STEVENS&BOLTON

GENERAL DATA PROTECTION REGULATION AND DATA PROTECTION ACT 2018 OVERVIEW

The European General Data Protection Regulation (the "Regulation") came into force in all EU Member States on 25 May 2018, replacing the Directive 95/46/EC (the "Directive"). The Data Protection Act 2018 ("DPA 2018") supplements the Regulation with additional provisions specific to English law. As anticipated, the Regulation and the DPA 2018 have had a significant impact on businesses and this is likely to continue, even with Brexit.

WHAT IS THE EFFECT OF THE REGULATION?

Key features of the Regulation include:

- **Greater harmonisation:** the Regulation aims to introduce one set of data protection standards which apply in a uniform manner across all EU member states, which should be a more attractive model for businesses which operate globally.

Key features of the Regulation include: greater harmonisation, territorial scope and accountability

- **Territorial scope:** the Regulation has wide territorial application even for businesses outside of the EU. It applies to controllers and processors that have an establishment within the EU even if the processing takes place outside the EU. "Establishment" has a wide meaning. In addition, it applies to "controllers" and "processors" outside the EU if processing the personal data of data subjects in the EU, where the processing activities are related to services or goods that are offered to data subjects in the EU (whether or not provided for payment) or the monitoring of their behaviour within the EU. For example: simply providing a website, accessible in the EU, which enables goods or services to be ordered in a language or currency generally used in one or more member states may indicate that a controller or processor envisages offering goods or services to data subjects in the EU. This change marks a broadening of the previous position and impacts on many industries, including e-commerce companies and those that provide cloud computing services.
- **Accountability:** the general obligation for controllers to notify with the ICO is abolished in favour of more proactive accountability requirements for both controllers and processors. Controllers are required, in particular:

- to adopt internal policies and compliance procedures and demonstrate compliance with the Regulation;
- to implement privacy by design and default approach to processing;
- to implement appropriate security measures;
- where processing carries a high risk, to conduct risk assessments known as "Privacy Impact Assessments" and consult with the ICO before processing starts;
- depending on the type of processing, to appoint a data protection officer; and
- document their data processing activities and make their records available to the ICO upon request (some organisations with fewer than 250 employees will be exempt from this requirement).

Additionally, consents and privacy notices will need to be updated to take account of more detailed requirements to specify data retention periods and transfers outside the EEA.

The Regulation places a number of obligations directly on processors, including the responsibility to implement appropriate security measures when processing personal data on a controller's behalf

- **Processors:** the Regulation places a number of obligations directly on processors, including the responsibility to implement appropriate security measures when processing personal data on a controller's behalf (which was previously a contractual requirement). Certain of the accountability requirements, for example record-keeping requirements and the requirement to appoint a data protection officer in certain circumstances, also apply to processors and, in contrast to the position under the Directive, processors are liable to fines and other regulatory action. This is one of the major changes from the previous regime – see our separate note on this topic and the implications for processors.
- **Meaning of "personal data":** the definition of "personal data" captures all data from which a living person is identified or identifiable, and extends to online identifiers such as IP addresses and cookies when combined with other identifiers received by servers to identify the individual. The definition of sensitive personal data also now includes specific references to biometric data which uniquely identify an individual and genetic data.
- **Consent:** consent (if relied upon) must be "unambiguous" – or "explicit" for sensitive personal data, which reflects the previous position under the Directive. Consent still needs to be freely given, specific and informed and now must be demonstrated by an "affirmative act". Silence, pre-ticked boxes or inactivity are unlikely to be sufficient, whereas ticking a box when visiting a website or choosing certain technical settings may be. The burden of evidencing and proving consent falls firmly on the controller, so online service providers in particular will wish to consider how they will evidence and record data subject consent in each case.
- **Protection for children:** the Regulation includes provisions on how controllers process personal data belonging to children using their online services (e.g. email or social networking sites). Where relying on consent in the UK, parental or guardian approval will normally be required for children under 13 years old. Service providers may wish to consider what measures they have or will put in place to verify whether a parent has given or authorised consent.
- **Portability of data:** the Regulation includes several specific rights for data subjects and the controller is responsible for compliance. For example, data subjects have the right to receive in a structured and commonly used and "machine-readable" format, and to transmit to a new controller, a copy of personal data which they have provided to an existing controller. This applies to data which is electronically processed on the basis either of consent or contractual necessity. Where technically feasible, the controller may be required to transmit the personal data directly to the other controller. The right is designed to allow data subjects to move their personal data seamlessly between online providers. The Article 29 Working Party (a body composed of representatives of the national data protection authorities amongst others) has issued guidelines and FAQs which explain how controllers can comply with this requirement.
- **Right to be forgotten**: data subjects have a "right to be forgotten", or "right to erasure", entitling a data subject to require the controller to erase personal data "without undue delay", though the right is balanced (amongst other things) against the public interest and

