Introduction to Data Protection and FOI - Summary Sheet

April 2021

UK GDPR and the Data Protection Act 2018

In the UK, the General Data Protection Regulation (UK GDPR), sits side by side with the Data Protection Act 2018. The intention of this EU derived legislation was to harmonise data protection rules across EU member states. It applies to data processing carried out by individuals and organisations operating within the EU, but also applies to organisations outside the EU that offer goods and services to EU citizens. The UK GDPR significantly enhances the rights of data subjects in the processing of their personal data and strengthens the current system. The Data Protection Act 2018 controls how personal data is used by organisations, businesses and the government.

This new framework builds on and enhances existing data protection law. The key changes are:

- Greatly enhanced data subject rights
- An increased requirement for accountability and transparency by data controllers
- Visibility of the Data Protection Officer role in organisations
- Greatly increased sanctions for data breaches
- Stronger conditions for consent

Data Protection Principles

Everyone responsible for using data has to follow the data protection principles. They must make sure the information that relates to a living person, who can be identified from that data, or from that data when combined with other information is managed responsibly. There are seven principles to follow in processing such information:

1. It is lawful, fair and transparent
2. It is specific, explicit and legitimate
3. It is adequate, relevant and not excessive
4. It is accurate and kept up to date
5. It is kept for no longer than necessary
6. It is processed securely

7. Responsibility is taken for complying with the 6 other principles and appropriate processes and records are in place to show this – the accountability principle

There is stronger legal protection for special category personal information. There is a presumption that this data is private, open to misuse and therefore needs to be treated with greater care than other personal data. It covers private aspects of an individual's life such as:

- Ethnicity and religious beliefs
- Political opinions
- Health and sexual life
- Genetic and biometric data

Lawful Basis for Processing

Without a lawful basis for processing, an organisation cannot process personal data legally. Identifying the grounds for processing personal data is always your starting point.

There is no hierarchy of grounds for processing: all are equally valid. Controllers may choose a different lawful basis for different processing activities. The most appropriate lawful basis will depend on the personal data being processed and the purposes for processing. Depending on the personal data type and/or the organisation type there will be different grounds for processing. Where data is collected from the data subject, people must always be told of the legal grounds for processing.

<u>There 6 grounds for processing:</u>

Consent - the individual must give their consent freely. Pre-ticked opt-in boxes are not indications of valid consent. Consent must be clear and precisely explained so the data subject knows exactly how their personal data is being used. If using consent as a ground for processing, data subjects have increased rights to withdraw their consent. It must be opt in, unambiguous, specific and informed with no conditions. Note that children under the age of 13 require particular protection and there are additional requirements to obtain verified parental consent. Organisations have a responsibility to mitigate risks to children and young people's wellbeing by preventing, e.g. access to age-restricted online content or online services. Public-facing service providers' need to check that the age-related eligibility data is acceptable for the websites that they are accessing.

Contractual - processing is necessary for the performance of a contract or agreement to which the individual is party or is required prior to entering into a contract.

Legal basis - processing is necessary for compliance with a legal obligation.

Vital interests - processing is necessary to protect the vital interests of the individual or of another person, such as any life or death situation, or where their personal safety may be at risk.

Public interest - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

Legitimate interests - processing is necessary for the purposes of the business interests of the organisation or a third party, which would include the processing necessary for an organisation to carry out its core functions. The data is used in ways which people would reasonably expect.

Rights of Data Subjects - There are strengthened rights for individuals over their data that you are processing. They can request an organisation to make changes in how their data in handled and you must respond promptly should a request be made. Your organisation may be unlikely to receive such requests on a regular basis, so the important thing is to be able to recognise them should you receive one:

- Right to be informed – communicate clearly and use plain language in all your external messaging
- Right of access - have in place processes to respond to requests for what information you are holding (Data Subject Access Requests)
- Right to rectification - ensure you correct inaccurate information in the data you are processing without delay
- Right to erasure – you may be required to delete the data and stop processing it or publishing it (often called the Right to be Forgotten)
- Right to restrict processing – where the accuracy or lawful processing is challenged then temporary limits on the processing are required
- Right to data portability – you may be asked to provide the personal data you hold, securely and in a machine-readable format, so it can be moved, copied or transferred to be used across different services
- Right to object – ensure you have the right consents in place for activity such as direct marketing
- Rights related to automated decision making - if there is additional profiling based on the data you hold then an individual can object

Exemptions

There are a number of exemptions from the provisions to allow processing that supports:

- National security
- Prevention and detection of crime
- Legal proceedings
- Negotiations
- Parliamentary privilege
- Safeguarding of children and of individuals at risk
- Research and statistics
- Archiving in the public interest, which will be of massive importance to cultural heritage organisations in particular
- Other important public interests, in particular economic or financial interests
- The protection of judicial independence and proceedings

Privacy by Design

Under the new obligations outlined within the legislation organisations also need to embed a "Privacy by Design" approach into everything they do. As you start a new project build data privacy and respect for personal data into the planning from the outset. You can do this through embedding your data protection responsibilities by using the Naomi Korn Associates Compliance Framework - www.naomikorn.com/services/consulting which views compliance as a series of operational and strategic interventions built upon wide reaching data protection awareness and training and supported by robust governance and commitment.

For further information:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- https://ico.org.uk/for-organisations/data-protection-act-2018/http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/
- www.naomikorn.com/resources