DIXON WILSON
CHARTERED ACCOUNTANTS

GDPR – Key Provisions

1 March 2018

INTRODUCTION

The new General Data Protection Regulation (GDPR) will be introduced in the UK and the EU on May 25th 2018.

The rules replace the Data Protection Act (DPA).

The new regulation is intended to provide individuals with greater control over their data now that businesses are collecting more and more personal information.

The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Any business currently subject to the DPA will already have adopted good practices which will be strengthened under GDPR. However, GDPR adds new responsibilities for data controllers and data processors, and new rights for individuals.

All enterprises processing personal data will be caught by the new regulation and steps should be taken now to ensure businesses are prepared for the transition to GDPR early next year.

WHO IS IMPACTED?

GDPR refers to the term *'enterprise'*. Under GDPR, an enterprise is any *'natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in economic activity'*. GDPR applies to enterprises established in the EU and to non-EU enterprises that offer goods or services in the EU or monitor the behaviour of individuals in the EU.

THE DETAILED PROVISIONS

There are a number of key changes to the data protection regulations under GDPR.

INDIVIDUALS RIGHTS

The GDPR includes the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to be forgotten
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Generally, the rights of individuals are similar to those under the DPA but these have been significantly strengthened under GDPR and procedures should be in place to cover the new rights that individuals have.

The *'right to be forgotten'* means data subjects can request their data to be erased. However, the ICO (Information Commissioners Office) acknowledges that there are legal obligations and professional guidelines that may require data controllers or processors to retain certain kinds of data for specific periods. Organisations should have a retention policy in place and regularly review and cleanse databases in line with retention periods.

The individual's *'right of access'* is strengthened under GDPR. Information must be provided within one month of the data subject's requests, rather than the current 40 days. This can be extended to two months if the request is complex and the request can be declined in extenuating circumstances. In most cases, there should be no charge for the provision of this information. In order to help businesses comply, the ICO recommends (where possible) providing remote access to a secure self-service system so that the individual can have direct access to their information.

The right to *'data portability'* is new under GDPR. Data subjects now have the right to have data transferred to a third party service provider in machine readable format. However, this right only arises where personal data is provided and processed on the basis of consent or when necessary to perform a contract.

LEGAL BASIS FOR PROCESSING DATA

From May 2018, businesses will have to explain the lawful basis for processing personal data in their privacy notice and when answering a subject access request. Businesses should review the types of processing activities they carry out, identify the legal basis for doing so and document this.

Where a business relies on consent, it is not automatically required to refresh all existing DPA consents. Businesses can continue to rely on existing consents if these are in line with GDPR. Consent must be *'freely given, specific, informed and*

unambiguous' and separate from other terms and conditions. It should also be made just as easy to withdraw consent. If existing consents do not meet GDPR standards, then businesses will need to seek new consents from clients, customers, suppliers and other third party contracts.

However, consent may not be the most appropriate justification a business will want to rely upon for processing data. There may be an alternative basis which should be considered.

Processing is lawful where necessary for the performance of a contract with the individual, for example, processing address details to deliver goods or processing bank details to pay employees. Processing may also be necessary for compliance with a legal obligation and where processing is necessary for a businesses (or third party's) legitimate interests.

Practical guidance on this area is expected to follow when the ICO and various professional and trade bodies issue detailed guidance on GDPR.

CHILDREN

The GDPR contains new provisions intended to enhance the protection of children's personal data. Where online services are provided to a child and consent is relied upon as the basis for lawful processing, consent must be obtained from an authorised parental responsibility. Companies working with children need systems in place to verify the age of individuals and to obtain parental/guardian consent for processing activities. The GDPR sets the age when a child can give their own consent to processing at 16 (although this may be lowered to a minimum of 13 in the UK).

PRIVACY IMPACT ASSESSMENTS

Privacy impact assessments and privacy by design are now legally required in certain circumstances under GDPR. Businesses are obliged to carry out data protection impact assessments for new technologies and high risk projects. Businesses should therefore start to assess situations where it will be necessary to carry out privacy impact assessments.

