hours of being aware of breach
  - Inform individuals at high risk of being adversely affected
  - Keep records of ALL breaches, including justification of decision not to notify

Key Measures

- Consent
  - Explict (no opt-outs!)
  - Specific
  - Time limited
  - Can use Notice where mandatory for service provision
  - Special arrangements for children

Enforcement

- ICO is Supervisory Authority in UK
  - Report breaches to
  - Receive complaints from individuals
- Hefty fines
  - Greater of 4% of annual turnover or €20 million for breaches relating to data protection principles
  - Greater of 2% of annual turnover or € 10 million for breaches relating to internal record keeping

What should YOU do?

Prepare for GDPR!

- ICO checklist
- Audit your data!
  - What data do you hold? Personal? Sensitive?
  - Where and how do you hold it?
  - Who holds it?
  - How accurate is it? How many copies?
  - Why do you hold it? Lawful purpose!

Prepare for GDPR

- Privacy notices and consents
- Subject access requests
- Data breaches
- Data Protection by Design and Default

Further reading/advice

- www.ico.org.uk
- https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/
- https://gdpr-info.eu/