Guidance: A Practical Guide to Data Controller to Data Processor Contracts under GDPR

The General Data Protection Regulation ("**GDPR**"), which comes into force on 25 May 2018, will introduce increased obligations for both data controllers ("**Controllers**") and data processors ("**Processors**"). One such obligation is the obligation on Controllers and Processors to enter into a legally binding contract governing the processing of personal data when a Processor is engaged to process personal data on the instruction of a Controller (a "**Data Processing Contract**").

This guidance note outlines in brief the context of the obligation on Controllers and Processors to enter into a Data Processing Contract under the GDPR, when you need to enter into a Data Processing Contract and the minimum provisions which should be included in such a Contract.

Obligation on Controllers and Processors under the GDPR to enter into Data Processing Contract

Currently, the Data Protection Acts 1988 and 2003 ("**DPA**") contain obligations on both Controllers and Processors engaged in the processing of personal data. The introduction of the GDPR will mean that the obligations on Controllers and Processors engaged in the processing of personal data will broaden and strengthen. Whether you are acting as a Controller or a Processor under the DPA or indeed, the GDPR, will be a question of fact which you will need to assess on a case-by-case basis. Processors, for example, must only process personal data on the documented instructions of a Controller. A Controller, on the other hand, defines the purposes and means of the processing of personal data. More information in respect of the roles of Controllers and Processors is available on the Data Protection Commissioner's ("**DPC's**") website.

One obligation under the GDPR is the requirement of Controllers and Processors to enter into a legally binding contract when a Controller engages a Processor to process personal data on its behalf. When engaging a Processor, the GDPR stipulates that Controllers are obliged to use only Processors which provide sufficient guarantees to implement appropriate technical and organisational measures to comply with GDPR and to protect data subject rights.

Controllers and Processors should be mindful that there are a number of other obligations which the GDPR imposes directly on Controllers and Processors (for example, record-keeping obligations, ensuring the security of data processing etc.). These direct obligations of the GDPR will apply to Controllers and Processors in addition to any contractual obligations which a Controller and Processor may be subject to under a Data Processing Contract. Similarly, if found in breach of the GDPR, Controllers and Processors may be liable to fines and other penalties under the GDPR in addition to (potentially) being in breach of any Data Processing Contract to which they are a party.

More information in respect of the impact on the GDPR on both organisations and individuals may be found on the DPC's microsite: www.gdprandyou.ie.

How are data processing contracts changing under the GDPR?

The DPA provide that a written contract should be entered into between Controllers and Processors when processing of personal data is carried out by a Processor on the instruction of a Controller. The DPC has previously provided guidance on what should be contained in these contracts.

Similarly, the GDPR requires that when a Controller engages a Processor to process personal data on its behalf, the Controller and Processor must enter into a legally binding contract governing this processing of personal data. One important change to this obligation is that the GDPR prescribes more provisions for inclusion in Data Processing Contracts. These mandatory provisions for inclusion in Data Processing Contracts under the GDPR are detailed below.

Who needs to enter into data processing contracts?

All Controllers who engage Processors to process personal data on their behalf are obliged to enter into a Data Processing Contract. This obligation extends to all Controllers and Processors including Controllers and Processors in both the public and private sectors.

Overview of mandatory provisions of Data Processing Contracts

Article 28 of the GDPR prescribes the provisions which must be included in a Data Processing Contract between a Controller and a Processor. A Controller and Processor should enter into a Data Processing Contract which must, at a minimum, contain the following details:

- The subject matter, duration, nature and purpose of the data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed; and
- The obligations and rights of the Controller.

A Data Processing Contract should also contain the following mandatory provisions:

- That the Processor will only process personal data received from the Controller on documented instructions of the Controller (unless required by law to process personal data without such instructions) including in respect of international data transfers;

- That the Processor ensures that any person(s) processing personal data is subject to a duty of confidentiality;
- That the Processor takes all measures required pursuant to Article 32 GDPR (Security of Processing) including but not limited to implementing appropriate technical and organisational measures to protect personal data received from the Controller;
- That the Processor obtains either a prior specific authorisation or general written authorisation for any sub-processors the Processor may engage to process the personal data received from the Controller. The Processor must further ensure that where a general written authorisation to the Processor engaging sub-processors is obtained, the Controller has the opportunity to object in advance to each individual sub-Processor to be appointed by the Processor;
- That any sub-processors engaged by the Processor are subject to the same data protection obligations as the Processor and that the Processor remains directly liable to the Controller for the performance of a sub-processor's data protection obligations;
- That the Processor assists the Controller by appropriate technical and organisational measures to respond to data subject rights' requests under the GDPR;
- That the Processor assists the Controller to ensure compliance with obligations under the GDPR in relation to security of data processing (Article 32 GDPR), notification of data breaches (Articles 33 and 34 GDPR) and data protection impact assessments (Article 35 and 36 GDPR);
- That, at the end of the data processing by the Processor and on the Controller's instruction, the Processor deletes or returns the personal data received from the Controller; and
- That the Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and that the Processor allows for and contributes to audits conducted by the Controller or a third party on the Controller's behalf.

Other provisions which may be included in data processing contracts

There are a number of other provisions which Controllers and Processors may wish to include in Data Processing Contracts which are not mandatory for inclusion under the GDPR.

Such provisions may include but are not limited to:

- Liability provisions (including indemnities);
- Detailed (technical) security provisions; and/or
- Additional cooperation provisions between the Controller and Processor.

Such additional provisions may be agreed between Controllers and Processors on a case-by-case basis.

What do you need to do prior to GDPR?

If you are a Controller who engages Processor(s) to process personal data on your behalf or if you are Processor who processes personal data on the instruction of Controller(s), you should ensure that you have a legally binding Data Processing Contract governing this data processing. You should also ensure that Data Processing Contract(s) to which you are a party are updated (if required) to contain, at a minimum, the provisions which are prescribed and mandatory under Article 28 of the GDPR.