

HOW TO CREATE A SUCCESSFUL DATA PROTECTION PROGRAM



✓ Pridatect

Table of contents

01	Introduction	
02	Steps to create a successful data protection program	
	a) Be aware of the activities carried out by your company	4
	b) Analyze existing risks	5
	c) Analyze what situations require a DPO to be designated.....	6
	d) Identify the companies that provide services and have access to data.....	7
	e) Inform those interested	8
	f) Provide training to employees	9
03	Conclusion	

01. Introduction

The key to a good data protection program is to be meticulous and follow the steps below.

However, we must remember that organizations are changing entities, so the real success in carrying out a data protection program will be to keep track of it, in order to always keep it updated.

For example, If employees need to know who has access to personal data, this information should be updated whenever somebody new joins the company. This means that focus can be on the clarification of responsibilities in the event of a data breach. It is not enough to update the data protection program once a year, it should be modified periodically.



02. Steps to create a successful data protection program

Therefore, the steps described below require being completed cyclically:

a) Be aware of the activities carried out by your company

As a data protection consultant it is essential to know the ins and outs of the company in which you'll be carrying out the compliance program.

You should know the activities that they perform in order to know how personal data is treated.



For example, a hospital does not own the same data as a community of owners does: in the first case a large amount of data will be treated, including specially protected data such as health data, while a community of owners treat less personal and it isn't as sensitive.

Once the treatment activities have been identified, the registration provided in article 30 of the GDPR should be carried out, taking into consideration what activities the company carries out as responsible, co-responsible, responsible or under-responsible for the treatment.

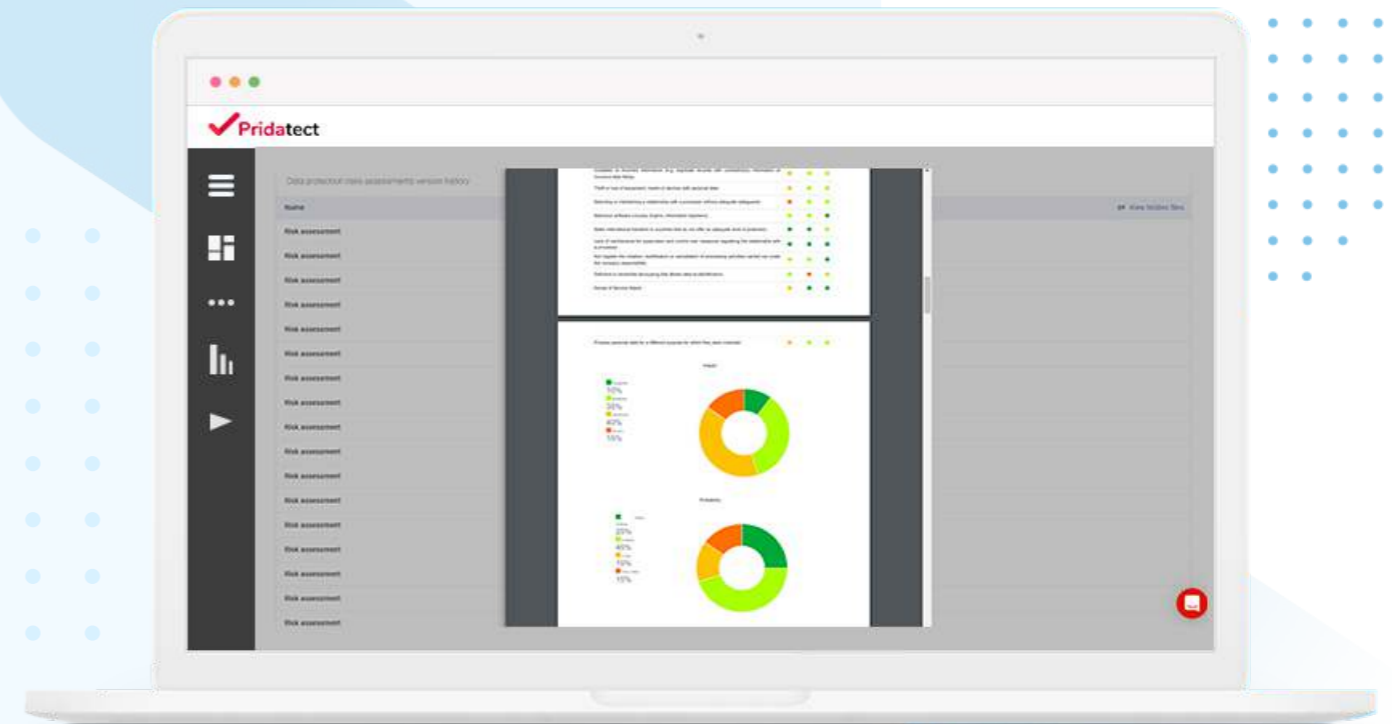
Performing the records of processing activities or RPA will be a fundamental step in identifying the legitimacy bases of each treatment, their length, their purposes, the existence of international transfers, etc.

