17 Kildare Street, Dublin 2

Tel: 01 6622755

www.isme.ie

Email: info@isme.ie

ISME Guide to GDPR

Table of Contents

What is GDPR?

GDPR stands for the "General Data Protection Regulations"- a new EU wide regulation that will repeal and replace existing Data Protection Legislation across all EU Member States.

A review of current Data Protection Legislation at an EU level some time ago raised 2 significant concerns:

1) Technological advances had evolved to the stage that current Data Protection legislation was becoming increasingly outdated and unfit for purpose in such an ever-changing climate
2) A lack of standardisation in Data Protection Legislation across the EU was resulting in differing levels of protection being offered to EU citizens, and was creating difficulties for business' attempting to act cross borders to ensure compliance with all Data Protection legislation

GDPR was therefore implemented to reflect these concerns through:

- Simplifying the "patchwork" data protection legislation that exists across the EU, into a single set of rules that will be applicable in every Member State
- Providing Stronger Individual Rights for EU citizens
- Ensuring Individuals have greater control over their personal data
- Providing for stronger protection/sanctions against Data Breaches

GDPR was formally adopted at an EU level in 2016, and will become directly applicable across the EU on **25th May 2018.** From this date every organisation will need to ensure full compliance with GDPR.

Will GDPR apply to my company?

GDPR will apply to every company that:

- is based in the European Union and is **processing Personal Data** or;
- is based outside the European Union but is offering goods or services within the EU, or monitoring behaviour of individuals in the European Union

The term "personal data" has a wide interpretation, and refers to any information relating to an identifiable, living individual. This individual could be a customer, a supplier, an employee, a client etc. Examples of personal data could include but are not limited to:

- a name
- contact information (including contact number, email address, home address etc.)
- credit card information
- PPS number
- medical records
- IP address
- photos, videos or CCTV footage

- username or password
- biometric data

The “processing” of data also has a wide interpretation and could mean anything from merely collecting or storing data, to adapting, disseminating, disclosing, or destroying data.

Therefore, based on the above, it seems likely that almost every organisation will be affected by GDPR and changes to Data Protection Legislation.

Am I a Data Controller or a Data Processor?

Organisations may be a Data Controller, a Data Processor or both, GDPR has adopted these roles from current data protection legislation. For clarity, however, these roles have been defined below:

A Data Controller is the organisation that determines the purposes and manner in which personal data is to be processed. Most organisations will be Data Controllers.

A Data Processor on the other hand, is an organisation, agency of other body that processes data on behalf of the Data Controller. Examples could include, an accountant that works on company accounts but is not an employee of the company, outsourced IT support or any other service provider that has access to personal data of a customer or employee.

Both Controllers and Data Processors will have responsibilities under GDPR which will be explored further below.

Key GDPR changes:

While many of the core principles of Data Protection remain unchanged, GDPR will introduce some changes that may require many organisations to reconsider how they process personal data. The key changes are summarised below:

1) Expanded Territorial Scope: GDPR will apply not only to organisations based in the European Union, but also to any organisation that processes the data of EU citizens, regardless as to where they are based.
2) Increased rights of data subjects**:** While the same data subject rights that currently exist will continue to be recognised, a number of new rights will be introduced with GDPR. These include the right to be forgotten (i.e. the right of the individual to request the deletion of his/her data) and the right of data portability (i.e the right to request data be transferred from one service provider to another).
3) Appointment of a Data Protection Officer: In certain circumstances organisations may be required to appoint a Data Protection Officer. All public authorities; organisations whose core activity involves the processing of special categories of data on a large scale; or, organisations whose core activities consist of the regular and systematic monitoring of data subjects on a large scale must appoint a Data Protection Officer (DPO) who has sufficient expert knowledge to inform and advise on Data Protection and on GDPR compliance.

4) Direct obligations for Data Processors**:** For the first time, data processors will find themselves with direct statutory obligations under GDPR. They will have responsibility for maintaining a written **record of processing activities** carried out on behalf of a data controller and notifying the data controller of a data breach without undue delay. This record would usually be a separate document to the Data Protection Policy. They may also need to appoint a Data Protection Officer where their activities fall in line with the criteria outlined above. In addition, Data Processors could face sanctions and private claims by individuals seeking compensation in the event of a data breach.
5) Increased Data Subject Consent responsibilities: Where "consent" is relied upon, as the "legal basis" for processing data (more on this below), stronger requirements will exist under GDPR in relation to what consent can be relied upon. Consent under GDPR, must be freely given and explicit. In order to be explicit, there must be active agreement by the Data Subject (e.g. opt-in, rather than opt-out). Proof of consent must be recorded. The option to withdraw consent must be freely available and it should be as easy to opt-out or withdraw consent as it is to opt-in. Transparency in terms of what will happen with the data collected, how long the data will be retained, and who the data will be shared with is also stressed as a requirement under GDPR in order to rely upon the consent provided.
6) Stricter Data Breach Notification Requirements: Data Breaches must be notified to the Data Protection Commission (or equivalent in other EU member states) within 72 hours of becoming aware of the breach. Where the data breach is likely to result in a high risk to the rights of the individual, the data subject must also be informed "without undue delay".
7) Shorter timeframe for responding to Data Access Requests: Under GDPR the timeframe for responding to Data Access Requests will decrease from 40 days, to 1 month. In addition, in most circumstances there will no longer be an option for organisations to charge a fee of €6.35 per data access request.
8) Increased Sanctions: Fines of up to 4% of annual global turnover or €20 million (whichever is the greater) can be imposed for Data Protection Breaches. In addition, individuals will have the right to claim compensation against data controllers or data processors for damage resulting from a Data Protection Breach.

