BUSINESS BRIEFING: GENERAL DATA PROTECTION REGULATION

The law governing data protection will be subject to a radical change in 2018. The General Data Protection Regulation ("GDPR") will apply across the European Union, including in the UK, from 25 May 2018. The GDPR will replace the current European Data Protection Directive and the UK legislation, the Data Protection Act 1998, is expected to be repealed.

The Government has indicated that the UK will implement the GDPR to secure unimpeded data flows between the EU and the UK. Accordingly the GDPR is expected to continue to apply irrespective of the eventual Brexit outcome.

The GDPR will, however, impact on all businesses in the UK irrespective of whether they carry out business in the wider EU.

This note provides a summary of these new regulations and highlights some changes from the current Act.

What is the Reason for the Changes?

The aim of the GDPR is to harmonise the current data protection laws across the European Union. The GDPR updates and modernises data protection law and has a strong focus on giving more rights to individuals. It also recognises the significant technological advances since the original Data Protection Directive which dates back to the 1990s.

What are the key definitions in the GDPR?

Personal Data and Data Subjects

Personal data is any information relating to a living individual (who are referred to as "data subjects") from which that person can be identified, either directly or indirectly. Indirectly covers situations where a combination of data may identify an individual.

Accordingly personal data includes basic details such as name and address.

Although these concepts will be familiar the definition of personal data under the GDPR is more detailed than in current data protection legislation and specifically includes "online identifiers", such as internet protocol addresses, and genetic and biometric data.

Accordingly the width of the definition of personal data is perhaps even wider than under the Data Protection Act.

Processing

The definition of processing is in practice unchanged and covers anything done by a business with personal data. This includes collecting, recording, storing, combining and destroying personal data. Accordingly simply holding details would be processing.

Data Controllers and Data Processors

Data controllers are the person or organisation who determines how personal data will be processed. An example would be a business which will hold personal data about employees.

A data processor is a person or organisation who processes personal data on behalf of a data controller. An example is a business which contracts out the administration of payroll. This self evidently involves passing personal details about employees to a third party.

Again these concepts will be familiar.

What are the "Supervisory Authorities"?

Supervisory authorities are those public authorities established to oversee compliance with GDPR. In the UK the supervisory authority will remain the Information Commissioner's Office.

The Information Commissioner's role will continue to encompass providing guidance (principally on their website) and enforcement.

What are the Data Subject's Rights under the GDPR?

The principal rights for data subjects are:

Right to Information about Processing: Data controllers are required to provide certain information, including details of the purpose of processing and the legal basis for processing, to the data subject when information is collected from data subjects. Information also has to be provided to the data subject where the personal data was not collected directly from the data subject.

The obligation is to provide these details irrespective of whether the detail has been requested by the data subject. This is one of many examples of where the GDPR requires a proactive approach from data controllers.

The provision of this information is commonly referred to as a "privacy notice".

Right of Access: Data subjects have the right to request from the data controller certain information, including details of personal data stored and the envisaged period for which the data will be stored, as well as a copy of the personal data held. The data controller will normally have one month to comply with any request and cannot usually charge a fee.

There are exceptions in cases where requests are "manifestly unfounded or excessive" in particular repeat requests.

This right is similar to the current subject access request provisions.

Right to Rectification: Data subjects can request that the data controller (i) rectifies any inaccurate personal data and (ii) completes any uncompleted personal data without undue delay.

Right to Data Portability: In most cases data subjects have the right to receive their personal data from the data controller in a structured, commonly used and machine-readable format (for example, in an excel spreadsheet). Data subjects also have the right to require that data controllers transmit their personal data to another data controller.

Right not to be Subject to Automated Decision Making: Data subjects have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual. Examples include automatic refusal of online credit applications and e-recruitment practices which do not involve human intervention. Data controllers must ensure that individuals are able to obtain human intervention; express their point of view; and obtain an explanation of the decision and challenge it.

