clarkslegal

GDPR.....in a nutshell

What is the GDPR?

The General Data Protection Regulation ("GDPR") is an EU regulation which will come into force automatically in the UK from 25th May 2018. Its aim is to overhaul and modernise data protection rules across the EU member states.

In the UK, the Data Protection Act 1998 will be repealed and replaced by a new Act – currently the Data Protection Bill – which is making its way through Parliament. This Bill reflects many of the provisions of the GDPR but also expands on these, for example addressing data processing that does not fall within EU law (such as immigration and national security).

What are the major changes under the GDPR?

Increased penalty for non-compliance

The GDPR increases the fine the UK regulator, the ICO, can award for most offences to (a) EUR20 million or (b) 4% of the organisation's annual worldwide turnover based on the preceding financial year (whichever is greater), though some breaches (such as failure to report) attract a slightly lower penalty, EUR10 million or up to 2% of annual worldwide turnover.

Consent will be more difficult to obtain

Consent may still be relied upon as a ground for processing data, however, there are stricter requirements for what amounts to consent under the GDPR. As such, many existing consents may not be valid.

Key points:

- Consent must be 'freely given, specific, informed and unambiguous'. Consent will not be 'freely given' where an individual has no genuine choice (so possibly in employment contracts).
- Agreement must be signified by a 'statement or by clear affirmative action'. Pre-ticked boxes or inactivity will not, therefore, be sufficient.
- Where consent is given as part of a wider document it must be clearly distinguishable from the rest of the terms. If processing is for multiple purposes then consent needs to be given to each purpose.
- Consent must be as easy to withdraw as it is to give.

Duty to notify the ICO within 72 hours of breach

Organisations MUST report a personal data breach to the ICO without undue delay if it is likely to result in a risk to individual's rights and freedoms and, where feasible, not later than 72 hours after becoming aware of it. If the breach is likely to be 'high risk' to an individual's rights and freedoms then there may also be an obligation to report to the individual without undue delay.

Must appoint a Data Protection Officer (DPO) in certain circumstances

Organisations MUST appoint a DPO in certain circumstances. This will apply to public authorities or organisations which carry out large scale systematic monitoring of data subjects or large-scale processing of certain data categories.

Individual rights expanded

The GDPR enhances existing rights and creates some new ones. Under the GDPR, individuals have a right to:-

- Receive certain information, including the legal basis for processing, details of recipients of the personal data, data retention periods and their rights (including their right to complain to the ICO).
- Access their personal data.
- Correct personal data where it is inaccurate, incomplete or out of date.
- Restrict data processing where this is inaccurate, unlawful, no longer needed or, in some instances, where an objection has been raised.
- Object to data processing and automated decision making.
- Have, in certain circumstances, their personal data erased (known as the "right to be forgotten").
- Data portability. This is a new right entitling an individual to receive data which he/she has provided to the controller in a 'structured, commonly used machine-readable form' so that their data can be transferred without hindrance from one IT environment to another in a safe and secure way.

Typically, a data controller has one month to action any of the above requests.

Timeframe for compliance with data access requests changed

Requests must be complied with 'without undue delay' and within one month. However, an extension of two further months is available if this is necessary taking into account the complexity of the request and number of requests. There are some other changes to the data access request process to make it easier for individuals seeking access.

Greater accountability for businesses

You do not only have to comply – you must be able to demonstrate compliance.

This is achieved largely via three new requirements:

- A Data Protection Impact Assessment must be carried out if new technology, or the processing, is likely to result in high risk to the rights and freedoms of the data subject.
- Data controllers MUST be able to demonstrate compliance. Therefore, adequate records must be kept. This includes, for example, records clearly recording an individual's consent, where consent is relied upon as a means of processing.
- Data controllers MUST implement data protection measures 'by design and by default'.

Extension of liability to data processors

Data processors have obligations under the GDPR and can now be held directly liable for breaches of data protection legislation.

If you would like further information please contact our GDPR Team:
Louise Merrell: LMerrell@clarkslegal.com
Jon Chapman: JChapman@clarkslegal.com

E: contact@clarkslegal.com
T: 020 7539 8000