the right to freedom of expression. This is broader than the right confirmed by an ECJ ruling in 2014 to apply to search engine providers to remove outdated personal data from search listings, and is something that businesses across all industries should be aware of. If the data are publicly available (e.g. can be found and accessed through a search engine), the controller must take reasonable steps to inform third party controllers processing the personal data that the data subject has requested links and copies of the data to be erased. The controller must communicate the fact that it has been erased to any recipients of the data, unless it would be impossible or involve disproportionate effort to do so.

- **Data subject access requests:** controllers are not permitted (initially) to charge an administration fee (previously £10), but may charge a reasonable fee if asked to provide more than one copy of the personal data to the data subject. The request must normally be dealt with within one month (shorter than the previous 40 days) and the type of information that must be provided is broader.
- **Data protection officers:** as part of a drive for greater accountability, public bodies and businesses whose core activities consist either of the regular, systematic and large-scale monitoring of data subjects, or the large-scale processing of sensitive personal data or personal data relating to criminal convictions and offences, must appoint data protection officers. In the case of a group of companies, it is sufficient to appoint a single officer for the group, although sufficient access to that officer may need to be guaranteed for each group company. The data protection officer must be able to perform their duties independently and must not be dismissed or penalised for doing his or her job. The Article 29 Working Party has issued guidelines and FAQs which clarify when a data protection officer needs to be appointed, who can carry out the role and what it entails.
- **Data breach notification:** controllers have mandatory breach notification obligations, but there are materiality thresholds (the application of which are for the controller to assess in each case). Breaches which pose a high risk to the individuals must be notified to the regulator and (unless steps have been taken to encrypt the data or otherwise minimise the risk) to the affected data subjects. This can be done by a public communication, if it would involve disproportionate effort to contact each individual. If the breach is lower risk, only a notification to the regulator is necessary. However, if the breach is unlikely to result in risk for the individuals, there is no requirement to notify at all, though the breach and the remedial actions need to be documented. Controllers must advise the regulator "without undue delay" and within 72 hours of becoming aware of a notifiable breach, but information can be provided in phases if necessary. In contrast, notifications to data subjects must be carried out without undue delay but there is no deadline. Processors do not have to notify the regulator or data subjects, but must notify controllers of any breach without undue delay.

The maximum fine for controllers and processors for breaches of the Regulation is EUR 20 million or 4% of annual worldwide turnover in the previous year, whichever is higher.

- **Data transfers**: transfers to non-EEA countries are still restricted, but there are some changes that the Regulation has introduced. The Commission will continue to maintain a list of "adequate" countries to which transfers will be permitted but, following the *Schrems* case, the EU-US Safe Harbour scheme which permitted transfers to companies in the US was replaced by the EU-US Privacy Shield (the US has not yet been deemed adequate). Controllers and processors may make use of existing measures such as binding corporate rules and standard contractual ("model") clauses, but transfers may also be permitted according to certifications and codes of conduct issued under the Regulation, provided these are backed up by binding commitments of the non-EEA controller or processor to apply appropriate safeguards. There are still a number of derogations (including where the data subject having been informed of the risk has given "explicit" consent to the transfer).
- **Penalties:** the maximum fine for controllers and processors for breaches of the Regulation is EUR 20 million or 4% of annual worldwide turnover in the previous year, whichever is higher – for breaches of more minor provisions of the Regulation, the maximum fine is the greater of 2% of annual worldwide turnover or EUR 10 million. The previous penalty in the UK was £500,000 so the position under the Regulation represents a massive increase in potential sanction. In addition, controllers and processors could be liable to

compensate data subjects who suffer "material or non-material damage" as a result of their non-compliance.

- **One stop shop:** in an attempt to streamline the system of supervision of cross-border processing, controllers and processors will normally only have to deal with the regulator in the country of their single or "main" establishment, a concept which is defined in the Regulation. However, other national regulators would be able to deal with complaints that either only relate to establishments in their member state or substantially affect data subjects just in their member state. Businesses with pan-European operations will want to ascertain the country of their main establishment in order to work out who their lead regulator will be and should consider the relevant Article 29 Working Party guidelines and FAQs.

