GUIDE TO THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) represents the new legal framework of data protection law across the EU and is due to come into force on the 25 May 2018. The GDPR will supersede the Data Protection Directive (DPD), which has governed EU data protection law for over 20 years since its introduction in 1995. The DPD was implemented in the UK by the Data Protection Act 1998 (DPA).

Central to the vision for the GDPR were the dual aims of consistency and modernity, intending to harmonise the approaches of Member States through its direct effect and providing a future proof regime to meet the current and future demands of the age of digital communication.

Much of the GDPR mirrors existing data protection law. However, there have been significant changes imposing increased risks and obligations on businesses, some of which have created significant uncertainty surrounding implementation.

This guide aims to explain the key features of the new landscape of data protection, highlighting changes from the previous law and offering practical tips for compliance.

CONTENTS

BREXIT

Given the increased obligations inherent in the GDPR, it may be tempting for businesses to assume that after the UK voted to leave the EU they might escape compliance. After all the Government has announced its intention to trigger Article 50 by March 2017, over a year before the GDPR comes into force in May 2018.

However, in reality it is very unlikely that the UK will avoid compliance with the Regulation. Firstly, it seems fanciful to expect the government to conclude its exit negotiations within 14 months. Indeed, the Secretary of State, Karen Bradley MP confirmed to the Culture, Media and Sports Select Committee in October 2016 that the UK will be implementing the GDPR in May 2018. Furthermore, when the UK does leave the EU commentators have predicted that the Great Repeal Bill will enshrine the GDPR, along with other EU laws, into domestic legislation. After all, compliance with the GDPR may be a pre-condition to participation in the EU single market. (The preamble to the GDPR places great emphasis on the way in which free movement of goods goes hand in hand with free movement of data). Finally, even if the GDPR was repealed, UK businesses that offer goods or services to the EU would need to be GDPR compliant with respect to those activities, by virtue of the GDPR's increased scope.

OBJECTIVES OF THE GDPR

Before drilling into the details of the GDPR, it is important to grasp the spirit behind its enactment, and the objectives that it sets out to achieve. In summary, the GDPR has been created in pursuance of the following aims:

- the protection of fundamental rights and freedoms, including the right to privacy;
- to enable free movement of personal data within the EU;
- to contribute to economic and social progress and trade;
- to bring treatment of personal data into the digital age; and
- to harmonise data protection laws across the EU, with a coherent and consistent cross-border approach.

DATA PROTECTION PRINCIPLES

The principles governing the processing of personal data under the GDPR broadly mirror those under the previous regime of the DPD. In summary, the principles are:

1) **Lawfulness, fairness and transparency**: personal data must be processed lawfully, fairly and in a transparent manner.

2) **Purpose limitation**: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3) **Data minimisation**: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) **Accuracy**: personal data must be accurate and, where necessary, kept up to date.

5) **Storage limitation**: personal data must be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data is

processed.

6) **Integrity and confidentiality**: personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unlawful processing, accidental loss, damage or destruction. This principle ties in with the "*data protection by design*" concept [*link to later section*] that runs though the GDPR.

7) **Accountability:** the Data Controller shall be responsible for and be able to demonstrate compliance with the data protection principles. This is the biggest change to the principles: the need for Data Controllers to adhere to the principles is now paramount and evidence must be retained to demonstrate compliance.

DATA PROTECTION BY DESIGN

The GDPR places significant accountability obligations on Data Controllers to be able to demonstrate their compliance with the GDPR principles, a concept known as "*data protection by design*". While this is the first time that this principle has been an express legal requirement, it was an implicit duty under the DPA.

The Data Controller is required to implement technical and organisational measures designed to:

- implement data protection principles in an effective manner;
- integrate the necessary safeguards to comply with the GDPR and protect individual rights; and
- ensure that only personal data necessary for each specific purpose of the processing are processed (data minimisation).

Data protection by design measures may include pseudonymisation or anonymisation where appropriate, staff training on data protection, and undertaking audits. In the case of high risk processing (e.g. monitoring activities) a detailed privacy assessment (PIA) must be undertaken and documented.

Adherence to an approved code of conduct can be used to help demonstrate compliance with this principle.

