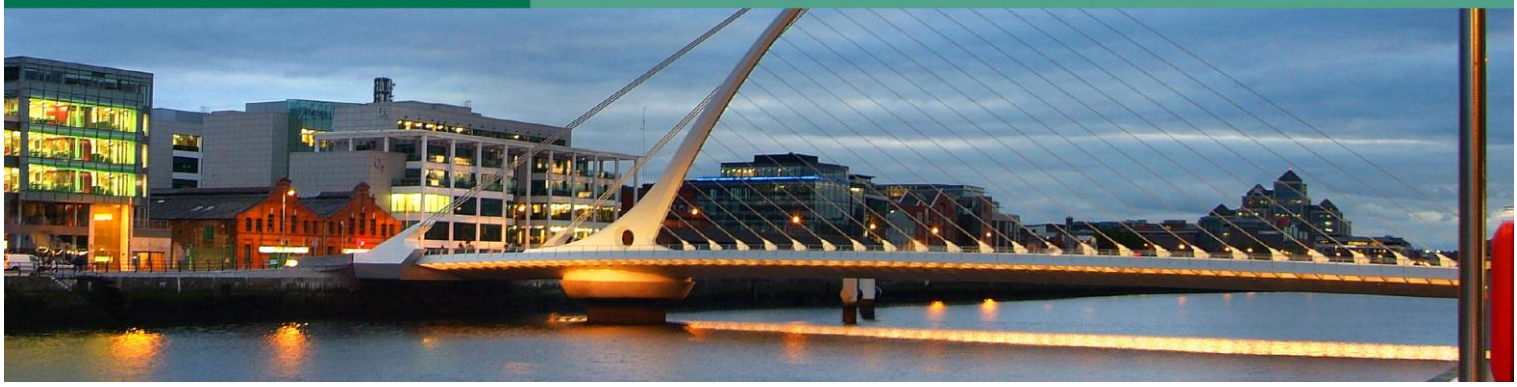

The European General Data Protection Regulation

The long-awaited European General Data Protection Regulation ("**GDPR**") entered into force on 24 May 2016 and, following a two year transition period, will apply from 25 May 2018[1]. The GDPR will replace Directive 95/46/EC (the "**Directive**") on which the Irish Data Protection Regime[2] is based. The GDPR will be directly applicable in all Member States without the need for implementing national legislation and it is hoped that the use of a Regulation will bring greater harmonisation throughout the European Union ("**EU**").

The GDPR does not fundamentally change the core rules regarding the processing of personal data which are contained in the Directive but rather seeks to expand and strengthen the rights of data subjects. The GDPR aims to make businesses more accountable for data privacy compliance and offers data subjects extra rights and more control over their personal data. This bulletin aims to summarise some of the main changes that will arise under the GDPR.

Consent

Obtaining consent for the lawful processing of personal data is more onerous under the GDPR. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. The data controller is required to be able to demonstrate that consent was given.

[1] The GDPR is accompanied by the Criminal Law Enforcement Data Protection Directive (2016/680) (which applies to the processing of personal data by law enforcement authorities) and must be implemented in all Member States by 6 May 2018 however it is not considered further in this article.
[2] The Directive was transposed into Irish law by virtue of the Data Protection Act 1998 and the Data Protection Amendment Act 2003 (the "**DPA**").

For further information on any of the issues discussed in this article please contact:

Breeda Cunningham
DD: + 353 (0)1 673 1846
breeda.cunningham@dilloneustace.ie

Michele Barker
DD: + 353 (0)1 673 1886
michele.barker@dilloneustace.ie

If consent is given in the context of a written statement/declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form using clear and plain language.

A data subject will have the right to withdraw his or her consent at any time.

Data Subjects' Rights

The GDPR largely retains and in some cases enhances existing rights of data subjects whilst also introducing new rights relating to (i) data portability, (ii) restricting processing and (iii) the right to be forgotten.

Data Portability

Under the right to data portability, data subjects have the right to obtain their data and to have their data transmitted to another data controller without hindrance where technically feasible. This right only applies to personal data provided to the data controller and does not therefore extend to personal data generated by the data controller.

Restricting Processing

The GDPR gives data subjects the right to restriction of processing in certain circumstances; i.e. a data subject can ask a data controller to restrict processing. This right to restrict processing replaces the right to blocking which is contained in the Directive.

Right to be Forgotten

Data subjects have the right to be forgotten without undue delay in certain circumstances including where the data subject withdraws his/her consent and there is no other legal ground for the processing. A data controller must provide information on the action it has taken to comply with the request to be forgotten without delay and in any case at least within one month of the receipt of the request from the relevant data subject.

Accountability and Governance

Under the GDPR, the data controller must be able to both comply with the principles relating to processing of personal data and also be able to demonstrate its compliance with the GDPR.

The data controller and data processor must implement appropriate technical and organisational measures to ensure that data is processed in a manner that ensures appropriate security and confidentiality of the personal data.

