Pridatect
POWERING PRIVACY COMPLIANCE

BEST PRACTICES OF A DPO

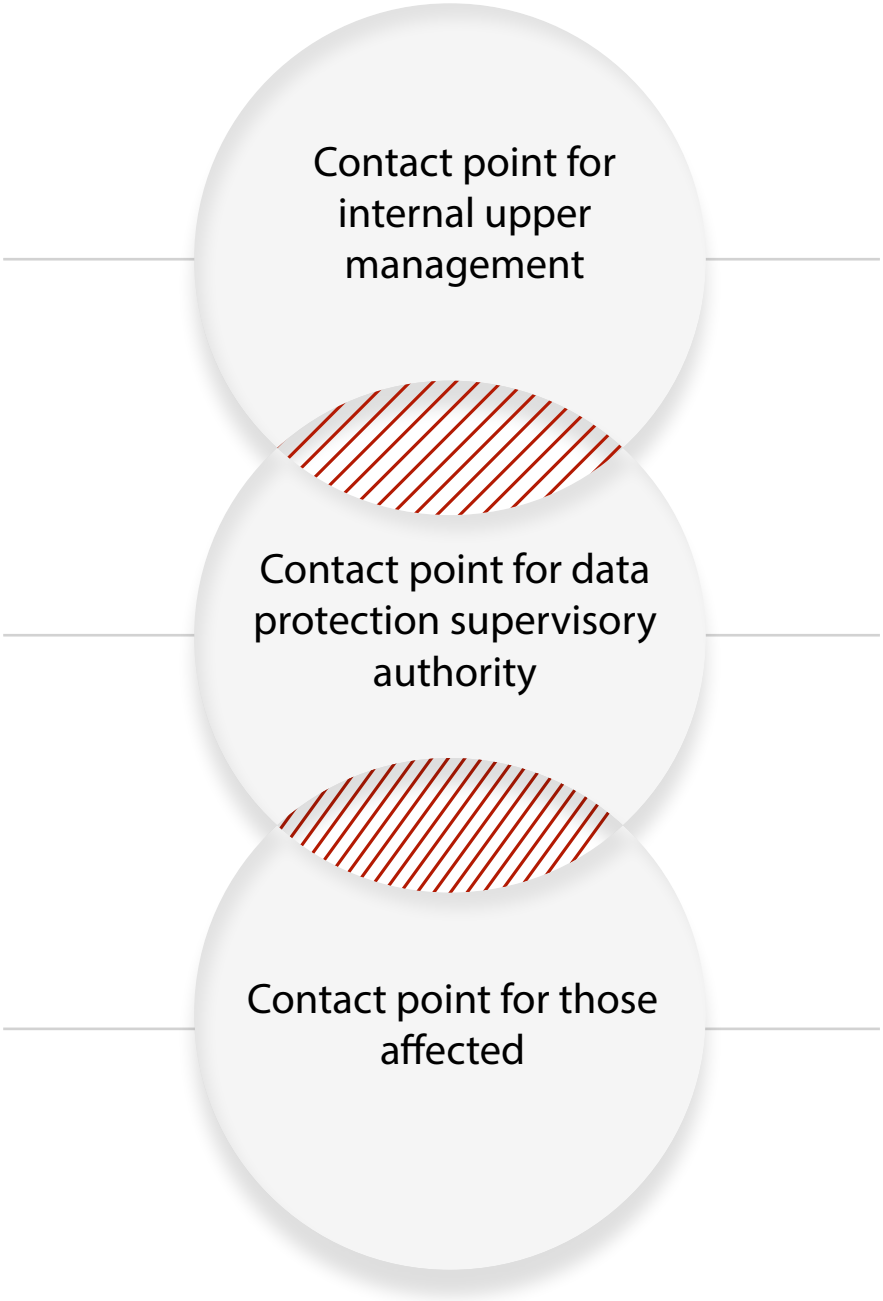
Introduction

With its entry into force on May 25th 2018, the General Data Protection Regulation (GDPR) caused a stir, mainly because of the stricter sanctions, in particular the possible fines of up to €20 million euros, or 4% of the annual global turnover in a company – whichever amount is higher.

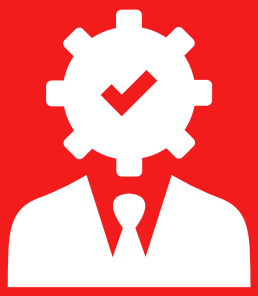
Due to these new European data protection regulations, the importance and need for effective data protection management and data protection officers (DPOs) has risen considerably.

The roles of a data protection officer

With the implementation of the GDPR, Data Protection Officers have been assigned an important role in the protection of data of natural persons. Therefore, a DPO, regardless of whether they are hired and thus appointed internally or appointed as external consultants, must be duly involved in all matters related to the protection of personal data (Art. 38 (1) GDPR).



Pridatect



In addition, the DPO has the role of point of contact for interested parties who can consult them about any matter related to the processing of their personal data and the exercise of their rights under these Regulations (Article 38 (4) GDPR).
The DPO also serves as a point of contact for the supervisory authorities (Article 39 (1) (e) GDPR).
Finally, a DPO should report directly to the highest level of management (Article 38 (3) sentence 3 GDPR).

Even though it is permitted by law to take on additional roles and thus at the same time further tasks, these may not conflict with the performance of their duties as DPO (Art. 38 (6) GDPR).
These conflict of interests would be most prevalent among senior executives in a company such as a Chief Technology Officer or a Head of Legal.

