STEVENS&BOLTON

AN OVERVIEW OF THE UK'S DATA PRIVACY REGIME

The EU has the EU General Data Protection Regulation (EU 2016/679) (the "EU GDPR") which, until Brexit, was directly effective in the UK. Notwithstanding Brexit, the rules underpinning the UK's data privacy regime have remained to a large extent similar, albeit with some changes in terminology and detail. The UK's data protection regime is now underpinned by the UK General Data Protection Regulation (the "UK GDPR"), which is the UK's retained version of the EU GDPR.

The Data Protection Act 2018 ("DPA 2018") supplements the UK GDPR with additional provisions, as it did regarding the EU GDPR pre-Brexit, and the Privacy and Electronic Communications Regulations ("PECRs") also continue to apply. Data privacy compliance in the UK is overseen by the Information Commissioner's Office ("ICO").

The UK's data privacy regime may diverge from the European model in time, and there are ongoing government/ICO consultations in this area.

This note focuses on the current position in the UK, with an eye on future developments.

WHAT IS THE EFFECT OF THE UK GDPR?

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

Key features of the UK GDPR:

- **Territorial scope:** The UK GDPR applies to businesses "established" (which has a purposefully wide meaning) in the UK even if the processing takes place outside the UK. In addition, it applies to "controllers" and "processors" outside the UK where they are processing the personal data of data subjects in the UK, where the processing activities are related to services or goods that are offered to data subjects in the UK (whether or not provided for payment), or where data subjects' behaviour is monitored within the UK. For example, simply providing a website, accessible in the UK, which enables goods or services to be ordered in English, may indicate that a controller or processor envisages offering goods or services to data subjects in the UK.
- **Defining Controllers and Processors:**
    - **A controller** determines the purpose and means of processing the personal data, and is the main decision-maker when it comes to how the personal data is handled. It is possible to be a controller as a sole trader or self-employed individual, and companies, organisations, charities, associations, public authorities, volunteer groups, and any other kind of business or organisation of any size may also be controllers.

- **A processor** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. It does not control the processing that is being undertaken, but acts strictly on the instructions of the controller. Distinguishing between processor and controller roles can be difficult in practice, but often examples of those in processor roles are organisations providing services using information provided by a client, such as a payroll services provider, as it is usually acting on the instructions of its client, the controller, and not making any independent use of the personal data.
- **Joint controllers** is a concept whereby two or more controllers together decide on the purpose and means of processing personal data, i.e. they have the same or shared purposes. Controllers will not be joint controllers where they process the same personal data, but for different purposes.

- **Accountability:**
  - Controllers are required:
  - To adopt internal policies and compliance procedures and demonstrate compliance with the UK GDPR.
  - To implement privacy by design and to apply this approach by default 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.
  - Depending on the international elements of the organisation, to appoint an EU representative.
  - To document their data processing activities and make their records available to the ICO upon request (some organisations with fewer than 250 employees may be exempt from this requirement). Examples include:
- Privacy notices, one each for third parties, employees and recruitment
- Data processing registers
- Data controller registers
- Data breach registers
- Legitimate interest assessments
- Data privacy impact assessments
- Article 28 clauses with processors known as data processing agreements
- Data retention policies
- Model clauses for transfers of personal data abroad
- Transfer risk assessments

The UK GDPR 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

Privacy notices and other documentation are considered "live documents" and should be updated on a regular basis; e.g. to take account of any ongoing changes in data retention periods and transfers outside the UK.

- **Processors:** The UK GDPR 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. 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 processors are liable to fines and other regulatory action. Processors therefore continue to be responsible for their own compliance under the UK GDPR.
- **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 information to identify the individual. The definition of special personal data (known also as sensitive) also includes specific references to biometric data (which uniquely identify an individual) and genetic data, and additional rules apply to its processing.
- **Lawful basis for processing personal data**: A controller must have a valid lawful basis for processing personal data, and there are six possible bases under the UK GDPR, being:
  - Data subject consent.
  - Necessity for the performance of a contract.
  - Compliance with a legal obligation.
  - To protect the vital interests of the data subject (or other natural person).
  - Tasks carried out in the public interest or in the exercise of official authority.
  - Legitimate interests.

    Which basis is most appropriate will depend on the purpose of the processing and, generally speaking, the processing should be necessary for that particular purpose. If the purpose could reasonably be achieved by another means (e.g. through complete anonymisation), the controller will not have a lawful basis for its processing. The lawful basis relied upon should be determined and documented before the processing commences.
  - **Consent:** Consent must be "unambiguous" and must be "explicit" for sensitive personal data. It must be freely given, specific and informed and 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 need to consider how they evidence and record data subject consent in each case.
  - **Legitimate Interests:** In order to rely on this basis a controller must a) identify the legitimate interest, b) show that the processing is necessary to achieve this, and c) balance this against the individual's interests, rights and freedoms. This needs to be documented in a Legitimate Interests Assessment.
- **Protection for children:** The UK GDPR 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 need to consider what measures they need to take to verify whether a parent or guardian has given or authorised consent.
- **Portability of data:** 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 or personal data that is collected by the controller through observance of the data subject's activities (e.g. website tracking). 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.

