THE ULTIMATE GUIDE TO APPOINT A DATA PROTECTION OFFICER

A practical guide for companies seeking GDPR compliance by appointing a DPO

The importance of data should not be underestimated in a modern company. Marketing uses data from (potential) customers to steer its campaigns, the HR department processes data of staff members in its hiring process or to improve the wellbeing within a company, the financial figures and dashboards are the cockpit for the company's managers and shareholders. If these data concern personal data, GDPR rules must be respected. In some cases this will even lead to the compulsory appointment of a Data Protection Officer (DPO), i.e. an adviser and privacy watchdog within your own organisation. This white paper focuses on the obligation to appoint a DPO and what you should pay attention to when filling this position.

TABLE OF CONTENT

Do I need to appoint a DPO?

Not all companies that process personal data need to appoint a DPO. A rough estimate in 2019, a year after the GDPR obligations were implemented, put the counter of the number of DPOs in Europe at 500,000. About 400,000 of them were officially registered with the national supervisory authorities. What criteria did these companies use to decide to appoint a DPO?

Originally, the European regulator specified arbitrary criteria such as the minimum number of staff that had to be employed in a company before a DPO had to be appointed. During the difficult political negotiations on the legal text, these criteria became more vague. As a result, it is not easy to determine whether a company should appoint a DPO. This white paper interprets the legal requirements and translates them into some practical workable criteria.

Criterion 1: The organisation is a **public service** (and, specifically in the Belgian context, when a company processes personal data for a public service in the context of a provision of services, i.e. as a supplier for the government).

Criterion 2: The organisation makes profiles based on personal data, for example of customers or staff members, with the purpose of **observing** a customer or staff member based on them. Usually, the purpose of profiling is to offer a product or service to a customer, or to assess the individual (e.g. the staff member). Other observation techniques such as camera surveillance may also lead to the appointment of a DPO if they are organised systematically and on a large scale (for example, by a surveillance company). A subcontractor who helps customers make profiles is also required to appoint a DPO.

Criterion 3: The organisation (or the subcontractor providing this as a service) processes personal data of customers or staff members that GDPR considers 'special' or, loosely translated, '**sensitive**'. This is an exhaustive list of personal data, including health data, data on political or religious preference or data on ethnic origin. Processing these data will not necessarily lead to the obligation to appoint a DPO. Only when you process these data on a large scale the appointment of a DPO will be required.

The above criteria are a simplified representation of the legally described conditions for appointing a DPO. They provide a first idea of when the obligation to appoint a DPO does or does not apply.

Tip: Make sure you document the decision whether or not to appoint a DPO. In concrete terms, it is best to check whether the above criteria apply and to document this evaluation, especially when there could be doubts about whether or not to appoint a DPO.

Tip: Still not sure whether you need a DPO?
Do the DPO test here.

I don’t need a DPO, bye bye GDPR?

As discussed earlier, appointing a DPO is compulsory in specific cases. If, based on the above criteria, you determine you don’t need a DPO, please read the following:

- GDPR rules continue to apply. In other words, you still have to comply with the rules when processing personal data. This means, among other things, that you are still obliged to record any processing of personal data in a record, to communicate about the processing of personal data in a transparent way or to report a breach against GDPR rules, under conditions, to the supervisory authorities.
- Business opportunities may lead to new ways of processing personal data. It is therefore best to re-evaluate the above criteria periodically, especially if the company is constantly innovating.
- The ethical and correct handling of personal data is more and more part of good management. Appointing a DPO can help to convince customers and suppliers of the intention to handle personal data correctly.

Tip: Even if you don’t need a DPO, compliance with the regulations remains necessary. Make sure you have implemented all the necessary GDPR obligations.

What if I fail to appoint a DPO?

Companies that are required to have a DPO but fail to fill this position may face sanctions from the supervisory authority. Each European member state has at least one such supervisory authority. These supervisory authorities have been given an arsenal of sanctions by the European regulator to support their supervisory function. Examples of sanctions include fines, the suspension of processing activities (e.g. shutting down a website, restricting a sales and marketing channel, etc.) or making the violation public (naming and shaming).

Not filling the role of DPO has already led to such sanctions a few times in Europe. Large fines, as of mid-2021, have not yet been given. The amounts of the administrative fines for not appointing a (compulsory) DPO are between EUR 25,000 and 50,000. The maximum fine for not appointing a DPO can be up to 2% of the global annual turnover or EUR 10 million.

I appointed a DPO: sit back and relax?

Data protection is part of corporate culture. The intention to correctly handle data on customers and staff members is determined by the 'tone at the top' and is carried out by everyone in the field. DPI believes that data protection is part of an organisation's value chain. A DPO cannot identify the corporate culture and monitor this value chain on his/her own. Rather, as explained further in this white paper, the DPO is the coach, inspiration and point of contact to install and monitor this culture.