The GDPR also requires data controllers and data processors to retain records of their processing activities, which should be made available to the supervisory authority on request. Organisations with less than 250 employees are exempt from the record retention obligation unless the processing

it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the data controller must, prior to the processing, carry out a data protection impact assessment of the envisaged processing operations on the protection of personal data to evaluate, in particular, the origin, nature, particularity and severity of that risk. The precise meaning of 'high risk' has not yet been defined. The GDPR sets out some examples of circumstances which should be regarded as high risk processing however it is hoped that further guidance on this point will issue from the Article 29 Working Group in due course. Data controllers should consider the outcome of the assessment when determining the appropriate measures to be taken in order to demonstrate compliance with the GDPR.

International Data Transfers

The rules in the GDPR regarding the transfer of data outside the EEA are broadly similar to the current regime. The GDPR prohibits the transfer of personal data outside the EEA unless certain conditions can be satisfied. In particular, the consent exemption has been amended such that explicit consent is required where an entity wants to transfer personal data outside the EEA.

Territorial Scope

The GDPR expands the territorial scope of EU data protection law. The GDPR applies to both data controllers and data processers established in the EU regardless of whether the data processing takes place in the EU or not.

It also applies to the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate to:

- the offering of goods or services to such data subjects in the EU, irrespective of whether a payment of the data subject is required; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

Where data controllers and data processors outside of the EU are caught by the new territorial rules, they will need to designate a representative in the EU unless they can avail of an exemption[3]. This representative must be established in one of the Member States in which the data subjects,

[3] There is a limited exemption to the obligation to appoint a representative where the processing is occasional, is unlikely to be a risk to individuals and does not involve large scale processing of sensitive personal data.

whose personal data is processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

One Stop Shop

Under the GDPR, Member States must establish a supervisory authority that will be responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU. The supervisory authority must be independent of the Member State and appointed for a minimum period of four years. There will also be a European Data Protection Board made up of one member from each of the supervisory authorities of each Member State.

In respect of cross-border processing, the GDPR also introduces the concept of the "one stop shop" whereby a lead supervisory authority will be appointed to the data controller or data processer that will cooperate with the other national supervisory authorities, where relevant. A business that carries out cross border processing should be primarily regulated by the supervisory authority in which it has its main establishment. There are circumstances in which the lead supervisory authority will be required to co-operate and consult with authorities of other Member States.

Data Processors

The GDPR will apply directly to data processors. The GDPR also expands the list of provisions data controllers must include in their contracts with data processers. This is a significant change as data processers were largely exempt from regulation under the Directive. Some of the main obligations imposed on data processors by the GDPR include the following:

- the obligation to appoint a representative if not established in the EU;
- the obligation to ensure certain minimum clauses in contracts with data controllers;
- the obligation to keep a record of all categories of processing activities carried out in behalf of a data controller;
- the obligation to cooperate with the supervisory authority;
- the obligation to notify the data controller in the event of a data breach without undue delay;
- the obligation to appoint a data protection officer, where applicable; and
- the obligation to comply with the rules on the transfer of personal data outside of the EU.

Data processors will now be liable for material or non-material damage suffered by any person as a result of an infringement of the GDPR. However, a data processor's liability will be limited to the extent that it has not complied with the data processor obligations of the GDPR or where it has acted outside or contrary to lawful instructions of the data controller.

Data Protection Officer

Under the GDPR, certain data controllers and data processors will need to appoint a Data Protection Officer ("**DPO**"). The entities that are caught by the requirement to appoint a DPO are (i) public authorities, (ii) data controllers and data processors whose core activities consist of regular and systematic monitoring of data subjects on a large scale or (iii) data controllers and data processors which consist of large scale processing of personal data. A group of undertakings may appoint a single DPO provided that the DPO is easily accessible from each establishment. The DPO may be an employee of the data controller or data processor or fulfil the tasks on the basis of a service contract. Details of the DPO shall be published by the data controller or data processor. The DPO is responsible for monitoring compliance with the GDPR and must report to the highest level of management within an entity.

Data Breach Notifications

The GDPR requires data controllers to notify the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of a personal data breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the data controller does not notify the supervisory authority within 72 hours, it must give reasons for the delay. The GDPR sets out what should be included in the notification to the supervisory authority. The data controller must document any personal data breaches.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the personal data breach to the data subject without undue delay.

Under the GDPR, the data processor must notify the data controller without undue delay after becoming aware of a personal data breach.

Sanctions

The GDPR increases the sanctions which may be imposed on organisations that breach EU data protection law. Organisations may now be subject to administrative fines of up to €20,000,000 or 4% of annual global turnover, whichever is higher. Administrative fines may be imposed in addition to, or instead of, the supervisory authority's corrective powers. The GDPR sets out a list of factors for supervisory authorities to consider when deciding on whether or not to impose a fine and the level of any fine to impose.

Currently in Ireland, the Data Protection Commission (the "**DPC**") does not have the power to impost administrative fines for infringements of the data protection law. The DPC's power to issue fines under the GDPR will significantly increase the risk profile of data protection compliance/non-compliance.

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.