Defradar Co.

GDPR

GDPR Implementation Guide

Table of Contents

[**1.** **Introduction** 2](#_Toc503866644)

[**1.1 The format of the Regulation** 3](#_Toc503866645)

[**1.2** **Definitions** 3](#_Toc503866646)

[**1.3.** **Principles** 4](#_Toc503866647)

[**1.4** **Lawfulness** 4](#_Toc503866648)

[**1.5** **Consent** 5](#_Toc503866649)

[**1.6** **Rights of the data subject** 6](#_Toc503866650)

[**1.7** **Data Protection Officer** 6](#_Toc503866651)

[**1.8** **Data protection impact assessments** 7](#_Toc503866652)

[**1.9** **Codes of conduct and certification** 7](#_Toc503866653)

[**1.10** **International transfers** 8](#_Toc503866654)

[**1.11** **Supervisory authorities** 8](#_Toc503866655)

[**1.12** **European data protection board** 8](#_Toc503866656)

[**1.13** **Remedies, liability and penalties** 9](#_Toc503866657)

[**2.** **Preparing for the GDPR** 9](#_Toc503866658)

[**2.1** **Secure management commitment** 9](#_Toc503866659)

[**2.2** **Plan your project** 10](#_Toc503866660)

[**2.3** **Define Roles and Responsibilities** 11](#_Toc503866661)

[**2.4** **Communication, awareness and training** 12](#_Toc503866662)

[**2.5** **Personal Data Inventory** 13](#_Toc503866663)

[**2.6** **Rights of the Data Subject** 14](#_Toc503866664)

[**2.7** **Data Protection Impact Assessments** 15](#_Toc503866665)

[**2.8** **Prepare for Personal Data Breaches** 15](#_Toc503866666)

[**2.9** **Collate records of processing** 16](#_Toc503866667)

[**2.10** **Review international transfers** 17](#_Toc503866668)

# **Introduction**

The General Data Protection Regulation (GDPR) was approved by the European Commission (EC) on 27 April 2016 and becomes law on 25 May 2018. It replaces the previous EC legislation which dealt with data protection which was the Data Protection Directive of 1995. One of the major differences between the GDPR and the previous law is that the **GDPR is a *Regulation***rather than a *Directive*. This means that it automatically becomes law in each of the countries that make up the European Union without each of these countries needing to create their own, individual laws (in contrast with the previous Directive where, in each of the member states, a separate Data Protection Act had to be passed by the relevant state legislative body to enact it).

Whilst the emphasis is often on the rights of the data subject when discussing the GDPR, it’s important to remember that the EC is also trying to make it easier for organizations to share personal data and “oil the wheels” of business within the EU, so it’s not as one-sided as often thought. However, there are a number of important things to realize about the GDPR before we get into the detail.

Firstly, it concerns the personal data of EU citizens wherever that data is held. This means that if your organization is not based in the European Union but has customers (or suppliers or other parties) within it whose data you hold, the GDPR applies to you.

Leading on from this, it means that if your organization doesn’t look after that data in the way the GDPR requires, your organization may be subject to the penalties that the Regulation allows. These penalties are a step change from previous legislation and in serious cases, they are designed to hurt.

Thirdly, if you do experience a breach of personal data, you have no choice but to tell the relevant supervisory authority about it. There are some caveats on that which we will come to later, but keeping a serious data breach to yourself is no longer an option.

But the mainstay of what the GDPR is about is forcing organizations to take the protection of the personal data of EU citizens seriously.

## **1.1 The format of the Regulation**

The GDPR document itself is eighty-eight pages long and consists of two main parts:

***Recitals*** – 173 numbered paragraphs that lay out the principles and intentions of the Regulation; if you like, the background.

***Articles***– the 99 sections that set out the detail of the Regulation – **this is the part that must be complied with.**

## **1.2 Definitions**

The Regulation provides a definition of twenty-six of the relevant terms, including the following (*GDPR Article 4 – Definitions*):

*(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;*

*(2)* ***‘processing’*** *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

*(7)* ***‘controller’*** *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;*

*(8) ‘****processor’*** *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

*(11)* ***‘consent’*** *of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

## **1.3. Principles**

The GDPR establishes a number of principles that underpin the legislation and are outlined using the following terms (with our quick summary given after each):

1. ***Lawfulness, fairness and transparency***– keep it legal and fair; say what you’re going to do with the data in clear terms
2. ***Purpose limitation*** *–* don’t do more with the data than you said you would
3. ***Data minimisation*** *–* don’t collect more data than you need
4. ***Accuracy*** *–* keep it up to date and deal with inaccuracies as soon as possible
5. ***Storage limitation*** *–* don’t keep the data for longer than necessary
6. ***Integrity and confidentiality*** *–* keep the data safe while you have it
7. ***Accountability*** – be able to show that you’re complying with the principles above

If you keep all of these principles in mind at all times, you’re unlikely to fall foul of the GDPR.

