**Data Protection**



A new European Union-wide framework known as the General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018.

The GDPR strengthens your rights and gives you much more control over your personal data. It also imposes more obligations on companies who control and process your data. You have more rights under the GDPR about how your personal data is handled and processed. Data controllers and processors are required to comply with the Regulation.

Under the GDPR, your personal data is data that relates to or can identify you either by itself or together with other available information. Examples of personal data include your name, phone number, bank details and medical history.



**You are a Data Subject when you are the person to whom the personal data relates. *Data Controllers* and *Data Processors* are organisations that collect or use your personal data.**

*As a data subject, you have the following rights:*

**Right to access data:** If you believe a person or organisation is processing personal data about you, you can request that they tell you whether they are processing this data. If your data is being processed you will be able to request a copy of that data to be sent to you. The controller will be able to charge a reasonable administrative fee for this. Under the current legislation, the fee cannot be more than €6.35, and must be provided within one month

**Your right to have your data rectified, restricted or erased:** For example if the accuracy of the data is in question, or the data is no longer needed for the purpose it was collected, you have the right to the above

**Your right to move or transfer your data:** The GDPR introduces the right to data portability. This means that you can request and receive personal data that you have previously provided to a controller in a commonly used and machine-readable format. The right also means that you can request one controller to transfer your personal data to another controller

**Your right to object to the use of your data:** The right to object means that you have the right to object to the processing of your data at any time - for example, to prevent your data being used for marketing purposes, including profiling. The controller must stop processing your data unless they can show that there are legitimate grounds or legal reasons for such processing that override your interests

**Your right to information about the protection of your data:** Data controllers must have appropriate measures to comply with your rights and must provide information to you in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

If a controller does not comply with a request from you, the controller must give you reasons for this and should inform you of your right to make a complaint to the supervisory authority. These rights will not apply where the data can no longer identify you.

*Obligations of Data Controllers and Processors:*

**The obligation to design appropriate processing systems:**For example, controllers should design their processes so that they collect only the data absolutely necessary for their purposes, and access to personal data should be limited to only those necessary for processing. Controllers may also temporarily anonymise personal data

**The obligation to use processors that meet the requirements of the legislation:** Where processing is to be carried out by a processor and not the controller, the controller must use only those processors who guarantee that their systems of processing meet the requirements of the Regulation

Examples of processors of his nature include payroll companies, accountants and market research companies, all of which could hold or process personal information on behalf of someone else. Cloud providers are also generally data processors

**The obligation to keep records:** Under the GDPR, any controller that has more than 250 employees, or that processes sensitive information, must keep a record of the processing activities under its responsibility, such as the purpose of data and erasure procedures. Processors must keep similar records. These records can be inspected by the Data Protection Commission on request

The obligation to keep data secure: The use of encryption passwords and back up data due to security risks.

**The obligation to report data breaches:** Under the GDPR, a controller must notify the Data Protection Commission of a personal data breach without delay where that breach is a likely to result in a risk to the rights and freedoms of the data subject. Notification should be made within 72 hours of the controller becoming aware of the breach. Data processors must notify the respective controllers if the processor becomes aware of a breach. The controller should also notify the data subject without delay

**The obligation to carry out data protection impact assessments:** Under the GDPR, when a controller intends to carry out high-risk processing they must first carry out a data protection impact assessment (DPIA). The Data Protection Commission will prescribe a list of the kind of processing operations that may be high risk

**The obligation to appoint data protection officers (DPOs):** Under the GDPR, data protection officers must be appointed by controllers and processors whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale or of special categories of personal data or data relating to criminal convictions and offences.

Functions include:

* Must provide contact details to the Data Protection Commission
* Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
* Must report directly to the highest level of management in their organisation

**Enforcement and Supervision of GDPR**

**(Under the**[**Data Protection Act 2018**](https://www.oireachtas.ie/viewdoc.asp?DocID=37646)**, the Data Protection Commission has replaced the Data Protection Commissioner.)**

**The Data Protection Commission will:**

* **Monitor and enforce the application of the GDPR**
* **Promote public awareness of the rules and rights around data processing**
* **Advise the Government on data protection issues**
* **Promote awareness among controllers and processors of their obligations**
* **Provide information to individuals about their data protection rights**
* **Maintain a list of processing operations requiring data protection impact assessment**

The Data Protection Commission has the power to order any controller or processor to provide information that the authority requires to assess compliance with the Regulation. It may carry out investigations of controllers and processors in the form of data audits, including accessing the premises of a controller or processor. It can order a controller or processor to change their processes, comply with data subject requests. The Data Protection Commission can also issue warnings to controllers and processors and can ban processing as well as commence legal proceedings against a controller or processor.

European Data Protection Board

The GDPR will introduce a new European data protection supervisory authority. The European Data Protection Board (EDPB) will be responsible for ensuring the GDPR is applied consistently across The European Union. It will issue guidelines and recommendations on the application of the Regulation. It will also advise the EU Commission on the application of the Regulation and any updates that may be required.

The EDPB is made up of the head of one supervisory authority of each member state and a European Data Protection supervisor.

Penalties

Penalties apply to both controllers and processors who breach the Regulation. There are different penalties, depending on the seriousness of the breach.

Serious infringements

For the most serious infringements (for example, not having sufficient customer consent to process data or violating the core of privacy by design concepts) organisations can be fined up to 4% of their annual global turnover or €20 million, whichever is greater.

Each member state may introduce further fines legislation, which will be enforceable within that state only.

Lesser breaches

Under the GDPR, organisations in breach of the Regulation can be fined up to 2% of their annual global turnover or €10 million, whichever is greater, for lesser breaches. Some examples of lesser breaches include: not having records in order, not notifying the supervisory authority and data subject about a breach or not conducting an impact assessment.

Task:

*Imagine you have been asked to teach First Years on this chapter. Create a One Page Summary (A3) for them on GDPR containing key points from this chapter. You are free to be creative and colourful. Make sure to upload onto OneNote when completed.*