- **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. 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:** Data subjects have a right to access their personal data and controllers are not permitted (initially) to charge an administration fee, but may charge a reasonable fee if a request is "manifestly unfounded or excessive" or if the data subject requests more than one copy of the personal data. The request must normally be dealt with promptly and as a backstop within one month, and the data controller has a duty to respond. Not all data requested must necessarily be provided to the data subject as there are exemptions in place; e.g. to protect the rights of other individuals, or where the personal data is being processed for the prevention or detection of a crime. However, the UK GDPR still places a high expectation on businesses to provide all relevant personal data wherever possible, and the ICO expects businesses to have well designed and maintained information management systems to assist with this. Responding to a data subject access request can therefore be time consuming and costly, and it is recommended that businesses have in place a procedure and relevant training for employees to assist in dealing with such requests accurately and within the statutory timescales.
- **Data protection officers:** As part of an overall focus on 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 special 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 their job.
- **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). Controllers must advise the regulator "without undue delay" and within 72 hours of becoming aware of a notifiable breach. There may be separate notifications to data subjects also which must be carried out without undue delay. Processors do not have to notify the regulator or data subjects, but must notify controllers of any breach without undue delay.
- **International data transfers**: The UK maintains a lists of "adequate" countries to which international data transfers (i.e. outside of the UK) will be permitted. This is kept under review and may in time diverge from the EU Commission's own adequacy decisions, on which the UK's list was originally based following Brexit. To transfer personal data to "non-adequate" countries, controllers and processors may make use of existing measures such as binding corporate rules and standard contractual clauses or model clauses ("SCCs"). In September 2021 the European Commission launched new SCCs for use within the EU, and as of March 2022 the UK has its own Addendum which works alongside the EU's new SCCs. However, the contractual requirements for international data transfers are complex, with the UK still using the EU's old SCCs in some cases, and we would recommend that advice is sought before permitting transfers to "non-adequate" countries.
    - **Data Transfers to the US**: The US has not been deemed "adequate" by either the UK or the EU. Following the *Schrems II* case, the EU-US Privacy Shield, which had previously been used as a means of permitting transfers to companies in the US, was deemed to not provide the levels of protection required for the safe transfer of personal data and was therefore invalid. A new deal between the EU and the US is currently under

negotiation, and this is expected to have an impact on the UK's approach going forwards.

The maximum fine for controllers and processors for breaches of the UK GDPR is £17.5 or 4% of annual worldwide turnover in the previous year, whichever is higher.

- **Penalties:** The maximum fine for controllers and processors for breaches of the UK GDPR is £17.5m or 4% of annual worldwide turnover in the previous financial year, whichever is higher. For breaches of more minor provisions of the UK GDPR, the maximum fine is the greater of £8.7m or 2% of annual worldwide turnover in the previous financial year.
- **Liability for compensation**: in addition to fines, controllers and processors that breach their obligations could be liable to compensate data subjects in certain circumstances. Where a controller and a processor are involved in the same processing and are responsible to a data subject for damage caused by the processing, either could be held liable for the entire damage. The party that had paid all the compensation would then need to consider claiming back from the other party a proportion of the amount paid (corresponding to the part of the damage for which the other party was responsible).

DATA PROTECTION ACT 2018

The DPA 2018 and the UK GDPR are designed to be read in conjunction with each other.

The DPA 2018 was implemented into English law on 25 May 2018, and it sets out the framework for data protection law in the UK. The DPA 2018 and the UK GDPR are designed to be read alongside and in conjunction with each other, with the DPA 2018 being amended following Brexit to reflect the UK's non-EU status (via the European Union (Withdrawal) Act 2018).

Broadly, the DPA 2018 supplements the UK GDPR by providing:

- Additional detail around the processing of special categories of personal data and data relating to criminal convictions and offences.
- Exemptions from the data protection obligations of the UK 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 regarding the role of the Information Commissioner in the UK, 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.

THE PECRS

The Privacy and Electronic Communications Regulations 2003 (PECRs) sit alongside the Data Protection Act 2018 and the UK GDPR within the UK's data privacy regime. The PECRs apply to i) any business which markets by phone, email, text or (in the rare instances of these still being used) fax, ii) those which use cookies or similar tracking technology, as well as iii) more specifically telecoms or other public electronic communications network providers or services. The PECRs cover:

- **Unsolicited marketing by electronic means**: the rules around when communications can be sent by which medium are detailed, but generally for individuals, consent will be required. When it comes to obtaining consent, the PECRs say that consent must:
  - Be freely given, specific and clear in order to be valid.
  - Cover the type of communication (i.e. whether by call, text or email) and the particular organisation doing the marketing.

- Involve a clear and positive action by the individual. Many businesses use a tick box consent mechanism by way of a positive action, but note that it must be clear to the individual what they're consenting to.

- **Not just individuals:** The PECRs also apply to business-to-business marketing, but generally speaking the rules are not as strict as those for marketing to individuals, and how they apply depends on the method of marketing and the type of business intended as the recipient of the marketing.

- **Use of cookies or similar tracking technology:** Put simply, businesses must tell people which cookies are being used on their websites or platforms, what these cookies are doing and why, and obtain individuals' consent to store such cookies on their device. Whilst the PECRs do not set out precisely what information should be provided or how, the ICO has issued guidance on how to inform individuals and correctly obtain their consent. Best practice in this area is frequently under review, and it is worth noting that these rules also apply to any technology which stores or accesses information on a users' device, such as apps or the Internet of Things.

- **The privacy of customers using communications networks:** This includes specific organisational and security requirements for public communications networks service providers (e.g. telecoms services), including ensuring that personal data can only be accessed by authorised personnel for legally authorised purposes, and requirements around the compilation of telephone or email directories.

- **New e-privacy regulation:** It should be noted that (pre-Brexit) the PECRs are due to be replaced by a new EU e-privacy regulation, but this has not been finalised. As and when the EU regulations are brought in they will not automatically form part of UK law, and it is unclear whether the UK will follow suit.

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

Charles Maurice
Partner
T: +44 (0)1483 406971
M: +44 (0)7557 677192
E: charles.maurice@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

DEPARTMENTAL\18505325v1