Right of Erasure ('The Right to be Forgotten'): Data subjects have the right to ask a data controller to remove their personal information without undue delay in certain circumstances in particular where the data controller no longer has justifiable grounds for holding the information (see below) or where the processing is unlawful .

Where the data controller requires to erase the data, the data controller is also expected to intimate the request to any other data controllers to whom the information has been passed. A data controller must take all reasonable steps to do this but it is acknowledged that in some cases complete erasure will not be possible.

Such requests may be denied if there is a legal or public interest requirement.

Right to Restrict Processing: The data subject has the right to require the data controller to restrict processing of the data to its storage in certain circumstances including when the accuracy of the personal data is contested by the data subject or where the processing is unlawful.

Right to Object: Individuals have the right to object to processing in certain circumstances including where processing (including profiling) is carried out for direct marketing purposes or where processing is for purposes of scientific/historical research and statistics.

The use of personal details for direct marketing purposes (including the need for data controllers to demonstrate consent for mailshots etc) is one of many areas where the GDPR should lead to an immediate change in practice.

What are the Data Controller's Obligations under the GDPR?

In addition to complying with data subjects' rights (as set out above) the GDPR places further obligations on data controllers. These will be broadly familiar to those with a working knowledge of the current data protection legislation but there are some significant innovations including a new emphasis on a business's ability to demonstrate compliance.

Data Protection Principles

The GDPR sets out a number of principles with which data controllers and processors must comply when processing personal data.

The data protection principles are:

Lawfulness, fairness and transparency. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation. Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Data minimisation. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Accuracy. Personal data must be accurate and, where necessary, kept up to date. Data which is known to be inaccurate must be erased or rectified without delay.

Storage limitation. Personal data must not be kept for longer than is necessary for the purposes for which the data is processed.

Security. Personal data must be processed in a manner that ensures its appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. In this regard, data controllers and processors must use appropriate technical or organisational security measures.

Accountability. The data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

In addition to the need to act in accordance with the above principles any processing of data must be "lawful".

Lawful Processing

Processing of personal data will only be lawful if one of the six requirements set out in the GDPR are met. Although similar to the current requirements the conditions are more onerous on both data controllers and data processers.

Accordingly one or more of the following must apply to the processing of data:

1. The data subject has given consent to processing.

    - Consent must be freely given, specific, informed and unambiguous.
    - Silence or inactivity does not constitute consent.
    - The data subject must be able to withdraw consent as easily as it was given.
    - The controller must be able to demonstrate that consent was given.

2. Processing is necessary for performance of a contract
    - For example, holding personal details such as name, address and payment details may be necessary when supplying goods and services that a data subject has requested.
    - Performance includes an intention to enter into a contract and steps taken before entering into a contract.

3. Processing is necessary for compliance with a legal obligation
    - This will apply if processing is required by UK or EU law for a particular purpose.

4. Processing is necessary to protect vital interests of a natural person
    - Required to protect an interest which is essential for the life of the data subject or another natural person.
    - Should only be relied on when the processing cannot be justified on another ground.

5. Processing is necessary for a task carried out in the public interest
    - Required to carry out official functions of a task in the public interest.

6. Processing is necessary for the purposes of the legitimate interests pursued by controller
    - When there is a genuine and legitimate reason as long as it is not outweighed by harm to the data subject's rights and interests.
    - Involves a considered judgement call and the data controller should be able to demonstrate the reasons behind any decision that processing is lawful when relying on this ground

Additional conditions apply to situations where the controller is processing "special categories of personal data". This is a new definition but is similar to, and will replace, the existing "sensitive data".

Special categories of personal data include data:

- revealing racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data, biometric data, data concerning health
- data concerning sex life or sexual orientation.

Despite some changes the need to apply by principles and act lawfully is broadly similar to the existing law governing data protection.

The GDPR, however, contains some more radical innovations which businesses require to comply with. There is a new emphasis on businesses being able to demonstrate compliance. These include "data protection by design".

