Data Security – Data Protection Regulatory Framework

The General Data Protection Regulation (EU 2016/679) came into force on 25 May 2018 adding new elements and significant enhancements to the existing data protection regime.

The Data Protection Act (DPA) 2018, which came into force on 23 May 2018, implemented the GDPR, whilst also adding provision for UK law to extend the GDPR to areas such as the security services and government bodies, which were not covered under the GDPR alone.

Post-Brexit (following the end of the Brexit transition period from 1 January 2021 onwards), the UK GDPR is the retained version of the EU Regulation by virtue of section 3 of the European Union (Withdrawal) Action 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendment Etc) (EU Exit) Regulations 2020.

The UK GDPR protects the rights of UK citizens with regard to their data, the EU GDPR protects the rights of EU citizens. For organisations that handle data on both UK and EU citizens both GDPRs apply.

The principles and requirements of the EU GDPR continue to apply in the UK with its post-Brexit version and here we look at the major areas of scope and some definitions.

Controllers and processors

The GDPR applies to both controllers and processors of data. Controllers say how and why personal data is processed. The processor acts on the controller's behalf to process the data. Your organisation may be a data processor, or a data controller, or both.

There are specific legal obligations on both controllers and processors:

- controllers must specifically ensure that contracts with processors comply with the GDPR; and
- controllers and processors have separate, but explicit, requirements to maintain records of personal data and processing activities
- processors are also legally responsible and liable for any security breaches.

Please see our related factsheet 'Data Security - General Data Protection Regulation - Ensuring Compliance' for more detailed information on the documentation requirements.

Data protection principles

Personal data shall be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose
- accurate and kept up to date. Inaccurate data should be erased or corrected
- kept in an identifiable format for no longer than is necessary
- processed securely and protected from unauthorised or unlawful processing, accidental loss, or destruction or damage.

GDPR rights for individuals

The right to be informed

Individuals have the right to know how their personal data is going to be processed. The GDPR promotes transparency over processing by way of a privacy notice encompassing (amongst other things) details of the controller, the source of the data, recipients of the data, data transfers made outside the EU, and the retention period of the data.

The right of access (subject access request)

Individuals have the right to obtain confirmation that their data is being processed, access to their personal data, and other information, such as that provided in a privacy notice.

The maximum amount of time allowed to deal with a subject access request is 30 days and the right to charge a subject access fee has been removed, unless the request is unfounded, excessive or repetitive.

The right to rectification

Individuals have the right to have inaccurate or incomplete personal data rectified. This must also include personal data which is shared or given to third parties.

The right to erasure

Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Again, this must also include personal data that is shared or given to third parties.

It is important to note that there are extra requirements when the request relates to a child.

There are some exceptions to the right to erasure, such as where data is held to comply with a legal obligation.

The right to restrict processing

Individuals have the right to restrict the processing of personal data. In these circumstances the personal data can be stored, but not processed.

The right to data portability

Individuals have the right to obtain and reuse their personal data across different services. It allows them to move, copy or transfer personal data. Personal data must be provided in a structured machine-readable format (such as.csv).

The right to object

Individuals have the right to object to the processing of personal data. Processing must stop immediately unless there are 'compelling' legitimate grounds for the processing, or if processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

Individuals have the right to ensure that safeguards are in place to protect against the risk of damaging decisions being taken without human intervention. This also extends to the safeguarding of personal data used for profiling purposes.

Accountability and governance

The principle of accountability requires that appropriate governance measures are in place to document compliance. Organisations therefore need to:

- implement measures that meet the principles of data protection
- document policies and procedures in relation to the storage and processing of personal data
- implement technical and organisational measures to ensure and demonstrate compliance.
- appoint a data protection officer where necessary.

Please see our related factsheet 'Data Security - Ensuring Data Protection Compliance' for more detailed information.

Lawfulness of processing

It is important to understand and document the lawful basis of your processing. There are six:

1. Consent
2. Contractual obligation
3. Legal obligation
4. Vital interests
5. Public interest
6. Legitimate interests.

On the issue of consent, it must be specific, unambiguous and freely given. Positive consent cannot be assumed from inaction, such as failing to click an online 'unsubscribe' box, or from the use of pre-ticked boxes. Businesses need to make sure that they capture the date, time, method and the actual wording used to gain consent, so it is important to ensure that your business has the means to record and document such information.

ICO consent guidance

Legitimate interest will grant you the ability to process the individuals' data but only within the bounds that they would expect. If you are to rely on legitimate interests, you will take on the responsibility for ensuring that:

- there is a basis to use legitimate interest
- the processing of data is limited to that interest and can be demonstrated
- the individual's rights have been considered in a balancing process
- the individual is informed of the legitimate interests in your privacy policies.

ICO legitimate interests guidance

Notification of breaches

A personal data breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

The UK Regulator the ICO has an online self-assessment tool which helps to determine the severity of the breach and whether or not it need be reported. Some breaches need to be notified to the relevant supervisory authority within 72 hours. It is vital to undertake the assessment as soon as the breach is discovered.

ICO personal data breach assessment guidance

Transfer of data

On 28 June 2021 the EU Commission adopted an adequacy decision for the UK which means that most data can continue to flow between the UK and the EU EEA without the need for additional safeguards. (The exception is data for the purposes of immigration control.)

When transferring data to a 'third country', then additional safeguards such as Standard Contractual Clauses or Binding Corporate rules may be applicable. The first link below is from the UK's regulator – the ICO. The second is from the European Commission.

ICO data transfer agreement guidance

EU rules for transfers outside of the bloc

Sources and links

ICO home page for organisations

EU GDPR portal - http://www.eugdpr.org/

For information of users: This material is published for the information of clients. It provides only an overview of the regulations in force at the date of publication, and no action should be taken without consulting the detailed legislation or seeking professional advice. Therefore no responsibility for loss occasioned by any person acting or refraining from action as a result of the material can be accepted by the authors or the firm.