The GDPR Principles:

In its simplest form GDPR can be summarised by reference to the below guiding principles:

1) Lawful, fair and transparent processing: For every piece of personal data collected there must be a "legal basis" for the processing of this data.

   There are a number of "legal basis" upon which the processing of data may be justified:

   i) ***Consent***-where the data subject has consented to their data being processed

ii) ***Contractual necessity***: Where the processing of the data is necessary in order to fulfil a contract with the data subject (e.g. the processing of a credit card transaction to complete a sale with the data subject matter)

iii) ***Compliance with legal obligations***: Processing of the data is necessary in order to comply with a legal obligation (e.g. for tax purposes)

iv) ***To protect the vital interests of the data subject or another person*** (e.g. in a life/death situation- a patient arrives at hospital in a critical condition. The patient will not be in a position to give consent. No consent is required to access previous medical information as the data will be processed to protect the data subject's vital interests.

v) ***Public Interest:*** Where the processing is necessary in order to perform a task carried out in the public interest or you have to process the data to exercise an official authority

vi) ***Legitimate interests:*** The processing is necessary for your legitimate interest. This right is limited however, by the requirement to consider the protection of the individuals personal data. Where these rights are not compatible, the data subject's right to protect their personal data will override the right to process data for a legitimate interest. As such, it is recommended, where possible to rely on another legal basis rather than legitimate interests.

2) Purpose Limitation: There must be specific purpose for the processing of data. Data must not be processed for any further reason that is inconsistent with the original purpose. For example, an email address that is initially collected for the purpose of fulfilling a contract cannot then be used to advertise to the data subject.

3) Data Minimisation: Personal data collected must be kept to a minimum. Data should be adequate, relevant and limited. If it is found that irrelevant or unnecessary data has been collected a process should be put in place to erase the excess data

4) Data Accuracy: Every effort should be made to ensure data is accurate and kept up to date. A process should be in place to rectify any inaccurate data

5) Storage Limitation: Data should be retained for no longer than is necessary. This may be outlined in legislation for some data (e.g. tax/employment law records). Where retention periods are not outlined in legislation, careful consideration should be given to how long it is reasonably necessary to retain data and the data subject should be aware of how long their data will be retained for.

6) Integrity and Confidentiality: Sufficient protections should be in place to protect personal data from loss, destruction, unauthorised access/disclosure or alteration.

7) Accountability: Each organisation should be capable of demonstrating commitment to protecting the data they process. Sufficient procedures should be place to demonstrate such a commitment.

8) Privacy by Design: The General Data Protection Regulation mandates organisations to embed Privacy by Design into the development of new initiatives involving the use of personal data. Consciously considering and planning for the personal data you want to use, the purpose for which you want to use it and how to do this legitimately greatly reduces the chance of discovering at a later stage that embedding privacy is technologically challenging, expensive or even impossible. The approach to achieving an efficient Privacy by Design implementation consists of three steps:

    i) ***Identify and understand***: In order to tailor privacy measures to an organisation's operations, it is important to firstly understand in detail your organisation's design processes.

    ii) ***Evolve***: Once the processes and ways of working are fully understood, specific privacy measures should be designed to fit this current way of working

    iii) ***Establish***: Implement the measures into your design processes and train employees involved in those processes to ensure the measures are understood and executed correctly.

What steps should I take to comply with GDPR?

While it's not possible to provide a prescriptive course of action, given the internal complexities of each individual organisation, in general compliance with GDPR can be broken down into 3 separate yet interlinked stages:

1) The preparation stage**:** The preparation phase includes gaining an understanding of the general principles of GDPR and understanding how these interact with the work performed within your organisation.

    The priority in this phase must be understanding where there are weaknesses in your current data protection approach and putting plans in place to address these weaknesses.

    In the preparation stage the below steps are recommended:

    i) **Educate** Senior Managers and Key Stakeholders as to what to expect under GDPR. In addition, anybody who handles or has access to Personal Data should be educated as to how GDPR will interact with their role. Signing up to a GDPR training event is recommended at this stage.

ii) **Identify** the personal data you hold by creating a Data inventory. This Data Inventory should outline what data you process, the legal basis for processing this data, how it is being processed (i.e. what use is the data being put to); who has access to the data; how long the data is being retained ; and whether the data is being transferred or shared with any 3rd party. It may be useful to get assistance from other departments to assist with this Data inventory as every department will interact with data in different ways.

iii) **Analyse** this data inventory to determine where the weaknesses lie in your current process. Identified weaknesses could be as simple as:

a. Data being retained for longer than is reasonably necessary
b. A lack of or insufficient consent to process data
c. More data than is reasonably necessary is being collected
d. Too many people having access to certain information
e. Information being left on office desks overnight
f. Confidential documents not being locked away

iv) **Prepare** an implementation plan to correct any weaknesses. Again, you may need to include other senior managers, key stakeholders, or other employees who handle personal data in this stage. Allocate tasks as necessary to a relevant stakeholder.