Accountability and Data Protection by Design

Data controllers will now be required to put in place effective organisational and technical measures which are designed to ensure compliance with the GDPR and protect the rights of data subjects. This is known as data protection by design.

This is an example of the GDPR's attempt to reflect the realities of data usage in the 21st century. It places a new emphasis on businesses to (i) reviewing the data they process and the reasons why (ii) to assess the risks to the data subject and (iii) to implement "appropriate technical and organisational measures" to protect the rights of data subjects.

Although compliance cannot be seen as solely an issue for the IT team, for most of us they will be involved in ensuring that we meet the requirements of the GDPR.

In the past data controllers in the UK were required to notify the Information Commissioner that they were processing data in certain circumstances. This requirement will be removed by the GDPR. Instead, in terms of GDPR, there is an obligation for the data controller to be able to demonstrate compliance with the new legislation.

Data Protection Impact Assessment

There is a new requirement for the data controller to assess the impact of processing before it is carried out in certain circumstances.

A data protection impact assessment is to be carried out where high risk processing is envisaged, such as extensive profiling activities, large scale processing or systematic monitoring of public areas. Supervisory authorities are required to establish a list of activities which require a data protection impact assessment. As yet the Information Commissioner has not published such a list.

Put broadly a data protection impact assessment is a risk assessment which will include a review of the data controllers' operation, consideration of the purposes for all processing and the risks arising including the security of the personal data held.

In cases where the data controller considers, after undertaking a data protection impact assessment, that the proposed processing is high risk the data controller should consider whether those risks can be addressed. The term "high risk" is not defined by GDPR but is likely to include handling large scale data particularly where

this is of a sensitive nature. If the data controller cannot sufficiently address the risks identified the data controller is required to consult the Information Commissioner and seek its opinion on whether the processing would comply with GDPR.

Data Protection Officer

There is a new requirement for data controllers to appoint a Data Protection Officer (DPO) to be appointed in certain circumstances, namely:-

1. For all public authorities;
2. Where there is regular and systematic monitoring of data subjects on a large scale; or
3. Where there is large scale processing of certain categories of personal data which are particularly sensitive (e.g. data relating to criminal convictions, health information, data revealing political opinions or religious belief etc).

A DPO does not have to be an independent individual, but must have a sufficient knowledge of data protection law and practices.

Records of Processing Activities

Data controllers are required to maintain a record of processing activities for which it is responsible. The GDPR stipulates specific information to be recorded including the purposes of processing, a description of categories of data subjects and personal data, envisaged time limits for erasure and a general description of technical and organisational security measures in place.

The requirement to maintain records of processing will not apply to organisations employing less than 250 peoples except in certain circumstances including where:

1. The processing is likely to result in a risk to the rights and freedoms of the data subjects;
2. The processing includes certain categories of personal data which are particularly sensitive (e.g. data relating to criminal convictions, health information, data revealing political opinions or religious belief etc); or
3. The processing includes personal data relating to criminal convictions and offences.

Notification and recording of Breaches

Data controllers are now under an obligation to report all data breaches to the ICO unless they are unlikely to represent a risk to the rights and freedoms of data subjects. This is a significant new requirement.

Breaches must be reported within 72 hours. If they are not reported within this time scale, reasons must be provided in order to justify the delay.

The data controller must also now document any personal data breaches including the facts relating to the breach, the effect of the breach and any remedial action taken.

There is a separate duty to report the breach to any data subject effected where there is a "high risk to the rights and personal freedoms" of the individuals. This should be done "without undue delay".

What are Data Processors' Obligations under the GDPR?

The innovations of the GDPR include a new emphasis on the activities of data processors (i.e. someone who handles data on behalf of the controller). This includes the need for controllers to consider the risks involved in engaging a particular processor.