## **1.4 Lawfulness**

For the processing of personal data to be lawful, it must meet at least one of a number of criteria, and an important first step in considering your processing activities is to clearly establish which of the criteria applies in any given situation.

In essence, the criteria to choose from with regard to the lawfulness of the processing are as follows:

1. The data subject has consented to it
2. It’s needed to perform a contract between your organization and the data subject, or to see whether a contract can happen
3. You legally have to do it
4. You’re protecting the vital interests of the data subject
5. It’s in the public interest
6. It’s for your legitimate interests – as long as it doesn’t affect the data subject’s rights and freedoms

So, whilst consent is an important aspect of the GDPR, it’s not the only way in which collecting and processing personal data can be lawful. In fact, you may find that a significant proportion of the personal data your organization holds and processes doesn’t require consent; instead it is required for lawful purposes such as providing support to customers (contractual), paying employees (contractual/legal) or dealing with the tax authority (legal). The process of obtaining and maintaining consent may involve changes to business processes and systems so it is a good idea to make sure there is no other lawful basis on which processing can take place first.

## **1.5 Consent**

If you believe that your processing is lawful because you have the data subject’s consent, then you must be able to prove it. You can’t hide the consent wording in amongst other contractual ramblings and expect to get away with it either. It must be in an “*intelligible and easily-accessible form, in clear and plain language” (GDPR Article 7, paragraph 2)* otherwise the consent doesn’t count and your processing could be judged to be unlawful.

Once given, the consent can be withdrawn at any time by the data subject and this must be as easy to do as it was to give it in the first place. A child must be at least sixteen years of age to be able to give consent (younger if a member state decides so, with a lower limit of thirteen) otherwise parental consent must be obtained.

## **1.6 Rights of the data subject**

The GDPR establishes a set of rights that the data subject can exercise and which the controller holding their personal data must react and respond to, generally within a month.

* **The right to be informed**
  + being told what data will be collected, why, by whom, for what purpose and where the data will go
* **The right of access**
  + being able to see personal data that are being held about the data subject
* **The right to rectification**
  + getting the data corrected if they are wrong or inaccurate
* **The right to erasure**
  + having personal data removed when they are no longer necessary
* **The right to restrict processing**
  + pausing the processing of the data if there are grounds to do so
* **The right to data portability**
  + obtaining the data in a transportable form and moving it to an alternative processor
* **The right to object**
  + stopping the data from being processed
* **Automated decision making and profiling**
  + having a human involved in important decisions

These rights follow on from the principles that we discussed earlier and are aimed at ensuring that personal data is processed fairly and transparently and that the data subject can do something about it if this doesn’t happen.

## **1.7 Data Protection Officer**

Depending on your organization and what it does with personal data, you may or may not need a data protection officer. You will have to designate one if:

* You’re a public authority or body
* You monitor data subjects on a large scale
* Large volumes of special category data are involved

Data protection officers may be part-time, may be shared across organizations and may be external resources or services. They must remain independent and their contact details must be freely available, especially to data subjects.

The data protection officer is the main contact with the supervisory authority and is likely to get involved when key issues of data privacy and protection are addressed within the organization, such as during data protection impact assessments.

The data protection officer will need to know a reasonable amount about data protection law in order to fulfil the role.

## **1.8 Data protection impact assessments**

In order to establish a culture where data privacy is “baked in” to new processes and systems, rather than added as an after-thought, the GDPR requires that data protection impact assessments be carried out where the risks involved to data subjects are reasonably felt to be high. This process involves understanding the personal data involved and addressing likely risks through the use of appropriate controls, so that proactivity, rather than reactivity, is the order of the day.

