Data Protection

1 Data Protection Overview

What kind of data?

- Data relating to an *identified* or *identifiable* **living** individual should not be collected without:
  - an explicit *purpose*
  - a *lawful basis* for collecting and using the data.

- There are two strands of data protection and privacy regulation in the Western world:
  - the US approach (self-regulation and market forces)
  - the European approach (government regulation and strict laws)

2 Data Protection Act 2018 (UK) www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

- A way for individuals to control their personal information
- Protects individuals from:
  - use of personal information:
    - by unauthorized persons
    - for purposes other than those identified when it was collected
    - for a longer period than needed
  - inaccurate personal information
  - irrelevant personal information
    - i.e. individuals have the right to have incorrect / irrelevant information corrected / deleted (e.g. Google case)

- Information Commissioner's Office (ico.org.uk)
  - regulates compliance with the Data Protection Act

3 GDPR Terminology (EU)

- European Union (EU) General Data Protection Regulation (GDPR)
  - Common European minimum standards that were agreed in 2016 and came into force 25th May 2018
  - Applies to organisations, not to personal use
- Data
  - Information that is
    - being processed automatically, or
    - is collected to be processed automatically, or
    - is recorded as part of a relevant filing systems.
- Personal data
  - Information that is or can be linked directly to an individual
    - Name, address, etc.
  - ID codes that can be linked to an individual
    - National Insurance Number
  - Must "relate to" the individual

4 GDPR

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- Infringements of the basic principles for processing personal data could mean a fine of up to 20 million euros, or 4% of your total worldwide annual turnover, whichever is higher.

5 GDPR Terminology (EU)

- Data controller
  - The individual / authority who determines the purposes and means of the processing of personal data
  - May need to pay an annual fee to the Information Commissioner's Office, depending on the type of processing
- Data processor
  - Anyone who obtains, records, stores, organises, transforms, transports, discloses, deletes, combines etc. data on behalf of the data controller
- Data subject
  - An individual identified or identifiable by personal information

What's new: www.youtube.com/watch?v=7mMnDsp7Weg

6 GDPR

- Member states must:
  - create legislation to ensure:
    - use limitation
    - purpose specification
  - set up a supervisory authority that will:
    - monitor the data protection level in the country
    - give advice to the government
    - start legal proceedings when regulation is violated
- Data Protection Act 2018 (updated from 1984, 1998) (UK)
  - Information Commissioner's Office (ico.org.uk)
  - Data controllers' and processors' responsibility
  - 7 data protection principles
    a. Lawfulness, fairness and transparency
    b. Purpose limitation
    c. Data minimisation
    d. Accuracy
    e. Storage limitation
    f. Integrity and confidentiality (security)
    g. Accountability

7 GDPR

Certain types of data have extra protections:

- Criminal offence data
- Special category data e.g. information about an individual's
  - race
  - ethnic origin
  - politics
  - religion
  - trade union membership
  - genetics
  - biometrics (where used for ID purposes)
  - health
  - sex life
  - sexual orientation

8 Principle (a): Lawfulness, Fairness and Transparency

- You must have a valid reason (a *lawful basis*) to collect and process personal data
- You must not do anything with the data that is illegal
- You must use personal data in a way that is *fair* i.e. you must not use data in a way that is
  - detrimental in an unjustified way
  - unexpected or
  - misleading to the individual concerned.
- You must be clear, open and honest with people from the start about how you will use their data

9 Lawful Basis

- There are six lawful bases for collecting and processing personal data:
  - **Consent:** individual has given clear consent for you to process their data for a specific purpose (must be opt-in; can withdraw their consent at any time)
  - **Contract:** necessary to carry out a contract or if they have asked you to take steps before entering into a contract
  - **Legal obligation:** so you can comply with the law
  - **Vital interests:** protecting someone's life (could be a third party, only applies if consent cannot be given)
  - **Public task:** to perform a task in the public interest that has a basis in law
  - **Legitimate interests:** necessary for your legitimate interests or those of a third party, unless there is a good reason to protect the individual's interests that overrides these legitimate interests
- You need to determine which is most appropriate
- It may be difficult to switch to a different one later

10 Principle (b): Purpose Limitation

- You must be clear from the start about *why* you are collecting personal data and *what* you intend to do with it.
- You need to document your purposes and include them in your privacy information for individuals
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law

11 Principles (c)-(e)

c Data Minimization

- You must ensure the personal data you are processing is:
  - adequate - sufficient to properly fulfil your stated purpose;
  - relevant - has a rational link to that purpose; and
  - limited to what is necessary - you do not hold more than you need for that purpose.