MATERIAL SCOPE

The GDPR applies to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*". The DPD defines "*personal data*" as "*any information relating to an identified or identifiable natural person*". An identifiable person is further defined as *"one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*. The GDPR extends these definitions to expressly include location details, operative information and online identifiers. It also catches pseudonymised data.

TERRITORIAL SCOPE

The GDPR has a two pronged territorial scope:

1) It applies to the processing of personal data by Data Controllers and Data Processors who are established within the EU (this is likely to be a wide category since this applies regardless of whether the processing itself takes place in the Union);

2) It applies Data Controllers and Data Processors outside the EU, whose processing activities relate to:

   a. the offering of goods or services (even where provided for free) to EU data subjects (this is a question of analysing the business's intention i.e. whether an offer to an EU based data subject was envisaged); and

   b. monitoring the behaviour within the EU of EU data subjects (e.g. apps and cookies that track web-users).

These represent important extensions to the regime under the DPA. Firstly, the statutory obligations under the DPA generally only applied to Data Controllers. Processors previously escaped statutory regulation, and were generally subject to data protection obligations only to the extent imposed on them contractually by Data Controllers. Data Processors are now subject to direct regulation, and will need to ensure that they comply with the GDPR.

Secondly, the territorial reach of the rules is expanded since the Regulation not only considers the location of the processing of data (which was the approach under the DPA) but also the location of the individual whose data is being processed. The logic of this expanded scope is that businesses who wish to benefit from selling into the EU and/or monitoring the activities of individuals based in the EU, must in turn comply with the obligations imposed by the GDPR thereby balancing commercial advantage with EU citizens' right to privacy.

While this expanded scope advances the objective of creating a level playing field in EU data protection law, it also casts some doubt on the effectiveness of the enforceability of the regime. This has caused some commentators to speculate that reputation, rather than sanctions, will be the main driver behind compliance outside of the EU.

ROLE OF THE DATA PROCESSOR

The definition of a Data Processor is the same under the GDPR as under the DPA i.e. any person which processes personal data on behalf of the Data Controller. A Data Controller by contrast is a person who determines the purposes for which and the manner in which any personal data are to be processed. The distinction essentially rests upon the degree of responsibility which the organisation in question has over the data processing. If a Data Processor goes beyond following the instructions of the Data Controller, then it becomes a Data Controller itself.

The new obligations imposed on Data Processors by the GDPR include the duties to:

- keep written records of the processing activities for which it is responsible;
- cooperate with the supervisory authority;
- implement appropriate and proportionate measures to ensure the security of the data processing in accordance with the instructions of the Data Controller;
- notify a personal data breach to the Data Controller without delay; and
- appoint a data protection officer where required.

The consequences of breaches of these obligations is explored more fully under the "*Enforcement*"

section *below* but in brief the Data Processor may be:

- liable to the data subject for the damage caused by the processing where the Data Processor has not complied with the GDPR or where it has acted outside or contrary to the lawful instructions of Data Controller;
- jointly and severally liable for processing carried out with the Data Controller;
- subject to sanctions for breach.

RIGHTS OF INDIVIDUALS

One of the key objectives of the GDPR is to fortify the rights of individuals in relation to protection of personal data and the right to privacy. Accordingly, the GDPR strengthens some of the rights existing under the DPA, and creates some new rights altogether. The substance of each of these rights is outlined below.

1) **Right to be informed (Article 12):** This right encompasses the need for Data Controllers to provide information notices to individuals, providing specified information including: the identity and contact details of the Data Controller, the purposes of the data processing, the recipients of the personal data, the period for which the data will be stored etc. The GDPR emphasises that the communication of such information must be transparent, clear and concise.

2) **Right of access (Article 15):** A Data Controller must on request provide confirmation that an individual's data is being processed, provide access to their personal data, and provide supporting, explanatory materials. This right is similar to the subject access rights under the DPA, and still only applies to Data Controllers (not Data Processors). However, the scope of the GDPR right of access is significantly broader, the timeframe for responding is reduced and the fee waived. The right of access is a qualified right; where a request from a data subject is excessive or manifestly unfounded, the Data Controller may either charge a reasonable fee or refuse to act.