b) Analyze existing risks

An analysis of the risks that may affect the treatment activities should be carried out in order to provide security measures to each risk scenario.

It is essential to correctly identify what measures should be applied, being consistent with the size of the company, and the risks that have been identified. The measures implemented must be preventive, contain problems and corrective, being able to differentiate between technical and organizational measures.

In some cases, companies must perform a data protection impact assessment. A previous risk analysis will help you determine if your company needs to.

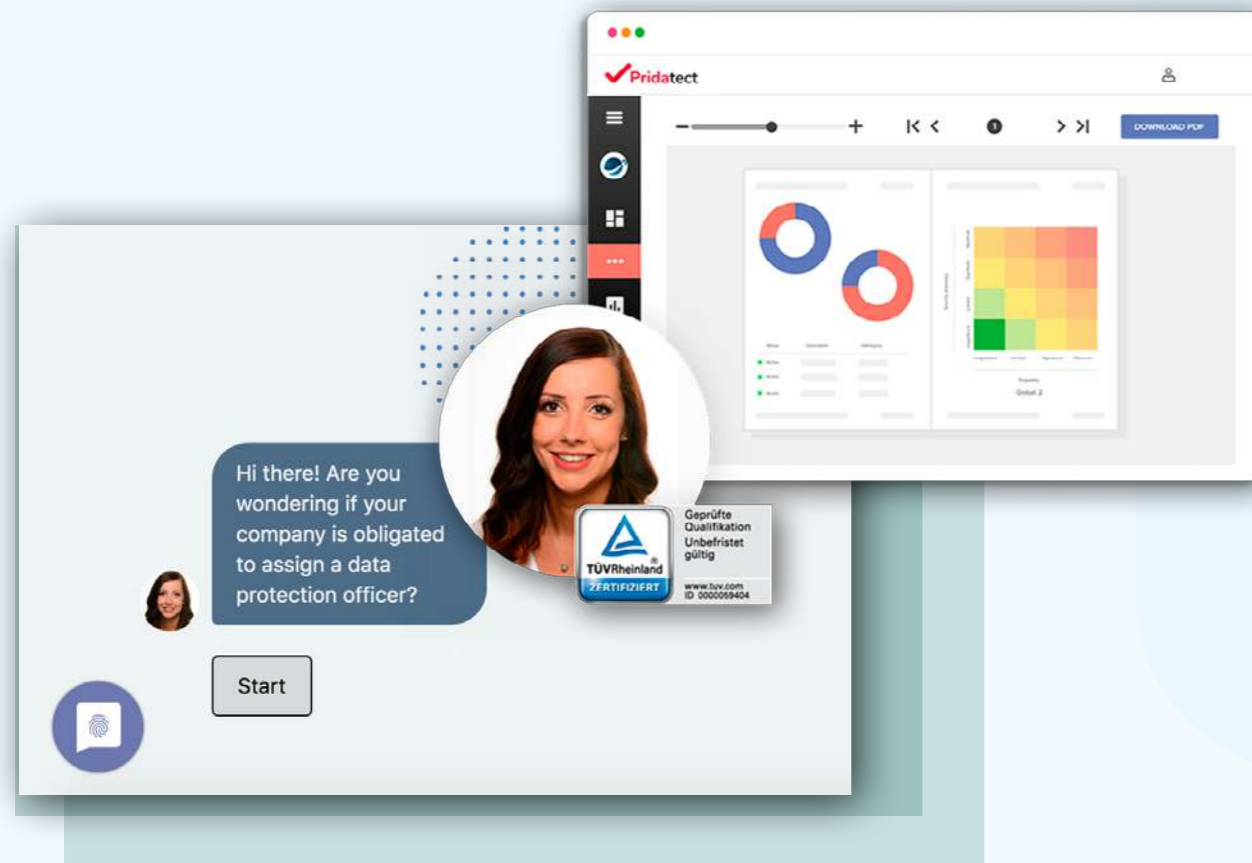


c) Analyze what situations require a DPO to be designated

The GDPR requires the need of a DPO in the cases established in art. 37:

- **If the treatment** is carried out by a public authority.
- **When the main activity of the organization implies** habitual and systematic observation of large-scale stakeholders.
- **When the main activities of the organization consists** of large-scale treatment of special categories of personal data.

Even so, in cases where it is not mandatory, it will be more than advisable to designate a DPO, as the company can benefit from having this figure monitoring compliance.



START TEST

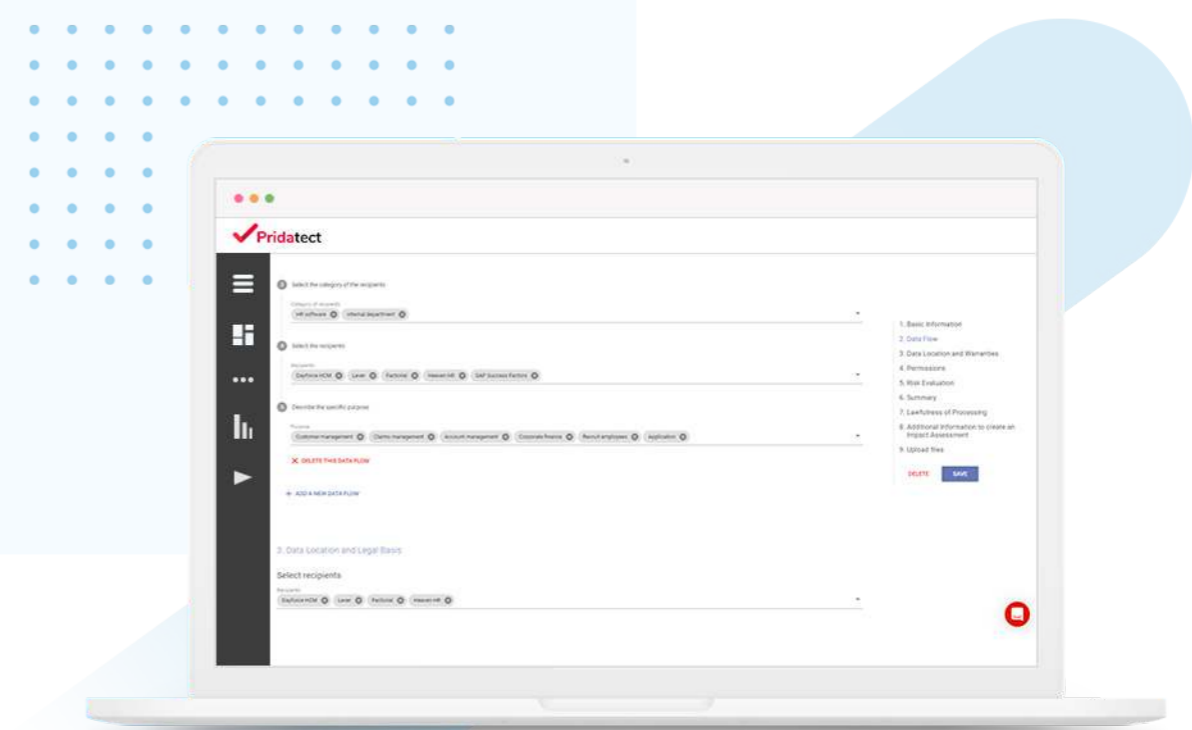
d) Identify the companies that provide services and have access to data

Another very important point to ensure the security of processing is to identify which companies or organizations provide services and access to data, in order to categorize them as data processors, recipients or assignees.

Identifying these companies will also help to define whether or not there are international data transfers and if the guarantees that allow data transfer outside the EU are applied.

