Software and Apps Data Protection Module

Course Notes

Applicable Legislation in UK

1. UK GDPR – retained version of the EU General Data Protection Regulation 2016
2. Data Protection Act 2018
3. Privacy and Electronic Communications Regulations 2003 ("PECR")

Fines for non-compliance are the higher of £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year.

Key Definitions

Personal data – any information identifying a data subject (individual in personal or business capacity) directly or indirectly from that data alone or in combinations with other information that is processed or can reasonably be accessed

Examples of personal data (non-exhaustive):

- Name
- Email address
- Postal address
- IP address
- User ID
- Photo (special category data)

Data Subject – individual whose data is being processed.

Data Controller – decides on the means and purposes of processing.

Data Processor – processes or has access to personal data, typically in the course of the provision of its services to data controller.

Special Category Data – information in connection with race or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Data Protection Officer – appointed in specific circumstances, such as processing on a large scale, or as a choice.

Data Processing – any activity involving the use of personal data - obtaining, storing, holding, recording, copying, sharing, organising, amending or retrieving.

Data Breach – any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the organisations, technical, physical or administrative safeguards; the loss of, unauthorised access, disclosure or acquisition of personal data.

GDPR Principles

- Lawfulness, fairness and transparency

- Purpose limitation
    - Specified, explicit and legitimate purpose
    - Only process personal data in a manner compatible with the purpose

- Data minimisation
    - Adequate
    - Relevant
    - Collect and keep what is necessary

- Accuracy
    - Accurate and kept up to date
    - Corrected or deleted promptly

- Storage limitation
    - Only keep data for as long as necessary for the purpose

- Integrity and confidentiality
    - Appropriate technical and organisations measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage

Controller or Processor

Every business is likely to be both.

Controller – in relation to users, customers, employees, contractors, suppliers and business contacts

Processor – where there is exposure to data entered or shared by customers or users in relation to their employees, clients, contractors and other parties

Compliance

Documents – Procedures – Training

Data Controller – record of data processing activities (use a flow charts), data protection policy, data retention policy, IT security policy, privacy policy for website/ app, terms and conditions, cookie policy, privacy policy for employees, other potential documents including data processing impact assessments and consent language

Data Processor – data processing agreement or data processing language in the relevant terms and conditions

Most of the documents are internal with user facing documents typically including privacy policy, terms and conditions, cookie policy, consent language and marketing communications including unsubscribe options.

Steps to demonstrate compliance:

- Privacy governance structure
- Policies/ documents and procedures
- Implement technical and security measures
- Training
- Tests and audits to demonstrate compliance

Lawful bases for processing

There must be a lawful basis to lawfully process personal data

- *Consent*
- *Contract or taking pre-contractual steps*
- *Legal obligation*
- Vital interests
- Public task
- *Legitimate interests*

Most businesses are likely to use the four lawful bases in *italics* above.

Data subjects' rights

- Right to be informed about processing
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights to data portability
- Right to object
- Right in relation to automated decision making and profiling

International data transfers

For transfers outside of European Economic Area (EEA) and UK use safeguards, including:

- transferring to countries that have adequacy decisions and are considered as having similar protection as countries within EEA;
- use Standard Contractual Clauses;
- when necessary for the performance of a contract;
- necessary to establish, exercise or defend legal claims.

If your company is not established in the UK and does not have a branch or a subsidiary in the UK you will need to appoint a UK data protection representative. The same applies to European countries.

What information to include in user/ customer privacy notice or policy

- name and contact details of organisation
- name and contact details of representative (if relevant)

- contact details of data protection office (if applicable)
- purposes of processing
- lawful basis for the processing
- legitimate interests for the processing (if applicable)
- categories of personal data obtained (if not directly from the individual)
- recipients or categories of recipients of the personal data
- details of transfers to any third countries of international organisations (if applicable)
- retention periods
- rights of individuals
- right to withdraw consent
- right to lodge a complaint with a supervisory authority (ICO in UK)
- source of personal data (if not obtained from individual)
- details of whether individuals are under a statutory or contractual obligation to provide the personal data
- details of any automated decision-making, including profiling (if applicable)

Brexit

There is currently a transitional period until 30 June 2021. If there is no adequacy decision towards the UK by the European Commission the UK will be seen as a 3rd country without adequate protection of personal data.