3) **Right to rectification (Article 16):** Data subjects can require a Data Controller to rectify their personal data where it is inaccurate or incomplete. This must be done without undue delay. The Data Controller must also inform third parties to whom the data has been disclosed of the rectification. This right is virtually unchanged in the GDPR compared to the DPA.

4) **Right to be forgotten (Article 17):** This right, otherwise known as the "*right of erasure*" has received particular attention. The right essentially allows individuals to request the deletion or removal of personal data without undue delay where there is no compelling reason for its continued processing. This right is accompanied by an obligation on the Data Controller to take reasonable steps to inform relevant third parties of the data subject's election to be "*forgotten*", which may be difficult to implement in practice. There are various exceptions to the right to be forgotten. For instance the right does not apply to the extent that it is necessary for exercising the right to freedom of expression and information, to comply with a legal obligation, or for archiving purposes in the public interest.

5) **Right to restrict processing (Article 18):** Individuals have a right to suppress or block processing of personal data in certain situations e.g. if the accuracy of the personal data is contested by the individual, if the processing is unlawful but the individual objects to erasure etc. This is a new right under the GDPR. Where processing is restricted, such

personal data can only be processed with the individual's consent. If the data has been disclosed to others, then the Data Controller must notify those recipients about the restriction, unless this involves disproportionate effort or is impossible.

6) **Right to data portability (Article 20):** This is a new right. It allows individuals to obtain and reuse their personal data for their own purposes across different services, providing that the data in question is provided by the data subject to the Data Controller, processed automatically, and processed on the basis of consent or fulfilment of a contract. The Data Controller is required to provide the data in a structured, commonly used and machine readable format and can be required to transmit the data to another Controller.

7) **Right to object (Article 21):** Individuals have the right to object to the following specific types of processing: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing, and processing for purposes of scientific/historical research and statistics. The right to object to marketing is absolute, while the other two are qualified. Individuals must be clearly notified of their right to object, and online services must offer an automated method of objecting.

8) **Right not to be subject to automated decisions or profiling (Article 22):** Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects the data subject e.g. e-recruiting and credit decisions. This right is broadly unchanged from the DPA and is intended to act as a safeguard against the risk of harmful decisions being taken without human intervention. Controllers are required to comply with this right by ensuring that individuals can obtain human intervention, express their point of view and challenge the decision. This right is not absolute, and is qualified by various exceptions e.g. if the decision was based on the individual's explicit consent.

Data Controllers will need to ensure that they have clear processes in place to enable them to meet these obligations. Existing processes should be audited to assess their compliance with the above rules, and adapted where necessary.

PERMITTED DEROGATIONS

It is worth noting that Member States retain the ability to restrict the rights granted to individuals under the GDPR. However, the grounds for such restrictions are limited. The derogation must be proportionate, and be necessary in a democratic society to achieve one of a list of prescribed purposes including the safeguarding of national security, defence, public security etc.

In order for such a legislative measure to be acceptable, it must set out a number of matters, including the purposes of the processing, the categories of personal data affected, the scope of the restrictions being introduced, safeguards to prevent abuse, unlawful access/transfer, the Data Controllers who may rely on the restrictions, the risk to individuals' rights and freedoms and the right of individuals to be informed about the restriction (unless prejudicial).

CONSENT

The definition of "*consent*" is stricter than under the DPA. "*Consent*" is defined in the GDPR as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing*". (The underlined words did not appear in the DPA definition). The GDPR also requires that, where

processing is based on consent, such consent be separate from other written agreements, clearly presented and as easily revoked as given. There is a prohibition on what may be called "*bundled*" consents, and on the offering of services conditional on consent to processing. Data Controllers must be able to demonstrate that consent was given. There are also special provisions relating to parental consent required for children to receive Information Society Services.

These heightened obligations represent one of the most significant changes in the GDPR. While existing consents used in your business may still work it will be vital to assess whether the new conditions are met. If not, your mechanisms must be altered or an alternative to consent found. You should also review your systems to ensure you have an effective audit trail to demonstrate that the required consents have been given.