Larger companies will, in addition to the (central) role of the DPO, also appoint 'stewards' in various departments. These so-called privacy stewards support the DPO. They ensure the DPO can maintain sufficient contact with the various departments of the company. DPI has experience supporting the DPO by training these stewards based on the **'Introduction to Data Protection'** course and **in-house training courses**: a basic knowledge of the GDPR principles is also necessary for them to involve timely the DPO in the challenges within the department they represent.

DPO profile and level of education

A DPO does not have a distinct profile. In practice, you will find DPOs with a legal background, although chances are almost as high of finding a DPO with a technical background. It is also possible the DPO has had no training in any of these areas. To date, DPI has trained 3,000 DPOs in **Dutch** and **French**. The Belgian data protection supervisory authority, the Data Protection Authority, reported that 5,000 DPOs were registered in Belgium. The breakdown of these DPOs is estimated to be as follows: the number of DPOs with more of a legal background is estimated at 45%. The remaining percentages are broken down between DPOs with a technical background (35%) and DPOs with another background (20%).

Which profile fits your company or organisation best? A technically trained expert will be more likely to be able to answer the question of whether all technical safety measures have been taken to ensure the secure processing of personal data. A legally trained DPO will be looking for the answer to the question whether all legal conditions set by the GDPR have been met. Whether as a company you are more likely to look for a technical or a legal expert will probably depend on the expertise you already have in-house. For example, an SME with a well-developed ICT environment is more likely to hire a legal expert to support the GDPR implementation. If the ICT environment is outsourced and/or an internal legal expert has been appointed, the necessary expertise may need to be more technical.

If an organisation has neither legal nor technical knowledge, it may look for a person who has (sufficient) knowledge of both areas of expertise. An alternative is to look for expertise offered by two different people who each possess a part of the required knowledge. A lawyer and a technician will then, together, look for an answer to the question of whether the GDPR rules are being respected.

A good DPO training ensures that the candidate DPO acquires sufficient knowledge about GDPR regulations. **During DPI's 5-day training** a legal expert will explain the GDPR rules to participants over the course of 2 days. Afterwards the GDPR is the main theme of the training and the technical aspects of processing personal data are discussed (this takes approximately one and a half days). Furthermore, attention is paid to the practical implementation of data protection in a company and the role of the DPO.

Please note that the regulator emphasises that the DPO must have expertise in the GDPR regulations and their practical implementation. They have to be able to prove this expertise. This is why the DPO training concludes with a certification exam. This allows you to prove you have sufficient DPO knowledge.

Tip: Prospective DPOs will have to put their knowledge into practice as part of the learning process. Moreover, the young field of expertise is still very much evolving. For example, decisions by supervisory authorities, their advice and recommendations. To keep track of all this, DPI offers 'Stay Tuned', a quarterly update of the most important evolutions. Former course participants and interested parties are also periodically invited to the free Privacy Café where professionals can meet.

The DPO's duties summarised in 3 core duties

Companies appointing a DPO for the first time often have to think about the best way to go about this. In practice, we regularly find that the company's expectations of this position often do not correspond to the duties the legislator has devised for the DPO. We will therefore focus on the DPO's legally laid down duties. His/her duties consist of at least three core duties: informing, advising and supervising.

Informing means the DPO must support the company's staff members in applying the regulations by informing them what the rules are and how best to apply them. This information must be customised to the staff member. For example, the person at reception registering visitors has different needs than the person managing the company's databases.

The second task, **advising**, is undoubtedly the one that requires most expertise. For this task, the DPO needs both technical and legal knowledge to test the processing of personal data with the legal requirements. This task is complicated by abstract rules that need to be translated to the organisation's specific context. The analysis may be influenced by sector-specific regulations in legal terms. The technical part may differ based on technical standards applicable to the processing. Both legal and technical knowledge are therefore required to provide comprehensive advice.

In addition to informing and advising internal and external stakeholders, the DPO must also **supervise** the processing operations of an organisation. The legislator has registered this duty in the GDPR to provide an initial check on the correct processing of personal data. To some extent, parallels can also be drawn with, for example, the position of internal auditor, ombudsman or a health and safety officer. This explains why the DPO is independent from the organisation and reports to the highest executive, the CEO.

In addition to informing, advising and supervising, the DPO will also act as contact for customers, staff members or other persons whose personal data the company processes. In practice, you see, for example, that the DPO's contact data are included in the privacy policy on the company's website. In addition, the DPO is also the contact for the supervisory authority.

Tip: When a company appoints a DPO, the company is obliged to notify this person to the supervisory authority. Most supervisory authorities have published a form for this on their website. Do not forget to renew this registration in case of a change of DPO.

And finally, in practice, the DPO will often be used to fulfil the obligations imposed by the GDPR. These obligations include, for example, drawing up a privacy policy, keeping a record of processing activities, the compulsory reporting of breaches of the regulations (think, for example, of a cybersecurity incident involving the viewing of personal data), etc. It is not illogical that a company appointing a DPO expects the DPO to also 'operationalise' all the legal obligations of the legislation. However, this is where the shoe pinches: for some of these duties, such as assessing the risks involved in processing personal data, the DPO has an advisory role under the law. Appendix 1 provides a handy overview of the possible duties and the DPO's role therein.