d Accuracy

- You must take reasonable steps to ensure that personal data you hold is correct, up-to-date and not misleading

e Storage Limitation

- data shall *not* be kept longer than necessary
- you must have a policy setting standard retention periods if possible
- you should periodically review data you hold and erase or anonymise it when you no longer need it
- exceptions apply if you are keeping the data for
  - archiving in the public interest
  - scientific or historical research, or
  - statistical purposes

12 Principle (f): Integrity and Confidentiality

- Appropriate technical / organisational measures must be taken against unauthorised / unlawful processing and against accidental loss / damage / destruction of personal data
- In particular, you will need to:
  - manage your *security* to fit the nature of the personal data you hold and the harm that may result from a security breach
  - be clear about *who* in your organisation is responsible for ensuring *information security*
  - make sure you have the right physical / technical security, backed up by robust policies / procedures

13 Principle (g): Accountability

- You are responsible for complying with the GDPR and you must be able to demonstrate you compliance
- There are a number of measures that you can, and in some cases must, take including:
  - adopting and implementing data protection policies
  - taking a 'data protection by design and default' approach
  - putting written contracts in place with organisations that process personal data on your behalf
  - maintaining documentation of your processing activities
  - implementing appropriate security measures
  - recording and, where necessary, reporting personal data breaches
  - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
  - appointing a Data Protection Officer and
  - adhering to relevant codes of conduct and signing up to certification schemes.
- You must review and, where necessary, update the measures you put in place.

14 Data protection - Not an Impediment to Life

In the autumn of 2003 a UK utility company stopped the supply of gas to an elderly couple's homes for non-payment of £140 — they died

"Data Act 'not to blame' for deaths" (http://news.bbc.co.uk/1/hi/england/london/3342977.stm)

The Information Commissioner's Office made it plain that in their view the protection of personal information such as unpaid bills could not be seen as overriding the protection of life offered by the social services.

15 Rights

The GDPR provides the following rights to individuals:

1. The right to be informed (about collection and use of their data)
2. The right of access (a copy of their data)
3. The right to rectification (correct inaccurate data and complete incomplete data)
4. The right to erasure (to have personal data deleted, also known as "the right to be forgotten")
5. The right to restrict processing (e.g. while considering a correction to their data)
6. The right to object
    - In particular, individuals have an absolute right to stop their data being used for direct marketing
7. Rights in relation to automated decision making and profiling
8. The right to data portability (move, copy or transfer personal data from one IT environment to another)
    - only applies in certain circumstances e.g. if the lawful basis is consent or in performance of a contract and the processing is carried out by automated means
    - must be provided in a format that is
        - structured,
        - commonly used and
        - machine-readable (e.g. CSV, JSON, XML).

Requests to access, rectify, erase, restrict or object must be:

- replied to within 1 calendar month
- for free
- may be denied in certain circumstances

16 Data Breaches

- Breaches must be reported to the ICO within 72 hours if there is risk to a person's rights or freedoms
- All breaches should be documented regardless of whether they are reported
- Individuals must be informed of breaches without undue delay

17 International Transfers

- The GDPR primarily applies to controllers and processors located in the European Economic Area (the EEA)
- Personal data can not be transferred to a country outside of the European Economic Area (EEA), unless that country ensures an adequate level of protection for the rights / freedoms of data subjects in relation to the processing of personal data.
- Before making a transfer:
  - consider whether you can achieve your aims without actually processing personal data
  - Example: if data is made anonymous, so that it is not possible to identify individuals from it (now or at any point in the future), then the data protection principles will not apply and you are free to transfer the information outside the EEA.

What will happen after brexit?

18 Scenario

You have set up an online business and hold personal details of your customers in a database. You use the data to email your customers regarding forthcoming offers. An unauthorised person accesses the database and alters product prices and some customers' details.

Discuss how the UK Data Protection Act 2018 relates to this scenario.

19 Scenario (Possible points to consider)

- You should collect the data in a fair, lawful and transparent manner
- The data subjects (customers) should give you their consent to processing the data
- Make it clear to them how you are collecting their information
- Make it clear why you are collecting their information
- Offer them the chance to request the removal of their details
- Offer an opt-in tick box for them to confirm their consent to use their data
- Take appropriate security precautions
- Do not transfer the data unless customers gave you the permission to do so
- Can you share the data with anyone and anywhere in the world?

20 You Should be Able To:

- Identify a source that will help you gain an understanding of the UK's data protection policy (Acts 1984, 1998, 2018)
- Write at least 5 key points about the Data Protection Act 2018
  - 3 fairly general - could include the influence of Europe
  - 2 very detailed - perhaps further investigation into two of the Data protection principles
  - Write out examples of the principles that make sense to you
- Compare the UK to another country's data protection policy or legislation.