THE GENERAL DATA PROTECTION REGULATION EU: A SYNOPSIS

MAY 2018

SCOPE

1. Data Controllers and Processors

Once the General Data Protection Regulation (GDPR) becomes effective on 25 May 2018, it will apply to both controllers[1] and processors[2] of personal data[3] who are established in the European Union (EU).

The GDPR also applies to non-EU controllers and processors who process personal data of data subjects in the EU, if the processing involves either offering of goods or services (irrespective of whether a payment is required), or the monitoring of behaviour of data subjects in the EU (e.g. activities like tracking individuals on the internet to create profiles will be considered data processing).

Data controllers are required to ensure compliance and be able to demonstrate to regulators how they stay compliant with the data protection principles listed below when transacting business: -

- Lawful, fair and transparent processing;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation; and
- Security, integrity and confidentiality; and
- Accountability. [4]

Under the GDPR, data processors, are also for the first time, subject to their own list of direct statutory obligations making them directly subject to enforcement by supervisory authorities, fines and compensation claims by data subjects.

2. Data Processing Contracts between Controllers and Processors (Arts 28-33)

Article 29 GDPR specifically provides that where a data controller outsources some or all of its activities to a data processor then a formal data processing agreement must be agreed between the parties.

---

[1] GDPR Article 4(7): '**controlle**r' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

[2] GDPR Article 4(8): '**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

[3] GDPR Article 4(1): '**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
The GDPR also extends the definition of "**special categories of data**" (i.e. sensitive data) to include, in addition to data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, "genetic data" and "biometric data" with more stringent conditions in place for the processing of such data.

[4] See generally GDPR Article 5.

For example, the main elements that must an must include: -

- The subject matter and duration of the processing;
- Nature and purpose of the processing;
- Type of personal data;
- Categories of data subjects;
- Obligations and rights of the controller; and
- To process data only on the documented instructions from the controller.

If the processor acts outside the instructions of the controller (e.g. determining the purposes and means of processing)[5] they will be considered a controller and may be held directly liable for any harm caused as a result.

ORGANISATIONAL AWARENESS

Ultimately, if your business is in scope it is imperative that key personnel in your organisation are aware that data privacy law is going to change fundamentally under the GDPR and immediately start to factor this into future planning if you have not already. Areas that could cause compliance problems under the GDPR should be identified. Initially, data controllers should review and enhance their organisation's risk management processes, as implementing the GDPR could have significant implications for resources; especially for more complex organisations. Any delay in preparations may leave your organisation susceptible to compliance issues going forward.

ACCOUNTABILTY

In scope businesses, should make an inventory of all personal data that they hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the GDPR's accountability principle. The inventory will also enable businesses to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

COMMUNICATING WITH EMPLOYEES AND SERVICE USERS

Businesses should review all current data privacy notices alerting individuals to the collection of their data, as well as identifying any gaps that exist between the level of data collection and processing

[5] See GDPR Article 28(10).

your business engages in, and how aware you have made your customers, staff and services users of this fact.

Before gathering any personal data, current Irish legislation requires businesses who process personal data of their clients / customers to notify them of your identity, your reasons for gathering the data, the use(s) it will be put to, who it will be disclosed to, and if it's going to be transferred outside the EU.

Under the GDPR, additional information must be communicated to individuals in advance of processing, such as the legal basis for processing the data (discussed below), retention periods, the right of complaint where customers are unhappy with your implementation of any of these criteria, whether their data will be subject to automated decision making and their individual rights under the GDPR. The GDPR also requires that the information be provided in concise, easy to understand and clear language in communications with data subjects.

A LEGAL BASIS FOR PROCESSING

In scope businesses, should look at the various types of data processing they carry out, and identify your legal basis for carrying it out and documenting it.