DATA PROTECTION ACT 2018

The DPA 2018 and the Regulation are designed to be read in conjunction with each other, with the DPA 2018 introducing the concept of the "applied GDPR".

The DPA 2018 was implemented into English law on 25 May 2018 and supplements the Regulation. The DPA 2018 and the Regulation are designed to be read in conjunction with each other, with the DPA 2018 introducing the concept of the "applied GDPR" (being the GDPR as applied and supplemented in the UK by the DPA 2018).

Broadly, the DPA 2018 replaces the Data Protection Act 1998 and is intended to achieve the following:

- **Implement the GDPR into English law**: despite the direct effect of the Regulation, the DPA 2018 also incorporates the Regulation into English law.
- **Provide UK-specific derogations in certain areas**: member states are permitted to derogate from the Regulation in certain areas, and the DPA 2018 provides various UK-specific provisions, including:
    - clarification of certain terms and concepts used in the GDPR, and their application in the UK, including (for example) additional detail around the processing of special categories of personal data and data relating to criminal convictions and offences;
    - UK-specific exemptions from the GDPR in certain (limited) scenarios, such as for national security and defence purposes;
    - specifics relating to law enforcement and intelligence services processing in the UK;
    - detail around the continued role of the Information Commissioner in the UK under the new regime, including its general function, competence in relation to courts, obligation to prepare certain codes of practice (e.g. with respect to data sharing) and ability to charge fees;
    - the enforcement process with respect to data protection legislation in the UK, including guidance, information and assessment requirements, enforcement and penalty notices, the appeals process and further detail on what constitutes an offence relating to personal data in the UK.

BREXIT

The Regulation and DPA 2018 will be relevant to businesses in the UK irrespective of Brexit. In particular, this is because:

- **The 'no Brexit' position is that the Regulation and DPA 2018 continue to apply**: until such time as the UK leaves the EU, the Regulation will continue to take direct effect in the UK, as supplemented by the DPA 2018.
- **The Regulation may continue to apply in certain Brexit scenarios**: the form that Brexit takes will likely have an impact and may mean that the Regulation continues to apply in the UK. For example, the deal documented in the EU Withdrawal Agreement and accompanying Political Declaration (the deal negotiated with the EU by the Theresa May administration) provides for a transition period in which the UK would be subject to EU data protection law until 31 December 2020 with a view to harmonisation thereafter. Whilst the status of that deal remains uncertain, it is possible that any subsequent deal may take a similar approach to data protection law. There are also other situations where

the Regulation may continue to apply directly in the UK (e.g. where the UK remains part of the single market), and it continues to be a watching brief as to whether the form of Brexit is such that the Regulation can continue to apply directly in the UK.

- **UK as a 'third country'**: if the form of Brexit means that the Regulation will not apply in the UK directly post-Brexit, the European Commission has confirmed that, once the UK leaves the EU, it will become a 'third country' for the purposes of personal data transfers to and from the EU and for the appointment of representatives. The current general assumption is that the UK will seek an adequacy finding from the Commission in respect of the data protection regime in the UK, thus ultimately continuing to enable the flow of personal data into and out of the UK without the need for additional measures (e.g. model clauses). Any finding of adequacy is likely to be premised on the compatibility (i.e. material similarity) of UK data protection law with the Regulation (see next bullet).
- **The DPA 2018 will continue to apply in the UK post-Brexit**: the DPA 2018 envisages harmonisation between UK data protection law and the Regulation post-Brexit, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 create a 'UK GDPR' in English law, comprised of the Regulation (in its form on exit day) merged with the DPA 2018. This is with a view to the adoption into English law of equivalent data protection standards to those in the Regulation and potentially paving the way for an 'adequacy' finding by the Commission.
- **Territorial scope of the Regulation**: even if the Regulation does not apply directly in the UK or is not otherwise implemented into English law, due to its extraterritorial scope, certain UK businesses that process the personal data of EU citizens will need to comply with the Regulation in any event (see the section on Territorial scope above).

KEY CONTACTS

For further information about any of the issues raised in this guide, please contact:

Beverley Flynn
Partner
T: +44 (0)1483 734264
M: +44 (0)7769 708486
E: beverley.flynn@stevens-bolton.com

Gary Parnell
Partner
T: +44 (0)1483 734269
M: +44 (0)7738 695666
E: gary.parnell@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road
Guildford, Surrey, GU1 4YD
Tel: +44 (0)1483 302264
Fax: +44 (0)1483 302254
DX 2423 Guildford 1
www.stevens-bolton.com

\41849v7