Pridatect

WEBINAR

Find a DPO model that works for your business

Lisa Hofmann

Chief of Legal Operations Pridatect

Legal specialist and certified Data Protection Officer (TUEV), broad experience in helping companies with their privacy compliance

Tash Whitaker

Global Data Compliance Director Whitaker Solutions

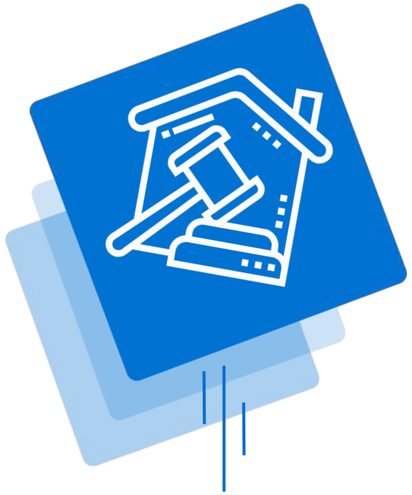
CIPP/E, CIPM, DPO Certification (Maastricht), PG Cert Data Protection Law & Information Governance

Send us your questions!

lisa.hofmann@pridatect.com

Agenda

What is a DPO and why is it important to have one?



When does a company need a DPO?

What are the responsibilities of a DPO?

How to pick the right DPO model for your business?

01. Introduction

What is a DPO?

A data protection officer (DPO) is a company security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.

Why is it important to have one?

A data protection officer assists you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

What different models are there?

A good DPO must be independent, an expert in data protection and have the necessary resources to carry out a professional data protection service. This service can be provided in two ways: internal, by having an employee appointed as DPO, or external, which means to outsource the tasks and responsibilities of a DPO to a professional.

02. When does a company need a DPO?

According to Article 37 (1) of the GDPR, a controller or processor must appoint a DPO under the following circumstances:

1. the processing is carried out by **a public authority or body**, except for courts acting in their judicial capacity;
2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, **require regular and systematic monitoring of data subjects on a large scale**; or
3. the core activities of the controller or the processor consist of processing on a large scale of **special categories of data** … or **personal data relating to criminal convictions** and offences…

But what if by definition of Article 37 (1) of the GDPR you don't need a DPO?

Personal data and special category data

There is certain data, such as that relating to children, that because of its relevance and importance to privacy must be treated and stored with greater care and in compliance with a series of requirements. Not all personal data is of equal importance.

What is "personal data", according to the GDPR?

- Identifiable information such as first name, last name, telephone number, etc.
- Pseudonymized data or non-direct identification information, which does not allow the direct identification of users but does allow individualized behavior.

What is special category data?

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Union membership
- Genetic data
- Biometric data in order to uniquely identify an individual
- Those data relating to health or sex life and/or sexual orientation

03. What are the responsibilities of a DPO?

the DPO should be an intermediary between relevant stakeholders (eg supervisory authorities, data subjects and business units within and organisation)

Inform and advise the controller/processor of their obligations under applicable data protection rules

Cooperate with and be the point of contact as needed for the supervisory authority

Monitor compliance and draw the institution's attention to any failure to comply with the applicable data protection rules

Provide advice and monitors the process on data protection impact assessments

Create a register of processing activities within the institution and notify the EDPS those that present specific risks (so-called prior checks)

Handle queries or complaints on request by the institution, the controller, other person(s), or on her own initiative

What is the liability of a DPO?

- Under GDPR and the DPA 2018, there is no specific liability outlined for DPOs

- A DPO *cannot* be dismissed or penalised by the controller for carrying out DPO duties (not to say a DPO can't be fired for eg. poor performance!)

- A DPO *can* face criminal liability if the individual "(a) Knew or ought to have known (i) That there was a risk that the contravention would occur, and (ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but (b) failed to take reasonable steps to prevent the contravention"
  - Note: This will only result in statutory damages, not imprisonment

- The DPO remains liable for non-compliance with general employment, contracts, civil (or tort, within a common law scenario) and criminal rules, as also set out by the domestic laws of the relevant member states.

The DPO isn't personally liable for data protection compliance. As the controller or processor it remains your responsibility to comply with the GDPR. Nevertheless, the DPO clearly plays a crucial role in helping you to fulfil your organisation's data protection obligations.

ICO. *(Information Commissioner's Office)*

A day in the life of a DPO

Tash Whitaker is giving us a peek behind the curtain of what a day in the life of an external DPO looks like:

8AM: Check emails and slack groups, respond to queries

10AM: Scheduled monthly Ropa review meeting

11AM: Slack and emails

12 noon Lunch

1PM: DPIA meeting

3PM: New Employee training session

4:30PM: slack and emails

04. What are possible DPO models

So, now that you understood the importance of appointing a DPO for your organisation, you have to find a DPO model that meets your data protection requirements.

Internal full-time DPO

Internal part-time DPO (conflict of interest!)