## **1.9 Codes of conduct and certification**

The regulation makes provision for member states, industry bodies and other organizations to create relevant codes of conduct and certification schemes that can be used to encourage and demonstrate compliance. It’s early days for such schemes, but they are likely to increase in popularity and availability as time goes by, so it’s well worth keeping eye on what’s happening in your country and industry.

## **1.10 International transfers**

Sending the personal data of European citizens outside of the European Union raises questions over how well the data will be protected and the GDPR places restrictions on how this may be done. To be helpful, the European Commission regularly decides which countries it trusts to look after EU personal data and publishes a list of those deemed to be acceptable. Currently, it’s a small list so you may need to look at the other ways to meet the GDPR if you need to do international transfers.

Other ways to get approval are:

* A legally binding agreement (public bodies only)
* Binding corporate rules
* Using standard clauses in your contract
* Signing up to an approved code of conduct or certification scheme

If you’re going to use binding corporate rules, be aware that they have to be approved by the relevant supervisory authority and that can take a while. There are a few get-outs (or “*Derogations*” as the GDPR calls them) for small, infrequent transfers so it may be worth checking the list in Article 49 if time is not on your side.

## **1.11 Supervisory authorities**

Each country within the EU will have a supervisory authority which is responsible for overseeing the operation of the GDPR in that country. Generally, these already exist and will not change. However, if your organization is outside of the EU but wishes to process the data of EU citizens in several countries, you will need to choose the most appropriate supervisory authority to act as the lead for your organization.

## **1.12 European data protection board**

The GDPR establishes the European Data Protection Board to oversee the application of the Regulation in the members states. Each supervisory authority has a seat on the Board, together with the head of the European Data Protection Supervisor. The Board will produce an annual report to tell us how well it’s going.

## **1.13 Remedies, liability and penalties**

And so we come to the teeth of the Regulation; the fines that can be levied for non-compliance with the GDPR are certainly larger than those for the Directive it replaces. The actual amounts demanded will depend upon a wide variety of factors, including the personal data involved, how hard the culprit organization tried to protect the data, how much they co-operated with the investigation and, most importantly, the specific article(s) of the GDPR they are judged to have contravened.

Fines allowable are up to **2% of global turnover** or **ten million euros** for lower level infringements and up to **4% of global turnover** or **twenty million euros** for more serious cases.

Data subjects can lodge a complaint with the relevant supervisory authority directly themselves or may use the services of a not-for-profit body active in the field of data protection.

# **Preparing for the GDPR**

## **2.1 Secure management commitment**

Before embarking on a project to achieve compliance with the GDPR it is very important to secure the commitment of top management. This is probably the single most significant factor in whether such a project (and the ongoing operation of the implemented processes afterwards) will be successful.

The first questions top management are likely to ask about the project are probably:

* What are the requirements we must meet?
* How much will it cost?
* When does it have to be in place by?

Probably the most important point is that compliance is not optional and the potential fines are big. Senior management support for the project may be demonstrated by publishing a letter/memo similar to the **Executive Support Letter** we have already provided as an example.

The accompanying workbook **Compliance Evidence** shows you how the various documents included in our report, map onto the requirements and what other evidence may be appropriate to show compliance. This may help when deciding whether a requirement is met or not.

In order to quantify how much work may be involved in complying with the Regulation, a **GDPR Gap Assessment Tool** is provided.

This summarises the key points of the relevant sections of the Regulation in question form and is intended to give you a reasonable idea of where your compliant and non-compliant areas are.

Roughly two thirds of the articles in the GDPR **are aimed at bodies** other than an organization trying to comply so they aren’t really requirements that you will need to worry about; these cover tasks such as the setting up of the European Data Protection Board, certification schemes and the rules that the supervisory authorities in each member state must follow.

## **2.2 Plan your project**

Having secured top management commitment, you will now need to plan how to achieve GDPR compliance. Even if you’re not using a formal project management method such as PRINCE2® we would still recommend that you do the bare essentials of defining, planning and tracking the implementation effort as a specific project.

We have provided a template **Project Initiation Document (or PID)** which prompts you to define what you’re trying to achieve, who is involved, timescales, budget, progress reporting etc. so that everyone is clear from the outset about the scope and management of the project. This is also useful towards the end of the project when you come to review whether the project was a success. Having written the PID, try to ensure it is formally signed off by top management and that copies of it are made available to everyone involved in the project so that a common understanding exists in all areas.