2) The Action Stage: This is the stage in which you put your implementation plan into practice. If, due to financial difficulties, or resource shortages you are unable to action all tasks at once, you may need to prioritise based on importance and/or risk.

Simple actions that you may need to take could include:

a. Developing new processes to ensure data is only retained for as long as is necessary
b. Reissuing consent sheets to data subjects
c. Deleting any data that is deemed to be excessive
d. Ensuring proper security measures are in place to protect data (e.g. encryption, confidential documents are locked away in a secure location, employee training on cyber security)
e. Get an Incident Response Plan in place to ensure you can deal with a Data Breach within the outlined timeframes
f. Review and update your Data Access Request Procedures
g. Restricting access to data, only to employees who have a genuine requirement to view/use that data

The steps you need to take will be very much dependent on your own business and what weaknesses you have uncovered in your own processes. The action plan should be reviewed regularly to ensure you remain on course to execute your plans before the May deadline.

3) The Maintenance Stage: Unfortunately, your obligations under GDPR will not automatically cease on 25th May 2018. As data processing is likely to be an ongoing practice, your obligations will therefore also be ongoing.

   Care should be taken to conduct regular reviews of the procedures that have been put in place as a result of GDPR to ensure they remain fit for purpose.

   Any major changes to data processing must be reviewed with GDPR in mind.

   Where new data is processed (say for example you install CCTV within your workplace), this should be included in your data inventory to ensure it remains accurate over time.

   In addition, if you do commence processing of new data, you may need to consider whether you should conduct a **Data Privacy Impact Assessment**. Under GDPR, Data Impact Assessments are now mandatory for High Risk Processing Projects i.e. where

data processing “is likely to result in a high risk to the rights and freedoms of natural persons”. Data that reveals a data subjects racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership or the processing of biometric, genetic and health data are likely to fall within the meaning of the above.

To assist you in preparing for GDPR we have included some useful templates and resources in the Annex’s below.

Contents:

Annex 1: Data Inventory Template

What data do we collect?	Why do we collect it?	How did we collect it?	What is our legal basis for collecting?	Do we need their consent to collect?	If yes, do we have their consent to collect?	Where do we store this data?	Who has access to this data?	How long are we retaining this data?	Identified Problems

Annex 2: Implementation Action Plan

Area of concern	Task	Task Owner	Priority	Deadline	Comments

Priority Levels:	
1	Immediate action required
2	Action required within set timeframe
3	Action required prior to GDPR deadline (25th May)
	Completed

Annex 3: GDPR Checklist

Checklist: Are you prepared for GDPR?:

General

Have you educated yourself as to what changes GDPR is bringing about (e.g. by attending a GDPR training/information session)?

Are you aware of exactly what data you collect and process?

Have you educated your staff in relation to how GDPR will impact on their role?

Have you an internal procedure in place to deal with Data Access Requests?

Lawful, fair and transparent processing

Do you have a legal basis for collecting all data?

Where consent is relied upon is the consent adequate under GDPR?

Was the consent freely given?

Was the consent informed (i.e. was the data subject aware of the purpose for which it was required)?

Can you prove consent if required to do so?

If the consent you currently hold is not adequate under GDPR, have you re-sought consent?

Is a process in place to allow for the withdrawing of consent?

Purpose Limitation

Is data only used for the purpose for which it was originally collected?

Data Minimisation

Do you only hold data that you genuinely require and is relevant?

Where irrelevant data has been identified, has a process been put in place to erase?

Data Accuracy

Can you be sure data that you have collected is accurate and up to date?

If not, is a process in place to ensure that these data is updated?

Is a process in place to ensure personal data is kept up to date going forward?

Is there a process in place for ensuring necessary changes can be made without delay?

Annex 3: GDPR Checklist

Storage Limitation

Is data only being retained for as long as is necessary?

Do you know what types of data have legislative retention periods?

For data that is not subject to a legislative retention period, have you given careful consideration to how long it will be retained for?

Are data subject aware how long their data will be retained for?

Is a process in place to ensure there is no unnecessary duplication of data?

Integrity and Confidentiality

Is a process in place to prevent loss of data?

Is a process in place to prevent unintended/unauthorised destruction of data?

Is a process in place to prevent unauthorised access/disclosure of data?

Is a process in place to prevent unintended/unauthorised alteration of data?

Is data only accessible by those who require access to it?

Have you accessed the risks involved with the data that you collect and put a process in place to mitigate these risks?

Do you have a Data Security Policy in place?

Do you have an incident response policy in place?

Accountability

Have you collated a Data Inventory outlining a complete list of all data you collect?

Do you have a Data Protection Policy in place?