External DPO

When does an internal DPO make sense for a business?

If the business is very complicated and/or high risk and the DPO needs to be on top of the business the whole time

+ team collaboration and internal influence
+ up to full-time availability
+ Easier to ensure data privacy is being considered in all business decisions

- difficulty to be independent
- cost of covering full-time specialist salary
- difficult to guarantee “always on call” responsibility, in case of a data breach for example

“The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.”

ICO. *(Information Commissioner’s Office)*

When does an external DPO make sense for a business?

An outsourced DPO is able to maintain an emotional distance from the company allowing them to

a) ensure the company adheres to strict guidelines
b) communicate with upper management, as this is far more difficult for an inhouse DPO.
c) provide a variety of skills and experience to suit you, whilst remaining cheaper

+ less emotional connection to the business / independent
+ experience with various businesses
+ external DPO for the oversight of the business
+ direct line to the board
+ Always on call team or qualified substitute

How to make the choice for your business?

Understanding the different models available, there are a few questions you can play through to find the best choice for your business.

- How high is the complexity of your business?
- Do you have a qualified person inhouse who could cover the topic or could you hire one?
- Is there a danger of having the person handling tasks that are conflicting the independence of the DPO?
- Do you have a backup who could cover in case of a data breach for example?
- Financial consideration: Which model is more cost-efficient for your business?

"A DPO should report directly to the highest level of management be given the required independence to perform their tasks. The DPO should be, in a timely manner, involved in all issues relating to the protection of personal data."

ICO. ***(Information Commissioner's Office)***

Pridatect, a platform to simplify the process of identifying risks and protecting data

DETECT AND IDENTIFY RISKS

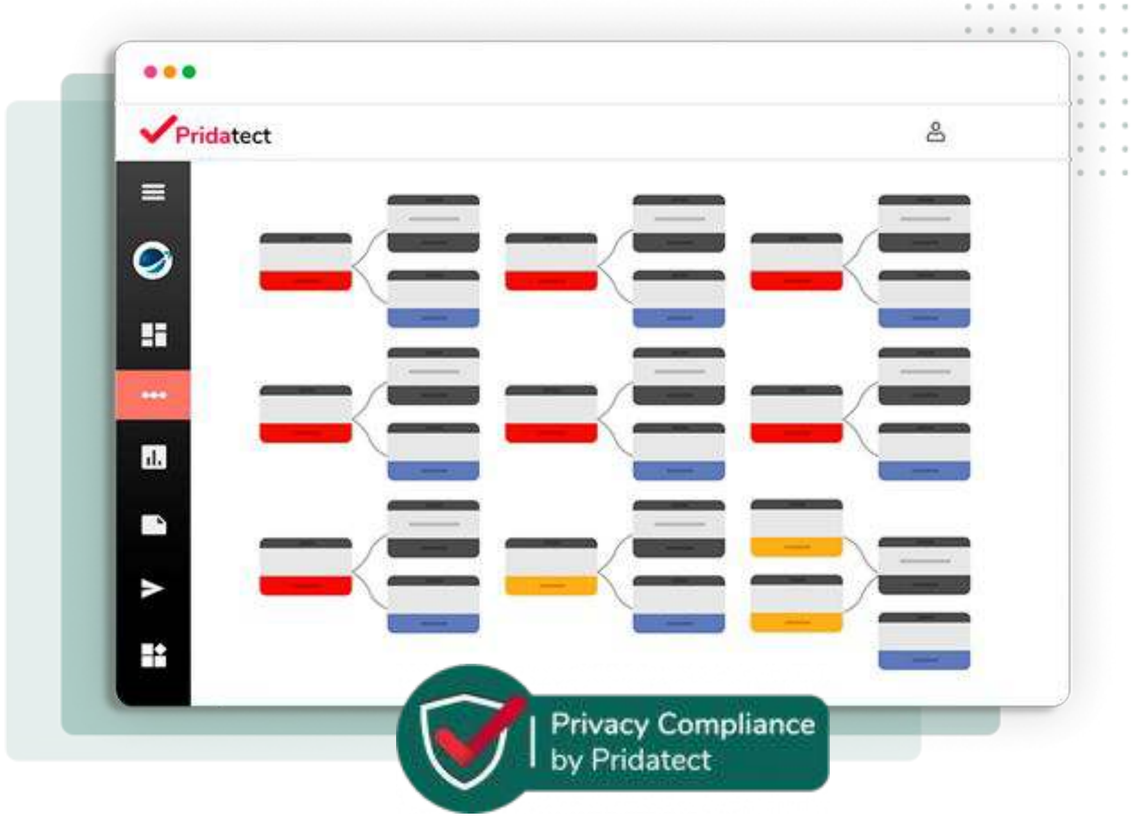
Detect and identify risks in your personal data processing (**customers, employees, suppliers...**). With the Pridatect platform we can identify and analyse the threats and vulnerabilities in your processes.