Basic requirements for Processors

Broadly, data processors will be required to: provide guarantees that they will meet GDPR requirements (e.g. by reference to a code of conduct or approved certification); process any personal data in accordance with GDPR requirements; in certain circumstances, maintain written records of all processing activity; co-operate with the supervisory authority; implement appropriate technical and organisational measures to ensure appropriate security; take into account in particular the risks of processing (e.g. accidental/unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data); notify the data controller of any personal data breach; and (in certain cases) designate a data protection officer.

If a processor takes on the active role of determining the purposes and means of processing the data, the processor shall be considered to be a data controller in respect of that processing and subject to the applicable obligations.

The processor shall be required immediately to inform the controller if, in its opinion, an instruction infringes GDPR or other EU or Member State data protection provisions.

How to engage a Data Processor under the GDPR?

General requirement to use a "reputable processor"

The data controller will be obliged to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet GDPR requirements and ensure the protection of the rights of the data subject.

Requirement to regulate processor's activities with a contract

Processing by a processor on behalf of a data controller is to be governed by a contract (or other legal act) under EU or national law that is binding on the processor.

The GDPR states that "*Processing by a processor shall be governed by a contract.....*". It does not specifically state whether the duty to put that in place falls

on the controller, processor or both, but that might be expected to be the responsibility of the data controller.

The GDPR stipulates various matters which require to be set out in the contract including the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

The contract (or other legal act) referred to above may be based, in whole or in part, on standard contract clauses prepared by the Commission or the supervisory authority, which in the UK is the Information Commissioner. As far as we are aware these standard clauses are not yet available.

Conditions for engaging another processor

A processor should not engage another processor without prior specific or general written authorisation of the controller.

Where a processor engages another processor to carry out specific processing activities for the controller, the same data protection obligations as set out in the contract between the data controller and processor are to be imposed on that other processor by contract. The contract should provide in particular sufficient guarantees to implement appropriate technical and organisational measures so that processing will meet the requirements of GDPR. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the data controller for the performance of any other processor's obligations.

What are the Penalties?

The penalties under the GDPR for any breach are now tougher. Fines can be up to 4% of annual global turnover or €20 million, whichever is greater.

Jurisdiction

One of the key objectives of the GDPR is the 'one stop shop' vision. A company operating in several EU countries should only need to deal with one supervisory authority, normally where its main establishment is located.

Children

Particular care is required when handling persona data related to children including the need for parental consent. Children are any child under the age of sixteen. Member states have the option to lower this age to thirteen.

First Steps for Preparing for GDPR

1. Carry out an audit of all personal data held, the reasons why and who it is shared with
2. Review your data protection policies and procedures for compliance with the GDPR
3. Plan your approach to GDPR compliance including considering who will have particular responsibility within the business, review your relationship with data processors and consider where express consent from data subjects may be required.
4. Review whether you require a Data Protection Officer
5. Raise awareness of the GDPR within your organisation including reviewing the need for training.

Ledingham Chalmers Assistance

Ledingham Chalmers LLP are happy to assist data controllers and data processors to prepare for the GDPR including by reviewing current GDPR compliance, drafting and revising data protection policies and procedures and providing training on GDPR for your organisation.

For further information please contact:

Kirk Tudhope, Partner
Telephone: 01463 667400
Email: Kirk.Tudhope@ledinghamchalmers.com

Sine Mackay, Associate
Telephone: 01463 667400
Email: Sine.Mackay@ledinghamchalmers.com

Veli-Matti Räikkönen, Senior Associate
Telephone: 01224 408474
Email: Veli-Matti.Raikkonen@ledinghamchalmers.com

Ledingham Chalmers LLP, Solicitors
Johnstone House, 52-54 Rose Street, Aberdeen AB10 1HA (Registered Office)
DX: AB15 Aberdeen
www.ledinghamchalmers.com
Ledingham Chalmers LLP is a limited liability partnership - Registered in Scotland No. SO300843
A list of members is available for inspection at the above address