DATA BREACH NOTIFICATION

As mentioned above, Data Processors now have a duty to notify a personal data breach to the Data Controller without delay. The Data Controller, in turn, must report breaches to their supervisory authority (where feasible within 72 hours of awareness), and in some cases must also report the breach to the affected data subjects. Data Controllers are required to maintain an internal breach register. However, it is important to note that there is a materiality threshold; notification is not necessary where the breach is unlikely to result in a risk to the rights and freedoms of individuals.

It will be important for Data Controllers and Data Processors to develop and update their internal procedures for detection, reporting and investigation of data breaches. Some organisations are already subject to data breach notification requirements under the existing law. This duty now applies across the board.

ROLE OF THE DATA PROTECTION OFFICER

The GDPR requires certain organisations to appoint a Data Protection Officer (DPO). This obligation applies to:

- public authorities;
- bodies which undertake regular and systematic monitoring of individuals on a large scale; and
- bodies whose core activities consist of large scale processing of sensitive categories of data e.g. data relating to racial origin, sexuality, criminal convictions etc.

"*Public authority*" is not defined in the regulations, and while it is clear that core public authorities such as central and local government will be caught, the position is less clear for hybrid bodies. Interpretation of the terms "*core activities*" and "*large scale*" activities will clearly also be central to determining whether your organisation triggers the requirement to appoint a DPO.

The role of the DPO is primarily to monitor the organisation's compliance with the GDPR. The DPO will be responsible for informing and advising the Data Controller or Data Processor and their employees of their obligations to comply with data protection law and providing advice with regard to data protection impact assessments. They will also act as a contact point for the relevant supervising authority (which in the UK is the ICO), and will cooperate with that authority on issues relating to the processing of personal data. The DPO is granted various rights by the GDPR including access to the company's data processing personnel and operations, a direct reporting line to the highest management level and protection from dismissal/penalisation for performing their function.

Before the GDPR comes into force, your organisation should assess whether it will be required to appoint a DPO, and if so appoint a suitable candidate. The DPO should be selected on the basis of professional qualities and expert knowledge of data protection law. If none of your employees are appropriate for the role then you can contract a third party who offers professional DPO services. If your organisation is part of a group of undertakings, or a group of public authorities, then the group may in certain circumstances appoint a single DPO.

It is important to bear in mind that if your organisation is not strictly required to formally appoint a DPO, it will be a good idea in most cases to designate someone to take responsibility for data protection compliance.

REGULATORS

Supervisory Authorities

Supervisory Authorities (or National Data Protection Authorities) such as the ICO in the UK, will continue to exist under the GDPR, as under the DPD. There is one supervisory authority per member state and each exists as an independent public authority. Their functions are extensive, and essentially encompass all tasks related to the protection of personal data.

In line with the drive for consistent application of data protection law, the GDPR provides that businesses carrying out cross border processing should be primarily regulated by the supervisory authority in which it has its main establishment (the "*Lead Supervisory Authority*"). This is the "*one-stop-shop*" mechanism which was a key element of the vision behind the GDPR (though it has been watered down from the original proposals).

If your organisation carries out cross border processing it will be important to familiarise yourself with the rules that determine who is the lead supervisory authority.

European Data Protection Board (EDPB)

The GDPR creates a European Data Protection Board, composed of senior representatives from each member state supervisory authority and a (non voting) representative of the European Commission. This Board will supersede the Article 29 Working Body and will have a greater role in providing guidance and advice, and ensuring consistent application of the Regulation.

ENFORCEMENT

One of the most significant aspects of the GDPR is the tougher sanctions regime.

Remedies

Individuals have the following rights against Data Controllers and Data Processors:

- to lodge a complaint with supervisory authorities where their data have been processed in a way that does not comply with GDPR;
- right to an effective judicial remedy where a competent supervisory authority fails to deal properly with a complaint;
- right to an effective judicial remedy against a relevant Data Controller or Data Processor; and
- right to compensation from a relevant Data Controller/Data Processor for damage resulting

from breach of GDPR.

It is well worth noting that individuals can bring claims for non-pecuniary loss (e.g. distress), not just compensation. The potential for group actions to be brought is also facilitated.

Both individuals and entities have the right to appeal to national courts against a legally binding decision concerning them made by a supervisory authority.

