DATA SECURITY – GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) will replace the existing Data Protection Act and will apply from 25 May 2018.

Whilst there are similarities between the Data Protection Act and the GDPR, there are some new elements and significant enhancements.

The new GDPR will require all organisations that deal with individuals living in an EU member state to protect the personal information belonging to those individuals and to have verified proof of such protection. Failure to comply with the new regulation will result in significant fines.

Here we look at the scope and some of the key principles of the GDPR.

Controllers and processors

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

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 - preparation' for more detailed information on the documentation requirements.

Scope of the GDPR – data protection principles

The GDPR has a number of principles relating to personal data. Whilst these are not dissimilar to those under the UK Data Protection Act, there are some differences, together with a new accountability requirement. 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.

Finally, the GDPR requires that the controller shall be responsible for, and be able to demonstrate, compliance with these principles.

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 has been reduced from 40 to 30 days under the GDPR, 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 which is shared or given to third parties.

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 GDPR contains the principle of accountability, which requires that appropriate governance measures are in place. 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 (Please see our related factsheet 'Data Security - General Data Protection Regulation - preparation' for more detailed information on the documentation requirements.)
- implement technical and organisational measures to ensure and demonstrate compliance
- appoint a data protection officer where necessary (also see below)
- certain types of organisations, such as public authorities, must appoint a data protection officer

organisations which perform particular types of processing (large scale monitoring of individuals, or large scale processing of special categories of data, or data relating to criminal convictions and offences) must also appoint a data protection officer.

Conditions for consent

The new law places particular emphasis on the issue of consent, stating that an indication of consent 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 also 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.

Notification of breaches

Breaches must be notified to the relevant supervisory authority where *'it is likely to result in a risk to the rights and freedoms of individuals'.*

A notifiable breach must be reported within 72 hours.

Transfer of data

The GDPR places restrictions on the transfer of data outside of the EU.

Sources and links

ICO home page for organisations

ICO GDPR micro site self assessment toolkit 12 preparatory steps

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

How we can help

We can provide help in the following areas:

- performing a security/information audit of the storage and processing of personal data
- training staff in security principles and procedures
- notification
- advising on appropriate procedures to ensure compliance with regulations applicable to the organisation.

Please contact us on 0121 711 2468 or 024 7651 8555 if we can be of further assistance.