COM6655 Professional Issues

Autumn 2022-23

Data protection, privacy and freedom of information (part 2)

Dr Maria-Cruz Villa-Uriol
Department of Computer Science, University of Sheffield
m.villa-uriol@sheffield.ac.uk

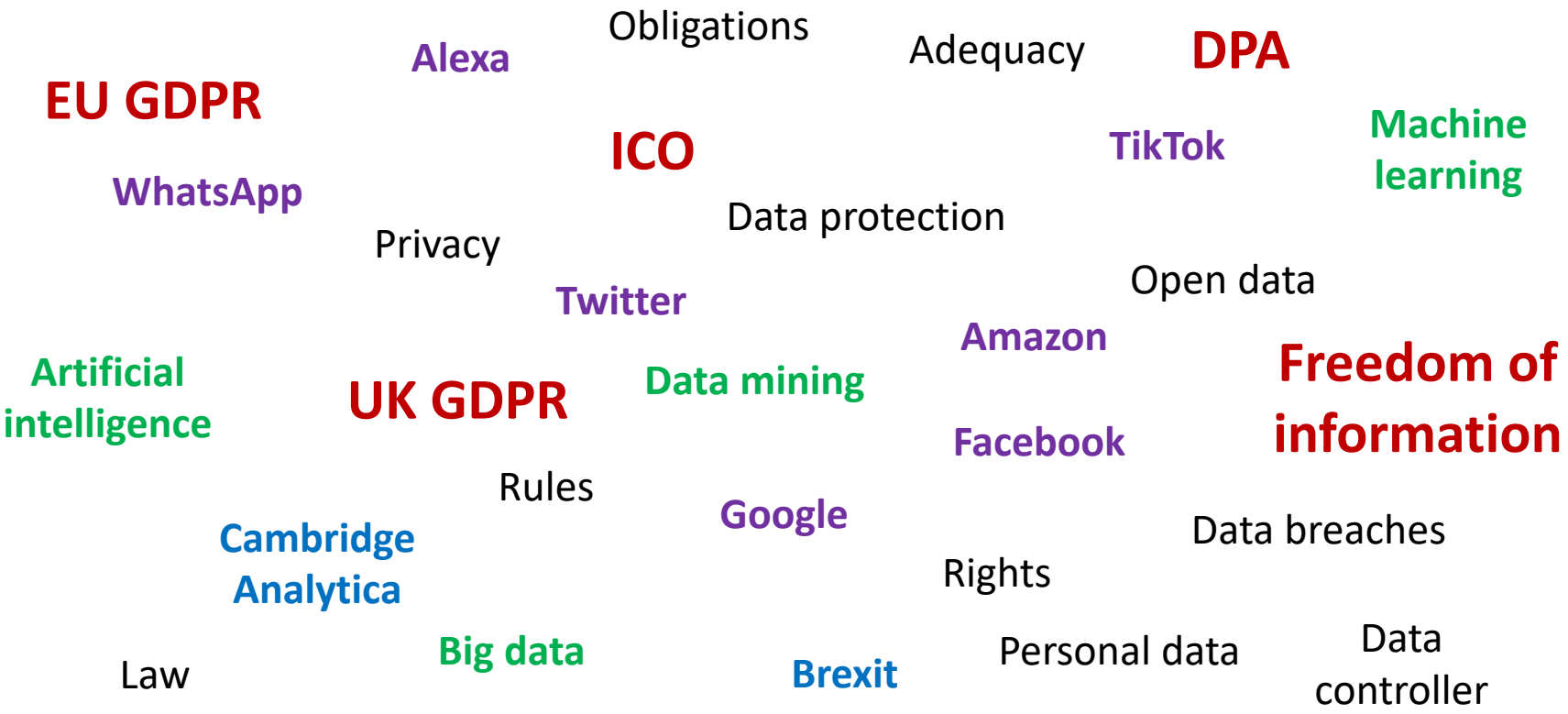
Overview

- Privacy in the computer age
- Three aspects of privacy
- DPA 2018 (Data Protection Act)
- EU GDPR (EU General Data Protection Regulation)
- UK GDPR (UK General Data Protection Regulation)
- Information Commissioner’s Office - ICO
- Investigatory powers
- Summary

DPA 2018 and UK GDPR

- Q. Have you heard of these?
- Q. Which terms come to mind associated to these?

DPA 2018 and UK GDPR



UK Data Protection Act (2018)

- Sets out the framework for data protection law in the UK
- Amended on 1st January 2021 to reflect the UK's status outside the EU
- Three data protection regimes:
  - General processing regime (the UK GDPR) [Part 2 of DPA 2018]
  - Regime for law enforcement authorities [Part 3 of DPA 2018]
  - Regime for intelligence services (e.g. national security and defence) [Part 4 of DPA 2018]
- Which regime to apply? →
  Most organisations fall under the general processing regime, hence UK GDPR will apply.
- Sets out the Information Commissioner's Office (ICO) functions and powers
- Updates the previous DPA (1998) to adapt to our data-centric era

A preamble to UK GDPR - EU GDPR

- EU GDPR – the EU “General Data Protection Regulation”
- Europe’s latest data protection regulation, adopted by European Parliament and European Council in April 2016
- Came into force May 18th 2018, and applies across Europe, but each country can make its own small changes

A preamble to UK GDPR - EU GDPR

- EU GDPR – the EU “General Data Protection Regulation”
- Europe’s latest data protection regulation, adopted by European Parliament and European Council in April 2016
- Came into force May 18th 2018, and applies across Europe, but each country can make its own small changes
- Until 31st December 2020, EU GDPR applied in the UK (frozen GDPR)