In this situation, the DSB would review its decisions of a senior employee operating as a data protection officer, as it would be possible to not do proper justice to the statutory freedom of instruction of the DPO (see Article 38 (3) sentence 1 GDPR).
As a result, the DPO h
as a special and significantly relevant role in any company that could be taken over by a new employee, an external service provider or an existing employee, as long as there is no conflict of interest.

The tasks of a data protection officer

The duties of a data protection officer are specifically listed in the GDPR. However, it is clear from the wording that these are only the bare minimum tasks required, since they can also have other roles and thus additional tasks (see below):

- Informing and advising a the person responsible / contrat processor and his employees regarding data protection law. (Art. 39 (1) (a) GDPR)
- Monitoring compliance with data protection law including assigment of responsabilities. (Art. 39 (1) (b) RGPD)
- Advice on data protection and monitoring of implementation. (Art. 39 (1) (c) RGPD)
- Cooperation and contact point of supervisory authorities.(Art. 39 (1) (d) RGPD)

When carrying out its tasks, the DPO shall also take due account of the risk involved in processing operations, taking into account the nature, scope, circumstances and purposes of the processing (Article 39 (2) GDPR).

This is particularly relevant because the data protection officer is to advise the respective controller or processor in fulfilling his data protection obligations, but does not himself fulfill these obligations.

For example, according to Article 30 GDPR, the controller should keep a record of processing activities, not the data protection officer.

However, he will advise the person in charge how such a directory should look for the responsible person.
The DPO thus supports the responsible person in carrying out his duties correctly, but does not accept them.

The challenges in implementing data protection law.

Regardless of whether a person in charge must appoint a data protection officer under Art. 38 GDPR, in any case he needs suitable means to enable him to fulfill his data protection obligations.
This applies above all to the obligation to provide proof according to Art. 5 para. 2 GDPR.

The focus of the charge lies in the observance of data protection law, without having to tie up high human and financial resources that could hinder or even prevent its implementation of its economic goals

When a data protection officer is appointed, he, in addition to strong communicative skills and technical knowledge of law, technology and business, must first of all be able to rely on appropriate organizational means for participation and conduct of privacy inspections.

Ensuring the necessary knowledge...		
...about data flow	...about the data protection measures	...about the data receivers

Guarantee of optimal communication...		
...on the scope of the data protection obligations	...about data processing, risks and measures	...about the processing status of documents

Enabling an efficient organization...		
...the cooperation between the DPO and the person responsible	...the data protection documentation	...the cooperation with several responsible persons

The data protection officer should be involved by the responsible person according to his needs, so that he can explain to him and his employees the regulations of the data protection law. Above all, this means informing the responsible person of their data protection obligations as well as the corresponding rights of the involved parties.
In addition, the DPO should support those responsible in the risk assessment and finding suitable data protection measures.

Inevitably, therefore, an organized communication is required, so that in all departments of the person responsible as the appointed data protection officer, the necessary knowledge about the data flows, the parties involved and the risks of those affected is present.
This is especially important when special personal data is the subject of data processing, several data recipients are involved or data is transferred to third countries.

If data processing is then checked, the practical challenge is to compile the corresponding data protection documentation for it.
Often, documents of the most varied format are sent back and forth between technical contact persons at the person responsible and between the person in charge and his DPO.

This often results in different versions of documents that work without control and documentation. A central filing and historization especially of final documents is not done regularly. Rather, questions arise, such as:

Which categories of personal data have been processed for AB by the end of last year?

What is the latest version of the privacy information for the app XY?

Which processors ar involved in procedure 123?

These types of questions can not be answered without structured documentation, so that the person responsible can not fulfill his obligation to provide proof according to Art. 5 para. 2 GDPR.

Without efficient data protection management, it is therefore impossible to collate all necessary information in an orderly manner to verify compliance with applicable data protection law, to include DPO as required by law and to document these activities.

A data protection officer is also interested in documenting his activities. This is especially true for external data protection officers. In addition, for data protection officers who have been appointed for several persons in charge, working without suitable data protection management also entails considerable additional personnel and financial expenses. Expenses, which in the result carries the responsible person.

Pridatect 360 - The Data Privacy Management Solution

In order to ensure the necessary knowledge of the parties concerned about the rights and obligations of the person responsible, to ensure optimal communication with each other and to enable an effective organization of data protection, the use of a data protection management solution is indispensable. This is exactly what Pridatect 360 offers.

Pridatect 360 is an online platform where managers and data protection officers can centrally collate, and historically document and use the information they need to create relevant documents. These include above all:

- The register of processing activities under Article 30 of the GDPR,
- A list of recipients of data i.S.v. Art. 4 (9) GDPR,
- A compilation of the technical and organizational measures (TOMs) according to Art. 24 para. 1 GDPR,
- An assessment of risks for those affected as well as a data protection impact assessment according to Art. 35 GDPR.

The high degree of customizability of the data types, data categories and data flows and information on participants leads to extremely precise data protection analyzes.
At the same time, the reusability of once individually created templates for other processing activities and / or persons responsible means that data protection documentation and checks can be created more effectively and resources conservatively.

An optimal modern solution for both responsible persons and data protection officers.

Pridatect
POWERING PRIVACY COMPLIANCE

COMMITTED TO DATA PROTECTION

More information at
pridatect.com

Contact
info@pridatect.com