**Documents/Templates provided and nice to have:**

* GDPR Preparation Project Plan - provided
* GDPR Compliance Project Initiation Document (PID)
* GDPR Documentation Log

## **2.3 Define Roles and Responsibilities**

It’s important to establish from the start who is going to do what, both within your initial project to comply with the GDPR, and for the long-term protection of the personal data that you hold. The provided document ***GDPR Roles Responsibilities and Authorities*** sets out various roles, including an information security steering group to oversee the way in which data protection is controlled, an information security manager and, most importantly, information asset owners who have the most day-to-day involvement with the data in question. If not already allocated, decisions need to be taken about who will fulfil these roles, including potential recruitment.

The only role that is explicitly mandated in the GDPR is that of the data protection officer (DPO). As we mentioned in 1.1.7 above, you may or may not need to appoint one of these. If you’re a public body there’s no decision to be made, but otherwise you may need to get views from different perspectives within the business about whether you handle personal data on a scale that might be considered large. Your supervisory authority may be able to advise, either directly or via their website, if you’re unsure about this.

If you do need a DPO, you’ll need to decide whether to appoint internally, share a resource with one or more similar organizations, or to contract a service from a third party. Make sure the person that is appointed has the relevant competence, including “expert knowledge of data protection law and practices” (GDPR Article 37, paragraph 5).

One of the other points you may need to clarify is the supervisory authority that you will report into. For single-country organizations within the EU this should be a straightforward matter, but if your organization is based outside the EU or you operate across borders within the EU, there is a decision to be made about who will be your lead supervisory authority. Remember that you will need to be able to justify this choice, based mainly on where you do business the most, but there may be some flexibility if you have a preference.

## **2.4 Communication, awareness and training**

Once you’ve initiated your project and defined who will perform which role, there is a lot of value in raising general awareness about the GDPR and information security in general so that people know what it is and why it’s important. Audiences will include various stakeholders such as suppliers and contractors as well as employees and it’s useful to create a managed programme of communication so that it happens regularly.

You also need to identify the training needs of the people that are taking on the various roles involved in achieving compliance on an ongoing basis. This may be done by defining what competences are required and then conducting a comparison exercise by questionnaire to find the gaps; these may be filled via a combination of formal and informal training, including courses, webinars, seminars, books and, of course, reading the Regulation itself. Training may typically be needed in areas such as data mapping, data protection impact assessments and incident management.

**Documents/Templates nice to have:**

* GDPR Communication Programme
* GDPR Briefing Presentation
* GDPR Competence Development Procedure
* GDPR Competence Development Questionnaire
* Information Security Awareness Training
* Meeting Minutes

## **2.5 Personal Data Inventory**

Once your people are in place and they’ve received some training, the next step is to do some analysis of the way in which personal data is currently collected, stored, processed, transferred and disposed of within your organization. There are many ways to represent this but most come down to drawing diagrams of the flow and recording the relevant information on a spreadsheet.

You’ll need to involve the people who are responsible for collecting and processing the data on a daily basis to ensure that as full a picture as possible is obtained. You could do this by arranging workshops and using whiteboards and sticky notes, or you could send them a spreadsheet and ask them to complete it, or you could do both; whatever fits the culture of your organization.

What’s key here is to understand the main facts such as the data items that are being collected, for what purpose, by what method (e.g. on the website, face to face, paper form), where, how and for how long the data is stored and where it gets sent to. This will help in identifying any additional controls that need to be applied to it (such as encryption) and in establishing the legal basis under which it may be collected and processed (e.g. consent, contractual).

This Assessment/Guide provides some help with this exercise in the form of a Personal Data Asset Inventory which is intended to be used to record an overview of all of the personal data you hold, a **Personal Data Capture Form** for use when looking at individual projects or business processes, a template for a **Personal Data Mapping Diagram** if you prefer to use a diagrammatic representation of your data and a **Personal Data Flow Mapping Tool** which can be used to document the journeys the personal data take both within and outside your organization.

The overall approach you decide to take regarding data retention can be reflected in the Records Retention and Protection Policy.

