



## *Flynn O'Driscoll Legal Update*

# ***General Data Protection Regulation Statutory Obligations of Data Processors***

With the imminent introduction of the General Data Protection Regulation (“**GDPR**”) on 25<sup>th</sup> May 2018, the scope of data protection has been noticeably widened in comparison to the outgoing Data Protection Directive and its implementing legislation and nowhere is this more obvious than in the new direct statutory obligations on data processors. Under the Directive, the data processor’s obligations were generally light, and they would only be subject to such obligations if they were imposed on them by way of contract. With this dramatic change in the law, Data Processors should be aware of the changes made by the GDPR in order to implement an appropriate strategy prior to the 2018 launch date.

For the purposes of the GDPR, a data processor is defined as any *“natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.”* These processing activities are normally carried out under the authority and instruction of the data controller.

### **Maintain Records of Processing Activities (Article 30 GDPR)**

Under the GDPR, data processors and their representatives are obliged to maintain records of all processing activities carried out by them on behalf of a data controller. These records should include the following details:

- The name and contact details of the data processor, its representatives and any relevant Data Protection Officer;
- The categories of processing carried out on behalf of each data controller;

- Details of any transfer to a country outside the EU or to an international organisation, if applicable; and
- Where possible, a description of the security measures implemented by the data processor.

### **Breach Reporting (Article 33 GDPR)**

The GDPR imposes stricter obligations on data processors in relation to the reporting data breaches and has adopted specific data breach notification guidelines which are binding upon data controllers. Processors will be required to



notify the relevant data controller of any breach without undue delay after becoming aware of it.

#### **Data Protection Officers (Article 37 GDPR)**

Data processors will be required to designate a Data Protection Officer where the processing is being carried out on behalf of a public body (except for courts), where the core activities of the data controller or processor consist of the processing on a large scale of special categories of data (race, political opinions, religious/philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) or personal data relating to criminal convictions and offences.

#### **Cross-Border Transfers (Article 44 GDPR)**

Transfers of personal data to countries outside of the EU may only take place where the transfer is to an Adequate Jurisdiction, or if the person exporting the data has put appropriate safeguards in place, as further set out in Article 49. An Adequate Jurisdiction is one which the European Commission has deemed to have an adequate level of data protection in place and includes countries such as Canada and Switzerland. Since the Safe Harbour framework was declared invalid, the Privacy Shield is the new framework for the protection of personal data which is transferred to the US and helps for the moment to bring greater legal certainty for businesses relying on transatlantic data transfers. Like the Safe Harbour framework, the Privacy Shield is a self-certification process, and remains subject to review and, as such, we expect it will be subject to change.

#### **Data Processing Agreements (Article 28 GDPR)**

In addition to the obligations imposed by the GDPR on data processors, as outlined above,

Article 28 of the GDPR explicitly states that the processing of data by a data processor must be governed by a contract between it and a data controller stating the nature and purpose of the processing, the types of personal data being processed and the obligations and rights of the data controller. In particular, the contract must state that the processor:

- processes the data on foot of instructions by the data controller, unless required to do so by law (in which case the processor must notify the data controller of such requirement);
- ensures that the people processing the personal data will keep it confidential;
- takes all measures required to ensure the security of processing under Article 32;
- respects the provisions of Article 28 when engaging any permitted sub-processor;
- assists the data controller in responding to data access requests;
- deletes or returns all personal data to the data controller at the end of the provision of services relating to processing; and
- makes available to the data controller all information necessary to demonstrate compliance with the obligations of Article 28.

#### **Get GDPR Ready**

- Identify the processing activities you or your organisation carry out and start keeping records of these;



- Consider whether you should appoint a Data Protection Officer;
- Ensure that you have sufficient procedures in place to appoint responsible people to identify data breaches and notify these to the data controller; and
- If you are a data processor, or engage the services of a data processor, it is important to be aware of and comply with these new rules.

*Should you have any queries arising out of the foregoing please contact Ciarán Ferry or any member of our [GDPR](#) team who will be happy to assist.*



**Ciarán Ferry**

---

E: [ciaranferry@fod.ie](mailto:ciaranferry@fod.ie)

P: 091 396540

**Dublin:**

1 Grants Row, Lower Mount Street,  
Dublin 2, Ireland

Phone: +353 1 6424220

Fax: +353 1 6618918

**Galway:**

Unit 23, Galway Technology Centre,  
Mervue Business Park, Galway, Ireland

Phone: +353 91 396540

Fax: +353 91 792649