It will be mandatory to establish agreements or contracts for data processing by third parties and for confidentiality in the provision of services. It will not be possible to have processors who do not agree to sign such agreements or that do not comply with the measures established in them, nor can

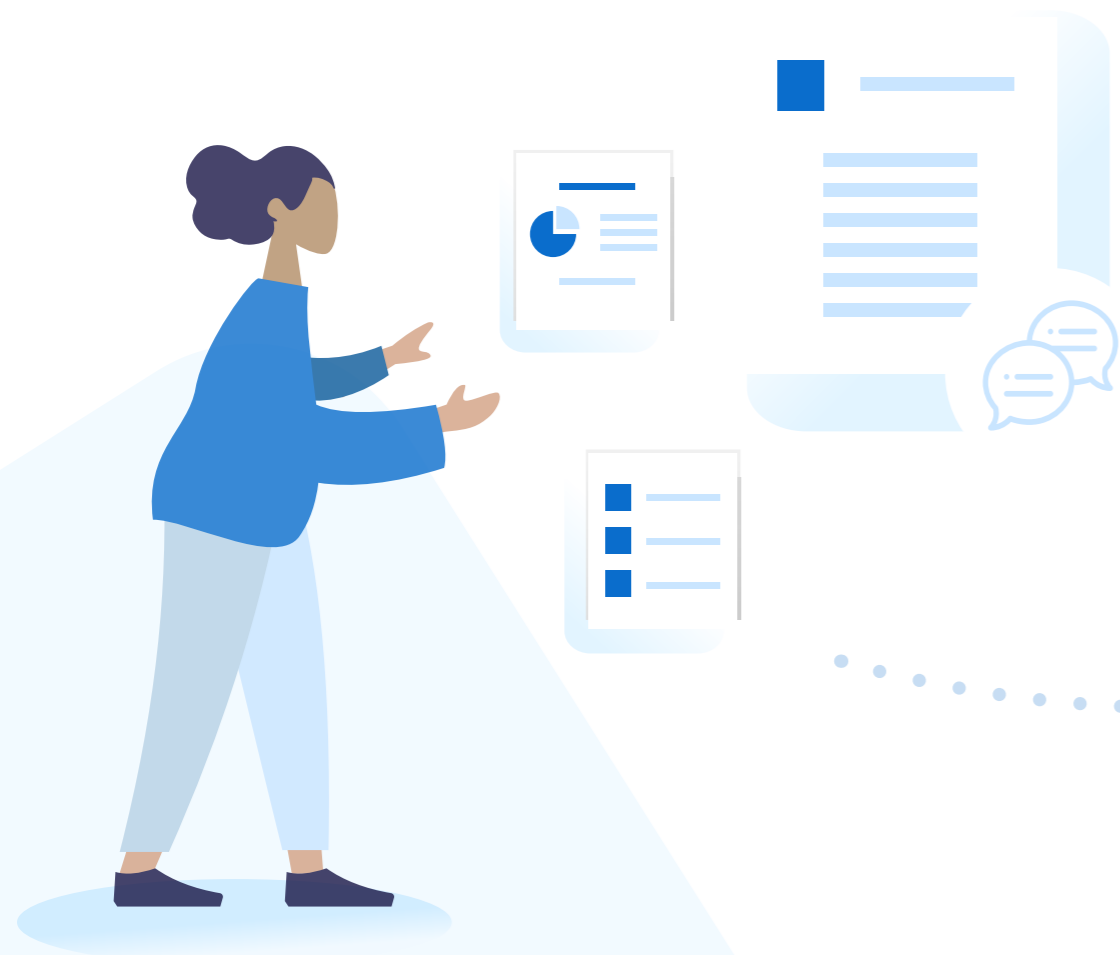
international data transfers be made without their corresponding guarantees, so the organization must be especially careful in the selection of suppliers and you would even have to stop working with some of them if they are not guaranteeing compliance.



e) Inform those interested

The most important obligation found in the Regulation is to inform data subjects about the processing of their data. This obligation must be carried out at the time of data collection.

The need to report on commercial communications or on data collected online is especially relevant. A good practice for a successful data protection program is to inform through a double layer: give a first layer of basic information and include a link with the additional information. In this way, even when the user does not access the second layer, he will have an overview of the basic information.



f) Provide training to employees

Finally, one of the crucial points for the company or organization to comply with data protection is to train all the people who are part of it so that they know how they should treat the data, how to act in a security breach or how to manage a rights request.