There are six lawful basis for data processing permitted under Article 6(1) of the GDPR, which include:-

a) *the data subject has given consent* to the processing of his or her personal data for one or more specific purposes

This is the most common lawful basis relied upon by data controllers to legitimately process personal data. However, it is extremely important to note that consent to processing under the GDPR must be freely given by the data subject, and be specific, informed and unambiguous. This means, silence, pre-ticked boxes or inactivity will not be sufficient to constitute consent under the GDPR. An affirmative action is required from the data subject.[6] The data subject must also be informed of his / her right to withdraw their consent at any time. All and all, organisations must have a reliable method for recording consent to ensure they have an effective audit trail;

b) *processing is necessary for the performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) *processing is necessary for compliance with a legal obligation* to which the controller is subject;

d) *processing is necessary in order to protect the vital interests* of the data subject or of another natural person;

e) *processing is necessary for the performance of a task carried out in the public interest* or *in the exercise of official authority* vested in the controller; and

f) *processing is necessary for the purposes of the legitimate interests* pursued by the controller or by a third party.

[6] See GDPR Article 4(11).

Businesses will have to explain their legal basis for processing personal data in their privacy notice and when they answer a subject access request and they need to carefully consider how much personal data they gather, and why. If any categories can be discontinued, they should do so.

PRIVACY RIGHTS OF INDIVIDUALS / DATA SUBJECTS (Arts 12-23)

Organisations should review their systems and procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Rights for individuals under the GDPR include:

- subject access requests

  Data subjects have the right to request a copy of the personal data that a controller has on file. The controller has one month from receipt of an access request to respond, unless the request is deemed to be “manifestly unfounded or excessive" or a legislative provision provides that the data should not be provided);

- to have inaccuracies corrected;
- to have information erased;
- to object to direct marketing;
- to restrict the processing of their information, including automated decision-making;
- data portability;

PROCESSING OF CHILDRENS DATA

If the work of your business involves the processing of data from underage subjects, you must ensure that you have adequate systems in place to verify individual ages and gather consent from guardians.

The GDPR introduces special protections for children’s data, particularly in the context of social media and commercial internet services. The state will define the age up to which an organisation must obtain consent from a guardian before processing a child’s data. The GDPR and the Irish Data Protection Bill 2018 (soon to be enacted) defines a child as being anyone under the age of 13. It should be noted that consent needs to be verifiable, and therefore communicated to your underage customers in language they can understand.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA) AND DATA PROTECTION BY DESIGN AND DEFAULT (Art 25)

A DPIA is a new process established under the GDPR to increase data protection by systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It is envisaged as being a tool to allow businesses to identify potential privacy issues before they arise, and come up with a way to mitigate them. A DPIA can involve discussions with relevant parties / stakeholders. Ultimately, such an assessment may prove invaluable in determining the viability of future projects and initiatives.

The GDPR introduces mandatory DPIAs for those organisations involved in high-risk processing; for example where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

Where the DPIA indicates that the risks identified in relation to the processing of personal data cannot be fully mitigated, data controllers will be required to consult the Data Protection Commissioner (DPC) before engaging in the process.

It has always been good practice to adopt privacy by design as a default approach; privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. However, the GDPR enshrines both the principle of 'privacy by design' and the principle of 'privacy by default' in law. This means that service settings must be automatically privacy friendly, and requires that the development of services and products takes account of privacy considerations from the outset.

REPORTING OBLIGATIONS FOR DATA BREACHES (Arts 32-34)

Businesses should make sure that they have the right procedures in place to detect, report and investigate a personal data breach.

The GDPR brings in the concept of mandatory breach notifications, which will be new to many organisations. All breaches must be reported to the DPC, typically within 72 hours, unless the data was anonymised or encrypted. In practice this will mean that most data breaches must be reported to the DPC. Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned. Now is the time to assess the types of data you hold and document which ones which fall within the notification requirement in the event of a breach. Larger organisations will need to develop policies and procedures for managing data breaches, both at central or local level.

Processors are only obliged to report data breaches to controllers.