DEFINE AND SUGGEST MEASURES

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

PROGRAMME MONITORING AND IMPLEMENTATION

Data protection is a constant task within a company. Pridatect not only helps with the initial implementation, but also with the continuous monitoring of risks, measures and task management among your company's employees.



Trusted technology solution for your data protection

Everything you need to comply with the GDPR

Risk assessment

Eliminate data risks

Impact assessment

Automated impact assessment

Compliance analysis

Identify gaps in your data protection

Processing Activities

Have an up-to-date record of processing activities

Data map

Map your company's data flows

TOMs

Defines technical and organizational measures to reduce risk

Privacy reports

Generates privacy reports automatically

International transfers

Manages international data transfers

Security Gap Management

Successfully handles security breaches

Fulfillment of your website

Generates privacy policies, cookie policies, terms and conditions

Subject access rights

Manages requests for access rights and subjects

Secure Userdesk Cloud

100% secure, collaborative cloud environment

External DPO service

Virtual DPO for your company

Contracts with suppliers

Generate the contracts you need for GDPR

Document Automation

Create legal documents based on our models

Try Pridatect!

Take control of the data protection management in your company and ensure that your whole team has the necessary guidelines to protect the data of your clients. At Pridatect we help you to detect risks and take the appropriate measures.

Contact us for a free demo or use our 7-day free trial.

Request your free demo

Lisa Hofmann

Chief of Legal Operations Pridatect

Legal specialist and certified Data Protection Officer (TUEV), broad experience in helping companies with their privacy compliance

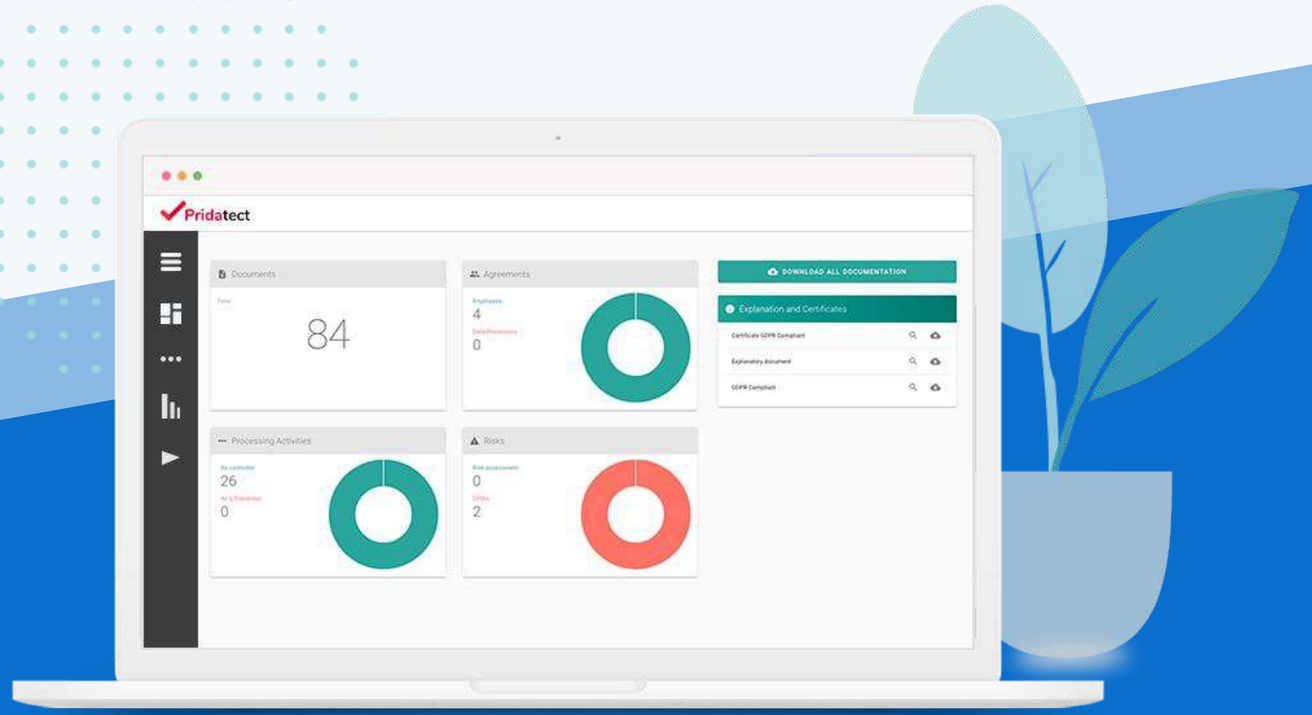
Tash Whitaker

Global Data Compliance Director Whitaker Solutions

CIPP/E, CIPM, DPO Certification (Maastricht), PG Cert Data Protection Law & Information Governance

Send us your questions!

lisa.hofmann@pridatect.com



Thanks for joining our webinar!