UK GDPR

- UK GDPR stands for "UK General Data Protection Regulation" and came into effect as a law after the Brexit transition period (from 1st January 2021):
  - It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.
  - The UK GDPR is based on the EU GDPR
  - The key principles, rights and obligations remain the same
  - The UK has now the independence to keep the framework under review*
  - The UK has become a third country to the EU
  - The rules on transfers of personal data and cross-border processing between the UK and the European Economic Area (EEA) are affected

* Updates are to be officially published in https://www.legislation.gov.uk/

Data transfers outside the UK

- UK GDPR applies to controllers and processors in the UK, with some exceptions
- Individuals risk losing the protection provided by the UK GDPR if their personal data is transferred outside the UK
- UK GPDR restricts transfers of personal data outside the UK, or the protection of the UK GPDR, unless the rights of the individuals in respect of their personal data is protected in another way
- A transfer of personal data outside the protection of the UK GDPR is referred as ‘restricted transfer’

UK GDPR and EU GDPR

- The rules on transfers of personal data and cross-border processing between the UK and the European Economic Area (EEA) are affected.
- If operating in Europe, offering goods or services to individuals in Europe, or monitoring the behaviour of individuals in Europe, you may need to comply with both the UK GDPR and the EU GDPR.
- UK GDPR applies to controllers and processors based outside the UK if their activities relate to offering goods or services to individuals in the UK, or monitoring the behaviour of individuals taking place in the UK
- EU GDPR applies to the processing of UK controllers with an establishment in the EEA, with customers in the EEA, or monitoring individuals in the EEA.
- How UK controllers interact with EU data protection authorities has changed → Adequacy decisions

*https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

** Legacy data holders of overseas data (i.e. collected before 1st Jan 2021) will be subject to the EU GDPR as it stood on 31 December 2020 ('frozen GDPR'). In the short term, significant changes between the frozen GDPR and the UK GDPR are highly unlikely

Data protection and the EU

- For UK businesses or organisation with an established presence in the EEA, or with customers in the EEA
  - On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED).
  - In the majority of circumstances, most data from EU/EEA can continue to flow to the UK as it did before, without the need for additional safeguards.
  - Adequacy decisions do not cover data transferred to the UK for the purposes of immigration control, or where the UK immigration exception applies. For that data, different rules apply and the EEA sender needs to put in place other safeguards.

In a map…

UK GDPR key principles

UK GDPR

Article 5(1) requires that personal data shall be:

> "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Seven key principles

- The UK GDPR sets out seven key principles:
  1. Lawfulness, fairness and transparency
  2. Purpose limitation
  3. Data minimisation
  4. Accuracy
  5. Storage limitation
  6. Integrity and confidentiality (security)
  7. Accountability

1. Lawfulness, fairness and transparency

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- This means that you must:
  - Identify valid grounds under the UK GDPR (known as a ‘lawful basis’) for collecting and using personal data.
  - Ensure that you do not do anything with the data in breach of any other laws.
  - Use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
  - Be clear, open and honest with people from the start about how you will use their personal data.

2. Purpose limitation

- Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’)
  - You must be clear about what your purposes for processing are from the start.
  - You need to record your purposes as part of your documentation obligations and specify 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.

3. Data minimisation

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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
  - limited to what is necessary – you do not hold more than you need for that purpose.
- **Q: You are testing a system and ask testers to complete a consent form that asks for their *date of birth*. Is that excessive?**

4. Accuracy

- Personal data shall be: accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
  - You may need to keep the personal data updated, although this will depend on what you are using it for.
  - If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
  - You must carefully consider any challenges to the accuracy of personal data.

5. Storage limitation

- Personal data shall be kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed;
- Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes … subject to **implementation of the appropriate technical and organisational measures** required by the GDPR in order to safeguard the rights and freedoms of individuals

5. Storage limitation (continued)

- Practically, this means that:
  - You must not keep personal data for longer than you need it.
  - You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
  - You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
  - You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
  - You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
  - You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.
- When applying for ethical approval you need to say where and for how long you will keep data, and when it will be destroyed.
- **Q. In a scientific study, when does it become impossible for participants to withdraw consent?**

6. Integrity and confidentiality

- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- This means that:
  - You must ensure that you have appropriate security measures in place to protect the personal data you hold.
  - This 'integrity and confidentiality' principle of the UK GDPR is also known as the security principle.

6. Integrity and confidentiality (continued)

- Security is key to avoid fraud (e.g. identity theft)
- Establishing the 'appropriate' level of security depends on the risks presented by your processing, and in relation to the nature, scope, context and purpose of the processing, and on the state of the art and cost of implementation.
- Every aspect of the processing of personal data needs to be covered, not only cybersecurity. Security measures need to ensure that:
  - the data can be accessed, altered, disclosed or deleted only by those with the right authorisation;
  - the data you hold is accurate and complete in relation to why you are processing it;
  - the data remains accessible and usable. For example, in case of accidental loss, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.
- The above will likely require the implementation of organisational and technical measures
- When choosing a data processor, the controller needs to ensure that they comply

7. Accountability

- The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.
- You must have appropriate measures and records in place to be able to demonstrate your compliance. This might involve/require:
  - ‘Data protection by design and default’ approach
  - Documentation is essential at all levels and includes recording and keeping track of consents, contracts…
  - Security is paramount, requiring among others: information security policies, access controls, security monitoring and recovery plans
  - Data breaches need to be detected, reported, investigated and documented.

Why do the principles matter?

- These principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation, and inform everything that follows.
- **They don't give hard and fast rules,** but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.
- Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the UK GPDR.
- **Failure** to comply with the principles may leave you open to **substantial fines.** Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of **up to €20 million**, or 4% of your total worldwide annual turnover, **whichever is higher**.