STEVENS&BOLTON

GENERAL DATA PROTECTION REGULATION - WHAT IT MEANS FOR PROCESSORS

The European General Data Protection Regulation (the "Regulation") came into force on 25 May 2018, replacing 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.

This note summarises the impact of the Regulation from a UK perspective on processors (those entities that process personal data on behalf of controllers), and on controllers who engage processors to process personal data on their behalf. The term "process" is very wide and includes the use, holding or disclosure of personal data. If you would like to read about the Regulation more generally and about the potential effect of Brexit on its implementation in the UK, please see our general briefing note on the General Data Protection Regulation.

The Regulation and DPA 2018 place a number of obligations on processors. As a result, processors may be liable for administrative fines and could be required to compensate data subjects for damage in certain circumstances.

WHAT HAS CHANGED?

The Regulation and DPA 2018 place a number of obligations on processors. This was not a feature of the Directive. As a result, processors may be liable for administrative fines and could be required to compensate data subjects (individuals whose personal data are being processed) for damage in certain circumstances. Broadly-speaking, the larger the scale and risk to a data subject from the processing of their personal data, the more onerous the processor's obligations will be.

It may be that businesses act as controllers in respect of their own personal data (for example, employee data) and processors in respect of certain other information (for example, customer information). In general, the distinction is that a controller determines the purposes for and manner in which personal data are processed, whereas the processor's role is limited to processing the personal data on the controller's instructions.

Where businesses act as processors, they will need to consider the enhanced requirements of the Regulation and adjust their policies and procedures accordingly.

KEY POINTS FOR PROCESSORS

Processors and controllers appointing processors may wish to consider the following key points:

- **Territorial scope:** the Regulation applies:
  - to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of where the processing takes place; and
  - to controllers or processors who are established outside of the EU, where the processing activities are related either to:
    - the offering of goods or services to EU data subjects; or
    - the monitoring of EU data subjects' behaviours within the EU.

Irrespective therefore of the data protection legislative landscape in the UK post-Brexit, processors falling in the second category above may still need to comply with the Regulation even if it does not form part of English law.

The Regulation requires processors to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Processors established outside of the EU who are engaged in more risky processing are required to appoint a representative in the EU.

- **Who can be a processor?** controllers must use processors who provide sufficient guarantees to implement and meet the appropriate technical and organisational measures and systems required by the Regulation. Processors may need to consider, for example, whether their IT systems are set up to deal with data subject requests (for example, that data can be erased or transferred to other providers – see our general GDPR briefing note which sets out some of the new data subject rights). Processors may be able to demonstrate their suitability by following approved codes of conduct or joining certification schemes published and made available under the Regulation and DPA 2018.
- **Data security:** the Regulation requires processors to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Those measures include, where appropriate:
  - the pseudonymisation and encryption of personal data;
  - the ability to ensure the ongoing
  - confidentiality, integrity, availability and resilience of systems and services processing personal data;
  - the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In deciding what measures to take, processors may take into account (amongst other things) the costs of implementation and the level of risk presented by their processing.

A processor must notify the controller of security breaches without undue delay.

- **Responsibility for sub-contractors:** a processor must not sub-contract its processing activities without the prior written authorisation of the controller. A processor must pass on the obligations under the processing contract to the sub-processor and will remain fully liable to the controller for the performance of the sub-processor's obligations. A processor must inform the controller if it intends to add or replace any sub-processors, so the controller has an opportunity to object.
- **Requirement to keep records:** a processor (and, where applicable, their representative) must keep records of the processing they undertake and other records, including details of the security measures taken, any transfers of data outside of the EEA and the controller(s) on behalf of whom they process personal data. Processor organisations with fewer than 250 employees ("SMEs") will be exempt from this requirement, unless the

processing is likely to result in risk to the rights and freedoms of data subjects, the processing is not occasional or the processing involves sensitive personal data or personal data relating to criminal convictions and offences. The records must be made available for the regulator (in the UK, the ICO) upon its request.

- **Requirement to appoint a data protection officer**: 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, will need to appoint a data protection officer with "expert" knowledge of data protection law and practices. The data protection officer's role involves (amongst other things) monitoring the business' compliance with its own policies, the Regulation and DPA 2018 and other applicable data protection provisions, and acting as liaison with the regulator and data subjects where necessary. The chosen individual could be either a member of the existing staff who has received special training or hired in specifically if is no one suitable for the position internally. The Article 29 Working Party (a body composed of representatives of the national data protection authorities amongst others) has issued guidelines and FAQs which clarify when a data protection officer will need to be appointed, who can carry out the role and what it entails.
- **Data transfers**: controllers and processors must provide adequate safeguards for data being transferred outside the EEA to countries which are not on the European Commission's adequacy list, for example by making use of existing measures such as binding corporate rules and standard contractual ("model") clauses or following approved codes of conduct or certification schemes issued under the new regime.

The maximum fine for a number of breaches of the Regulation (whether a controller or a processor) is EUR 20 million or 4% of annual worldwide turnover in the previous financial year, whichever is higher.

- **Penalties:** the maximum fine for a number of breaches of the Regulation (whether a controller or a processor) is EUR 20 million or 4% of annual worldwide turnover in the previous financial year, whichever is higher. For other breaches, the maximum fine is the greater of EUR 10 million and 2% of annual worldwide turnover in the previous financial year. For example, breaches of the data security obligations fall within the lower band (EUR 10m/ 2%), whereas breach of the data transfer requirements would be within the upper limit (EUR 20m/ 4%).
- **Liability for compensation**: in addition to fines, processors that breach their obligations could be liable to compensate data subjects who suffer "material or non-material damage" as a result. 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. However, this would not prevent a party that had paid the full sum from claiming back from the other party a proportion of the compensation (corresponding to the part of the damage for which the other party was responsible). The Regulation provides that controllers are liable for damage caused by processing which does not comply with the Regulation, whereas processors are only liable for damage caused by breaches of processor obligations specifically, or caused by processing that is outside, or contrary to the lawful instructions of the controller. A controller or processor would avoid liability, if it were able to prove that it was not "in any way" responsible for the event giving rise to the damage.
- **Processing contracts**: where a processor processes personal data on behalf of a controller, the Regulation requires there to be a contract between the controller and the processor which sets out the:
  - subject matter and duration of the processing;
  - nature and purpose of the processing;
  - type of personal data and categories of data subjects;
  - obligations of the processor including to:
    - process the personal data only on documented instructions from the controller;
    - ensure that persons authorised to process the personal data have committed

themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- take data security measures;

- observe the rules in relation to sub-contractors;

- assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;

- assist the controller in ensuring compliance with its own security obligations including in respect of data breaches and risk assessments;

- at the choice of the controller, delete or return all the personal data and copies to the controller after the end of the processing services, unless required by law to store the data; and

- make available to the controller all information necessary to demonstrate compliance with these obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

FINAL THOUGHTS

Although processors are directly liable and answerable to the regulator, given the potential size of fines, a controller may want to ensure that it is adequately protected from the acts and omissions of its processor. As a result, processors often face stringent obligations in their contracts with their controllers. That said, and again given the potential size of those fines, processors often look to focus more on limiting their contractual liability, and ensuring a number of the data protection obligations apply mutually.

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