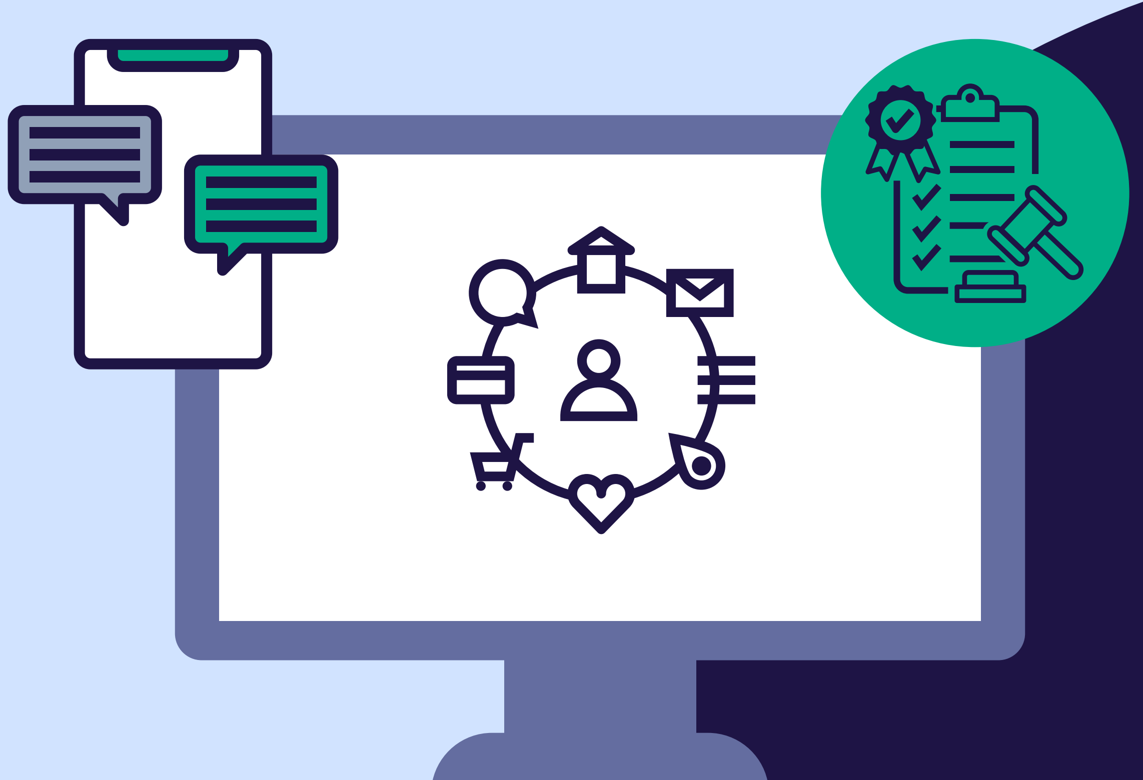
FAIRITY

## STEP BY STEP

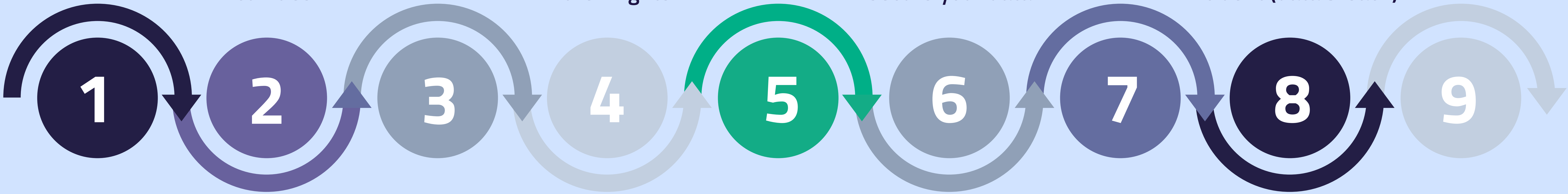
# GDPR COMPLIANCE GUIDE



# INTRODUCTION

The **General Data Protection Regulation (GDPR)** came into force in 2018 with the aim of strengthening users' rights and making companies that process personal data more accountable. You are confused by all these new regulations, uncertain about what is applicable for your organisation, and do not know where to start? Here is a **guide to help you understand the steps to be compliant with GDPR law**.

# STEPS



Identify all the activities involving personal data in your company

Create the Record of Processing Activities

Sort out your data

Make it easy for users to exercise their rights

Inform users you are collecting data

Secure your data

Appoint a Data Protection Officer

Be prepared for an incident (data breach)

Have control on third-party services that handle personal data on your behalf

# STEP 1

## Identify all the activities involving personal data in your company

To run your business, you have information about your customers or suppliers that identifies them: it is **personal data**.

> **Personal data**
>
> *Any information relating to an identified or identifiable natural person (so called ‘data subject’).*
>
> *It can be 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.*

You collect and process this data for different activities in your company such as recruitment, payroll, sales statistics, customer prospect management...

> **Process of personal data**
>
> *Any operation or set of operations which is performed on personal data. It can be collection, storage, consultation, use...*

Identify and meet the operational supervisors of several services likely to process personal data, analyse the website and **identify data collected** in online forms... Start by **making a list of all of these activities**.

STEP 2

# Create the Record of Processing Activities

Once you have identified the activities, you must **create a Record of Processing Activities** in accordance with Article 30 of the GDPR. This will give you an overview of all the personal data you process within your company.