It is worth noting that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

DATA PROTECTION OFFICERS (Arts 37-39)

The GDPR will require some organisations to designate a Data Protection Officer (DPO). Business and organisations requiring DPOs include public authorities, and organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process what is currently known as sensitive personal data on a large scale.

Businesses, should therefore, consider whether they will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements. A DPO can be an employee or a contractor, but should have expert knowledge of data protection law.

CROSS BORDER PROCESSING IN THE EU AND THE 'ONE STOP SHOP' (Arts 4 and 56)

The GDPR includes the one stop shop (OSS) mechanism, which will be in place for data controllers and data processors that are engaged in cross-border processing of personal data within the European Economic Area (EEA).

The OSS will allow your organisation to deal with a single lead supervisory authority (LSA) for most of your processing activities.

Who your LSA is located will depend on your Member State of main establishment. The way you will identify your main establishment depends on whether you are a data controller or a data processor, but in general it will be helpful for you to map out where your organisation makes its decisions about data processing. The LSA for Ireland is the DPC.

Data transfers to countries outside the EEA are prohibited under the GDPR unless the third country has "appropriate safeguards" are in place.[7]

REMEDIES, COMPENSATION, LIABILITY, FINES & PENALTIES

Remedies

Data subjects have a right to an effective judicial remedy against a supervisory authority, data controller or a processor.[8]

Compensation

The GDPR also aims to provide data subjects with the ability to recover "full and effective compensation" for any damage suffered as a result of a breach of the GDPR. Accordingly, data subjects can sue both controllers and processors for compensation for pecuniary or non-pecuniary damage suffered as a result of a breach of the GDPR.[9]

Liability

The processor will only be liable insofar as it has failed to comply with its specific obligations under the GDPR or has acted outside of its instructions, but the level of liability of the processor can be increased subject to the terms of the data processing contract agreed with the data controller. However, if both a controller and processor are engaged in the same processing, and are both deemed to be responsible for the damage caused, they will be jointly and severally liable for the whole of the damage.[10]

Penalties

Depending on the type of infringement in-scope organisations can face administrative fines up to €10m or up to 2% of the total worldwide annual turnover of the preceding financial year (whichever is greater)[11] or administrative fines up to €20m or up to 4% of the total worldwide annual turnover of the preceding financial year (whichever is greater).[12]

---

[7] See GDPR Article 46.
[8] GDPR Articles 78-79.
[9] GDPR Article 82.
[10] GDPR Article 82.
[11] See GDPR Article 83(4).

Article 83(1) of the GDPR requires that fines be “effective, proportionate and dissuasive". Article 84 of the GDPR also provides that Member States can lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83. In this context the soon to be enacted Data Protection Bill 2018 seeks to establish the offences of;-

- Unauthorised disclosure by processor;
- Disclosure of personal data obtained without authority; and
- Offences by directors, etc., of bodies corporate.

Notably, the above named offences carry criminal liability punishable as a summary basis or on indictment.

[12] See GDPR Article 83(5).

CLIENT NOTIFICATION

Here at O'Grady's Solicitors we provide clear, practical and bespoke legal services to commercial, and private clients. So please do not hesitate to get in touch with our Managing Partner J. Kirby Tarrant on the contact details listed below, in order to arrange a consultation.

O'Grady's Solicitors,
4th Floor,
8-34 Percy Place,
Ballsbridge,
Dublin 4,
Web: www.ogradysolicitors.ie
Tel: 01-6613960
Email: ktarrant@ogradysolicitors.ie

Institute of Legal Research & Standards – Q6000 Gold – The Legal Quality Standard

Corporate INTL Global Awards 2018 – Editor's Choice Insolvency Law Firm of the Year in Ireland

Member firm of CLG, with offices in Amsterdam, Antwerp, Athens, Baltimore, Barcelona, Bologna, Cleveland, Duisburg, Durban, East Lothian, Edinburgh, Glasgow, Lisbon, London, Malta, Milan, Munich, Nicosia, Paris, Shanghai, Tel Aviv, Vienna, Warsaw, Zurich. www.clglaw.eu