This point is what will make the organization have a right compliance policy and culture.



03. Conclusion



A **good data protection program** must be complete and cover all the obligations imposed by the regulations as well as ensure all the rights of people. Not 100% sure what this is in the trying to say, can you clarify?



Although the **GDPR does not establish any timeframe for audits**, it will be very beneficial to perform them in order to verify that the company maintains compliance and has implemented all recommended measures.



As always, **the most important thing for a data protection program to be successful are people**. So it would be important to train each new employee and to hold training sessions from time to time. Keep in mind that human errors are one of the most common causes of security breaches, and even these can be avoided or reduced with good training.



Likewise, **a good way to carry out a data protection program** is to use software such as **Pridatect** that will make the repetitive tasks that take so much of your time, a lot easier.

Pridatect simplifies the process of detecting risks and protecting data



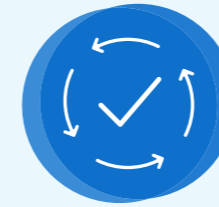
DETECT AND IDENTIFY RISKS

Detect and identify personal data treatment (customers, employees, suppliers ...) risks in your company. With the Pridatect platform we can identify and analyze threats and vulnerabilities in your data processes.



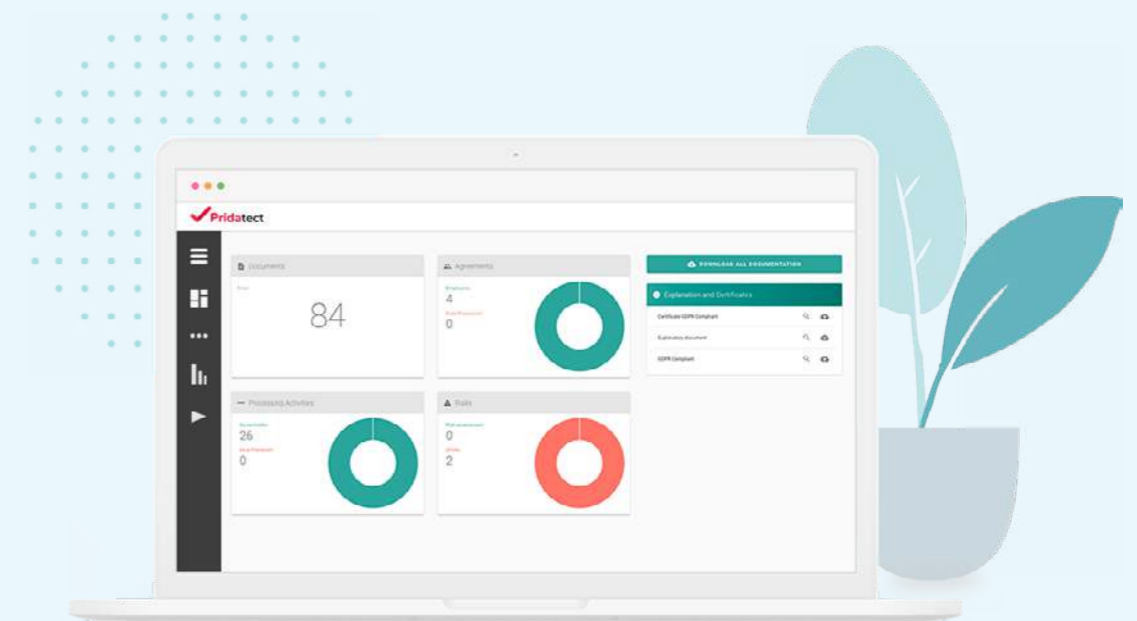
DEFINE AND SUGGEST PREVENTIVE ACTIONS

Knowing the risks in your company allows you to define the necessary measures to reduce and mitigate them. Pridatect helps you with the definition and suggestions of measures for your company.



MONITORING AND IMPLEMENTATION

Data protection is an ongoing task within a company. Pridatect does not only help with the initial implementation, but also with ongoing risk monitoring, measures, and the data protection related task management among your company's employees.



Contact us for a [free demo](#)
or make use of our [7 day free trial!](#)