For each activity, **create an excel sheet** with the following information:

- the **objective pursued** (the purpose - *e.g. for payroll*)
- the **categories of data** used (*e.g. for payroll: surname, date of birth, salary...*)
- **who has access** to the data (the recipient - *e.g. recruitment department, management...*)
- **how long** the data is kept (how long the data is useful from an operational point of view, and how long it is kept in the archives)

You can use this **template** (Excel format). All you have to do is fill it in!

# STEP 3
## Sort out your data

Now **check every record sheet** you created and make sure:

- that you only **process data that is necessary** for your activities

Processing only the necessary data will allow you to avoid dealing with more data and will better respect people's rights. For instance, it is not useful to know your client's gender, if you do not offer any services linked to this characteristic.

- you **do not process so-called 'sensitive' data** if you are not entitled to do so

> **Sensitive data**
>
> *Personal data subject to specific processing conditions, which must be processed with increased security. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.*

- that **only authorised persons** have access to the data they need
- you **do not keep the data longer** than necessary.

If any of these points are not met, **try to improve your procedures**: minimise data collection, redefine who should have access to which data in your company...

STEP 4

# Make it easy for users to exercise their rights

**Users have rights over their data that you collect**: right of access, rectification, opposition, information, erasure, portability and restriction of processing.

Give them the means to **contact you quickly and efficiently** to assert their rights. For instance, set up a telephone number, a form on your website, a contact email address, or a postal address for users to send their requests.

**Set up an internal process to ensure that requests are identified and processed** within a short timeframe.

Concerning the **deadlines**, you have:

- 1 month maximum for a simple request
- 3 months maximum for a complex request (*e.g. if a person requests a copy of their entire data*)
- 8 days maximum for health data

# STEP 5

## Inform users you are collecting data

**Whenever you collect data, you need to inform users about it.** According to article 12 of the GDPR, the information must be communicated “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”. To avoid long statements, you can give a first level of information and refer to a privacy policy on your website.

Here is the required information you need to provide:

- **why** you are collecting the data (the purpose)
- **what authorises you** to process the data (the legal basis: this may be the data subject's consent, the performance of a contract, your 'legitimate interest'...)
- **who has access** to the data (specify categories: relevant internal departments, a service provider...)
- **how long** you keep it
- the way in which **data subjects can exercise their rights** (via their personal space on your website, by sending a message to dedicated email address...)
- if you **transfer data** outside the European Union (specify the country and the legal framework that maintains the level of level of data protection).

You can use this template! Fill it in with your current information.

# STEP 6

## Secure your data

Take steps to secure data, whether **digital or printed**. You need to be especially careful when processing sensitive data, as it poses a risk to data subjects in the event of an incident.

**Actions you can take** include using locked filing cabinets, securing access to your buildings, changing passwords regularly, using anti-virus software, encrypting mobile devices, backing up data and setting up a data recovery procedure

Be aware of the consequences for individuals of the loss, disclosure or unwanted modification of their data, and take steps to minimise these risks.

You can find a detailed **template** for performing an **information security assessment** of your organisation.

# STEP 7
## Appoint a Data Protection Officer

It is **strongly recommended to assign a person responsible** for managing GDPR compliance within the organisation. If you are one of the following cases, it is even **mandatory to appoint a Data Protection Officer**:

- public authorities or bodies
- organisations whose core activities lead them to carry out regular and systematic monitoring of individuals on a large scale
- organisations whose core activities lead them to process sensitive data or data relating to criminal convictions and offences on a large scale

### How to choose a DPO?

The DPO has an **information, advisory and monitoring role.** There is no standard profile for the position of DPO, but it is necessary that the person has a certain level of legal and technical expertise in data protection.

It can be an internal DPO, like a member of the organisation's staff working part-time or full time as DPO. Or it can be an external DPO, on the basis of a service contract concluded with a natural person (e.g. consultant, employee of a group subsidiary, etc.) or legal entity (e.g. law firm, consultancy, management centre, mixed syndicate, etc.).

STEP 8

# Be prepared for an incident (data breach)

Even if you have been very careful with the personal data you process, it is still possible for an incident to occur. It is therefore important to be prepared and to know the procedure in case of a data breach.

> **Data breach**
>
> *A breach of security resulting in the destruction, loss, alteration, unauthorised disclosure or accidental or unlawful access of personal data*

As an organisation, it is essential to **implement appropriate technical and organisational measures** to avoid possible data breaches.

If that occurs,

1. **You have to notify the supervisory authority** within 72 hours after having become aware of the breach. Supervisory authority depends on the country. To notify a data breach in Sweden, please follow this link.

2. If the data breach puts the **data subjects at risk** by threatening their rights and integrity, they **must be informed.** It must contain the **nature** of the breach, the **consequences** of the breach, the contact details of the person to be contacted (DPO or other), the measures taken to rectify the breach and to limit the negative consequences.

# STEP 9

## Have control on third-party services that handle personal data on your behalf

**All actors involved in the processing of personal data of European residents have a responsibility, whether or not they are established in the European Union.**

Two roles can be distinguished:

- **Controller**

A controller is a natural or legal person, public authority, agency or other body which, **determines the purposes and means of the processing** of personal data: meaning the objective and the way it is carried out.
You are **ultimately accountable** for your own compliance and the compliance of your processors.

- **Processor**

You are a processor if you **process personal data on behalf of and under the authority of a controller**.
Processors, like controllers, **must comply with the GDPR**. We advise you to follow this step-by-step guide to ensure you comply with the law. Like the controller, you can be held **liable for non-compliance**.

This guide helps you to better understand the steps to be GDPR compliant.

**However, we know that it is challenging and tedious to complete the GDPR process without help. FAIRITY is the solution that will secure the data in your business in a simple way and give you peace of mind.**

# TAKE ACTION

MEET US

GET STARTED FOR FREE