Spring 2018

Business Matters
RENFREWSHIRE CHAMBER OF COMMERCE

DATA PROCESSORS BEWARE: WHAT THE GDPR MEANS FOR YOU

bto solicitors

With 25 May 2018 no longer just a distant thought, implementing the GDPR is, or should be, on the minds of all Data Controllers:

Who is the Data Controller and who is the Data Processor, according to the ICO?

Data Controller: *"... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed."*

Data Processor: *"...in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller."*

Examples of Data Processors could include cloud storage providers; marketing software and database providers; payroll providers; the company that shred your confidential waste etc.

The DPA placed the legal responsibility for the processing of personal data with the Data Controller, albeit the requirement to have a contract in place gave the Data Processor contractual obligations. Crucially, if anything went wrong it was the Controller who faced regulatory action from the ICO, and the Controller who was fined – see the case of Scottish Borders Council v the ICO where it was the Processor who put the papers in the recycling bin, but the Controller who remained responsible. The breach here was that Scottish Borders Council did not have an appropriate contract in place.

However, under the GDPR, Processors now have their own obligations. If you are a Processor, you could now be fined up to €10 million, or 2% of global turnover, if you are not compliant with these obligations. Read on to find out which areas of the GDPR apply to Processors as well as Controllers.

Contracts

Although there was a requirement for Controllers to have an appropriate contract in place under the DPA, the GDPR strengthens that obligation and provides a prescriptive list of what must be in that contract. As a Processor, you may have experienced Controllers asking you to sign up to new terms and conditions, or asking about your compliance with the GDPR. Remember that because these terms will reflect the GDPR terms below, with which you must comply, pushing back on these terms and conditions may result not only in lost contracts, but also in your organisation being in breach of the GDPR.

GDPR Requirements for Processors

Register of Data Processing: Data Processors must keep a Register of Processing Activities including:

- the name of the Processor and of each Controller on whose behalf the Processor is acting;
- the categories of processing that are being carried out
- any transfers of data to third countries or international organisations and the suitable safeguards that have been put in place;
- a general description of the security measures in place, where possible.

This information must be made available to the supervisory authority upon request.

Security Measures: Data Processors must implement appropriate technical and organisational measures to ensure data security. This is a risk based assessment and can include the consideration of pseudonymisation and encryption; regular reviews of system resilience; data availability; the ability to restore and recover lost data; and a process for regularly testing security.

Notification of Breaches: Processors must notify the Data Controller without undue delay (interpreted as immediately by the EU) on discovering a personal data breach. The definition of a personal data breach refers only to an incident where personal data is affected, and is not limited to simply unauthorised access, but also includes the accidental or unlawful loss or disclosure of data, as well as destruction or alteration of the data.

Laura Irvine, partner BTO

Data Protection Officer: Certain Processors will require to appoint a Data Protection Officer (an individual who does not make decisions about processing but who monitors and advises on compliance):

- Public authorities;
- those whose core activity consists of processing which requires regular and systematic monitoring of data subjects on a large scale; or
- those whose core activities involve processing special category data on a large scale

There are restrictions on who the Data Protection Officer can be. He or she cannot be the Chief Executive or Head of IT, for example, as they are likely to make decisions that would conflict with the DPO's advisory and monitoring role. This service can be outsourced.

Cross Border Transfers: Data Processors cannot transfer personal data outside the EU or to an international organisation

without there being arrangements in place to ensure an adequate level of protection in relation to that data. Some countries have been approved by the EU Commission, but if such an adequacy finding has not been made, then you must put other measures in place.

Representative in the EU: Data Processors established outside the EU, but who process the data of any person in the EU, are subject the GDPR and must appoint a representative within one of the Member States where the data subjects are located.

Data Protection Impact Assessments: Although Processors themselves are not obliged to conduct impact assessments, Data Controllers are if they embark on a new project and it is likely to be a high risk to the rights and freedoms of individuals involved. However, Processors are required to assist the Data Controller in carrying out such risk assessments.

Remedies against Processors
Judicial Remedies: The GDPR provides that all data subjects will have the right to an effective judicial remedy where they consider that their rights have been infringed as a result of any processing of their personal data which does not comply with the GDPR. This means that the Processor can be directly accountable to the data subject.

Compensation Claims: The data subject will also be able to seek compensation for material and non-material damage suffered as result of an infringement of the GDPR.

Fines: Processors can now also be fined by the ICO, as stated above.

Data Controllers and Contracts
There must be a written contract with a Data Processor and all contracts must include the following provisions:

- The Processor must only process the data on the instructions of the controller
- Anyone processing data on the authority of the Data Processor must be subject to a commitment to confidentiality
- Appropriate security measures are in place
- Permission is sought from the Data Controller to appoint a sub-processor
- The Controller is advised of any new sub-processor if permission has been granted in general terms in advance
- The Processor must assist the Controller to comply with data subjects' rights and reporting obligations in relation to data breaches
- To either return or delete the data once the processing has ended
- An obligation to provide the Data Controller with information for audit/ inspection purposes

The contract must also set out information about the processing that is to take place, including what data is to be processed and why. Controllers are also obliged to carry out due diligence in relation to Processors and to monitor compliance.

The above is a basic outline of the new obligations placed on Data Processors by the GDPR, and what you can expect from Data Controllers updating contracts. GDPR contracts are coming your way and it is essential that you take steps to commence implementation of the new GDPR requirements as soon as possible. BTO's experienced Data Protection team has clients who are Controllers and others who are Processors and we can assist you will all aspects of GDPR compliance.

Laura Irvine, Partner & Solicitor Advocate
E: lji@bto.co.uk
T: 0131 222 2939