Administrative Fines

One of the most significant developments in the GDPR is the power for Supervisory Authorities to impose hefty administrative fines on both Data Controllers and Data Processors for a wide range of infringements data protection law (even merely procedural infringements).

The following tiered approach is established, with the appropriate tier being determined by the nature of the infringement:

1) Fines of up to €10,000,000 (or in the case of undertakings, 2% of global turnover, whichever is higher); and

2) Fines of up to €20,000,000 (or in the case of undertakings, 4% of global turnover, whichever is higher).

A limited number of infringements fall into the lower tier, for example failure to notify a personal data breach. The majority of infringements are subject to the higher tier, including breach of the data protection principles and breach of the rights of data subjects.

This sanction regime is a big step up from the DPA, under which the highest potential financial penalty is £500,000.

Fines are discretionary, imposed on a case by case basis, and the Supervisory Authority must be satisfied that the fine is effective, proportionate and dissuasive. When deciding whether to impose a fine the Supervisory Authority must give consideration to wide range of factors including the nature, duration and gravity of the infringement, the level of damage suffered, the character of the infringement (whether negligent or intentional), the categories of personal data affected, and any aggravating or mitigating factors.

These fines heighten the need for organisations to run risk assessments to monitor their compliance, and prioritise necessary remedial action, especially in relation to high risk processing activities.

Other Sanctions

It is important to bear in mind that Supervisory Authorities have a broad array of other enforcement powers. Each Supervisory Authority has investigatory powers for instance to demand information from the Data Processor/Data Controller, to carry out data protection audits, and also corrective powers such as to issue warnings, reprimands, to order compliance with individual's rights, and to issue temporary or permanent bans on processing.

OUR RECOMMENDATIONS

Many organisations may be feeling justifiably overwhelmed by the GDPR, by the need to understand the reforms and make appropriate internal changes to ensure compliance. However, it is important to keep in mind that the GDPR's main principles mirror the existing law: it adds muscle to the skeleton created by the DPA. Accordingly, if you are currently compliant with the DPA then it should be a case of building on, and adjusting your current data protection policies, with a few new additions, rather than a radical overhaul.

Below are 10 suggested keys steps to prepare for the new data protection regime.

1) **Raising Awareness** – Make sure that decision makers and key management personnel are aware about the coming changes. It will be vital for this to be done in good time so that the potential impact of the GDPR can be assessed and responded to appropriately.

2) **Legal Basis for Processing** – Consider what data processing you undertake, identify the legal basis for such processing, and assess whether the legal basis is valid under the GDPR. This process should be documented to aid compliance with the Regulation's principle of accountability. You will bear the burden of proof for demonstrating that the legal basis is satisfied.

3) **Information held by you** – Document what personal data you hold, who your sources are and who you share it with. It may be necessary to conduct an information audit for these purposes.

4) **Individual Rights** – The rights of individuals have been extended and strengthened under the GDPR. You should expect individuals to enforce these rights and prepare accordingly. Check that your organisation's policies and procedures are consistent with all the rights protected by the GDPR, especially the new ones e.g. data portability and the right to be forgotten.

5) **Consent** – Review your current procedures for seeking, obtaining and recording consent. Review whether you need to make any changes in light of the heightened consent requirements in the GDPR. Ensure you have an effective audit trail for recording consent.

6) **Privacy notices** – information provided should be in clear and plain language, with your policies transparent and easily accessible. Audit your current privacy notices and policies to ensure they meet these requirements, and update them where necessary.

7) **Data Protection by Design** – the concept of data protection by design should be a central consideration going forward when developing new products, procedures or processing.

8) **Data Protection Officer** – Designate a DPO if you are required to do so under the GDPR. Even if the new regime does not expressly require you to make such an appointment, it may still be a good idea to designate someone to take responsibility for compliance with data protection law.

9) **Data Breaches** – Ensure you have clear policies and procedures to identify, assess, report and investigate personal data breaches. These policies should equip you to act quickly in response to breaches and make timely notification.

10) **Enforcement and Risk** – In light of the fortified enforcement regime, with the beefed up fines, you should identify any areas of non-compliance with the GDPR and prioritise remedial action. It is also a good idea to update your risk registers and review your insurance arrangements.