**Documents/Templates nice to have:**

* Personal Data Asset Inventory
* Records Retention and Protection Policy
* Personal Data Mapping Procedure
* Personal Data Capture Form
* EXAMPLE Personal Data Capture Form
* Personal Data Mapping Diagram
* EXAMPLE Personal Data Mapping Diagram
* Personal Data Flow Mapping Tool
* EXAMPLE Personal Data Flow Diagram

## **2.6 Rights of the Data Subject**

Making sure you allow the rights of the data subject to be exercised without hindrance is an important factor in GDPR compliance, and one which may attract the attention of the supervisory authority if not done properly. Although we provide a form within the Assessment, the most effective way to allow the data subject to access and maintain their personal data is likely to be via some form of portal that the user can log in to via the Internet and do it directly themselves.

Similarly, standard forms may be provided via such a portal for requests such as objections and processing restrictions. You will need to make sure you have the appropriate workflow behind the forms to ensure they are logged correctly, processed by the right people within the required timescales and that the identity of the requester is confirmed.

Some requests will require decisions to be made and sometimes these will not be straightforward, so having a clear process and roles will be important – see the **Data Subject Request Procedure** in the provided Templates.

You will also need to consider the best way to communicate your privacy notice to the data subject, making sure that it covers the information required by the GDPR. We peovide a procedure and a planning form for this purpose. Again, the best ways to do this will depend upon how you interact with your data subjects e.g. via the Internet, telephone, face to face.

**Documents/Templates provided and nice to have:**

* Privacy and Personal Data Protection Policy - provided
* Data Subject Request Procedure - provided
* Data Subject Request Register
* Data Subject Request Form
* Privacy Notice Procedure
* Privacy Notice Planning Form

## **2.7 Data Protection Impact Assessments**

This is a relatively new area for many organizations, but one which is clearly mandated by the GDPR. New projects and significant changes to existing processes will need to carefully consider the impact on personal data as part of their assessment and planning, with appropriate controls put in place, based on a fair assessment of risk. If you have a projects process, then this will need to be added to it; the GDPR states that this is necessary only where there is a high risk, but you may find that it is a good idea to perform these assessments as a matter of course for every project.

A process and supporting documents is provided as part of the Templates. These include a **Supplier GDPR Assessment Procedure** and accompanying form which should be used to fill in the gaps in your knowledge of how your suppliers store, process and protect the personal data you are the controller for.

**Documents/Templates provided and nice to have:**

* Data Protection Impact Assessment Process- provided
* Data Protection Impact Assessment Questionnaire
* Data Protection Impact Assessment Workbook
* Data Protection Impact Assessment Report
* Supplier GDPR Assessment Procedure
* Supplier GDPR Assessment Form

## **2.8 Prepare for Personal Data Breaches**

The general consensus within the information security industry nowadays is not if an organization will suffer a security breach, but when; and it may already have happened, but you just don’t know about it. So, having an appropriate and tested incident management procedure is a must. The procedure offered as a template is a good starting point for incidents affecting not only personal data, but for a range of information security events, including denial of service attacks and ransomware.

The GDPR insists that your supervisory authority be told about known breaches that represent a high risk to data subjects and is specific about the timescales and the information that must be provided. We provide a notification procedure, form and register which should help to speed things up if the worst does happen.

**Documents/Templates provided and nice to have:**

* Information Security Incident Response Procedure – will be provided in the next training
* Personal Data Breach Notification Procedure - provided
* Personal Data Breach Notification Form
* Personal Data Breach Register

## **2.9 Collate records of processing**

Your supervisory authority could at any time ask to see records of the processing of personal data that you carry out, so it’s a good idea to be clear from the outset about where this information is to be found. We suggest keeping a spreadsheet of the main items of information, but you also need to be aware of the records such as logs and audit trails that exist at a lower level, reflecting the detail of what was done when.

The full picture for GDPR purposes will consist of a wide variety of items such as data protection impact assessments, privacy notices, subject request registers, data mappings and risk assessments, which together reflect how seriously the protection of personal data is being taken within the organization. This will become particularly important in the event of a data breach when the supervisory authority comes to decide the level of penalty that might be appropriate.

**Documents/Templates provided and nice to have:**

* Record of Processing Activities
* Compliance Evidence - provided

## **2.10 Review international transfers**

As well as protecting personal data within your own organization, you also need to think about where else you send it to, and how well it is protected there. This is an involved area and could either be a long, protracted affair or a simple, timely one, depending on how well the requirements of the GDPR are understood. The first step is to know what data you send where, and why. You then have various options available to apply to the transfer, depending on factors such as the destination, type of data and the purpose. We provide a **Procedure for International Transfers of Personal Data** to help you to pick your way through this puzzle and understand what needs to be done.