Privacy by design involves considering privacy risk when designing a new product or service rather than as an afterthought.

DATA PROTECTION OFFICER (DPO)

It is widely accepted that having a DPO does increase the status and priority of data protection within organisations. A DPO is required if a business:

1. Is a public authority
2. Carries out systematic monitoring of data subjects on a large scale
3. Carries out large scale processing of special categories of data relating to health records, criminal convictions and offences

The DPO must:

- Be appointed based on professional qualities and expert knowledge on data protection law and practices.
- Be a director, partner, staff member or an external service provider.
- Be the first point of contact for supervisory authorities and have their contact details published.
- Have appropriate resources available to carry out their tasks and maintain their expert knowledge.
- Report directly to the highest level of management.
- Perform the role of DPO independently and not carry out other tasks that could result in a conflict of interest. For example, the DPO cannot have a position where they decide how the business processes personal data.

INTERNATIONAL

If the organisation operates in more than one EU member state, organisations need to determine their lead data protection supervisory authority and document this. The lead authority is the supervisory authority in the state where your main establishment is. However, this is only relevant where a business carries out cross-border processing.

Non-EEA data transfers continue to be prohibited unless an adequate level of protection is in place, for example, where a Privacy Shield or EU Model Clauses have been entered into between parties.

However, the GDPR potentially allows for greater flexibility on overseas transfers by including additional approved safeguards such as an approved code of conduct, an approved certification mechanism and standard model clauses approved by a supervisory authority.

DATA BREACHES

The GDPR introduces new reporting guidelines for data breaches. A breach may result in the loss, alteration, destruction or unauthorised disclosure of or access to personal data.

In case of a personal data breach which results in a high risk to the freedoms of an individual, all businesses are obliged to inform the relevant supervisory authority within 72 hours after

having become aware of it. Businesses will also be required to notify those concerned directly. They must state the nature of the breach, the approximate number of people affected and the contact information for the DPO.

All businesses need to ensure they have the right procedures in place to detect, report and investigate a personal data breach. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Under GDPR, a data subject can potentially claim against all parties involved in the processing chain. One important aspect will be determining how secure suppliers and third party processors' systems are.

TWO-TIER FINE POLICY

The GDPR imposes steep penalties for non-compliance with the new rules and sets out a two-tier fine policy:

Tier 1 – Data breaches which are considered to be the most important for data protection could lead to fines of up to €20 million or 4% of worldwide turnover, whichever is **greater**. Examples of such breaches include not complying with basic processing principles such as meeting the conditions for consent.

Tier 2 – Lower level data breaches, for example, not keeping proper written records of processing activities, could lead to fines of €10 million or 2% of turnover whichever is higher.

WHAT DO BUSINESSES NEED TO DO NOW?

Businesses that fail to comply with the GDPR could face fines of up to 4% of global turnover or €20m, whichever is greater, in the case of a breach. Most importantly, the reputational and brand damage of such a breach can have major consequences for a business.

All businesses processing data should take steps to understand how they will comply with the new regulation and start to put systems and processes in place to ensure they are compliant to avoid facing these penalties.

The following initial steps should be taken:

1. Carry out a data audit to identify what data the business holds, where data is stored, who data is shared with and identify the legal basis for processing data.
2. Review security procedures and identify any weaknesses. This should cover storage and transfer of data.
3. Conduct a review of suppliers and other third party processors' security systems to ensure compliance with GDPR.
4. Check third party contracts to ensure adequate safeguards have been included to protect personal data.
5. Update internal procedures to ensure compliance with individual's rights.
6. Have procedures in place for detecting, investigating and reporting breaches.

For an example of more specific steps, please see our note on the initial steps Dixon Wilson is taking to ensure the firm complies with GDPR. We expect these steps to be updated as it becomes clearer how GDPR should be applied in practice.

Dixon Wilson
22 Chancery Lane
London
WC2A 1LS

T: +44 (0)20 7680 8100
F: +44 (0)20 7680 8101
DX: 51 LDE

www.dixonwilson.com
dw@dixonwilson.co.uk