Tip: Make sure you define the DPO's duties before appointing one. It is best to lay down the DPO's duties from the start, i.e. in the vacancy, job description or service provision contract.

The DPO in the organisation chart

The legislator not only lays down the duties, the DPO's position is also laid down in the GDPR. In concrete terms, this means you cannot simply put the DPO anywhere in the organisation chart. When placing the DPO in the organisation chart, watch out for the following pitfalls:

- Make sure the DPO has an independent role. The DPO works on his/her own accord and cannot receive orders from others within the organisation in relation to the core duties (informing, advising and supervising). The legislator hereby protects the DPO by stating that the DPO cannot be dismissed as a result of giving advice or carrying out an inspection.

- Give the DPO access to all information and systems that process personal data at all times. In concrete terms: if the DPO wishes to access ICT systems containing personal data in the context of an audit, access to these systems cannot be denied.

- The DPO has a direct reporting line to the CEO. Although day-to-day reporting can be done to line managers, the DPO always has the possibility to report directly to the CEO.

- It is up to the organisation itself to involve the DPO in case of innovations, operational or structural problems in the processing of personal data, etc. Although the DPO can always issue an advice on his/her own accord, it is ultimately up to the company to request advice from the DPO. The legislator even goes a step further: the DPO must be involved in the project right from the design phase of a new innovation. We have learned from recent decisions by supervisory authorities that inspectorates look at the advice that the company requested from the DPO and the timing of the request.

- When the DPO combines duties, the organisation must consider whether this could lead to a conflict of interest. In short: if the DPO is able to make decisions about what can and may happen to personal data in the context of other duties, a conflict of interest is likely. Think of an ICT manager (who determines with which systems personal data are processed), the HR director (who makes the final decision about how data on staff members are processed) or a marketing director (who decides about the processing of customer data). None of these positions can be combined with the DPO's role.

Please note that the DPO must also ensure he/she only provides advice. It is not up to the DPO to make decisions regarding the processing of personal data. For example, a DPO who sees himself/herself as the person who has the final say on an innovative project, is exceeding his/her powers. **DPI's certification training** goes into this in more detail.

Tip: Which actions can a company implement to avoid conflicts of interest? The steps below help to avoid a conflict of interest:

- **Step 1: Compile a list of the DPO's different duties**

When the DPO combines multiple roles, the company must document why these roles do not conflict. If the company believes that in specific cases a conflict could arise, this situation must be appointed and how a conflict in roles is avoided must be indicated.

- **Step 2: Compile a list of additional duties in the context of GDPR**

As explained earlier, informing, advising and supervising are the DPO's core duties. The company has other duties that need to be performed in the context of the GDPR. The DPO can provide support in this. Appendix 1 provides an overview of these additional duties and what support the DPO can and cannot provide in this regard.

- **Step 3: Ethical code of conduct**

The DPO must at all times be neutral. Integrity is essential. Moreover, the DPO has a duty of confidentiality. As soon as he/she finds that this neutrality could be jeopardised, the DPO must take the necessary steps to bring this situation to

the attention of, for example, the internal audit department or the CEO, so that the necessary actions can be taken timely. Guidelines relating to this matter can be included in a code of conduct.

Internal or external DPO?

The role of DPO can be filled by a specially trained staff member or by an external consultant. Both options are possible and have advantages and disadvantages.

As mentioned earlier, data protection is part of a company's culture. A DPO on the payroll will most likely be in a better position to understand the culture and coach the organisation in developing good practices. The internal DPO will also provide the necessary continuity and usually is more approachable. A local DPO is able to develop a policy and provide consistency in this. The DPI's observation is that in companies and organisations where data protection is a truly important part of business operations, an internal DPO is always appointed.

The main disadvantage of an internal DPO is the risk of conflicts of interest. Although the DPO should be able to function independently, for personnel matters a manager will be indicated as contact. This may affect the DPO's independence. If this manager is, for example, the HR director, the DPO may feel intimidated when formulating advice on the processing of staff data. A combination of the role of DPO with other positions may also cause a conflict of interest (see above). A documented risk analysis of the independence of the DPO, as mentioned above, is therefore recommended.

Tip: Make sure that you keep the internal or external DPO's knowledge up to date. DPI provides update courses **(Stay Tuned)** and in-depth training (**masterclass** and **DP & technology**).

If you have an external DPO, the risk of conflicts of interest is more limited (but not non-existent, see tip below). Moreover, the external DPO will be able to share experiences of peers and thus inspire the organisation to deal correctly with personal data. The external DPO can hold up a mirror to the organisation: an external expert sometimes has more impact than an internal employee.

The advantages of an internal DPO are at the same time disadvantages for the external DPO. Compliance with data protection rules depends on the context. Sectoral regulations and agreements, the influence of suppliers and the management's impact determine the DPO's success. For external DPOs, the challenge is to capture and include these influencing factors within the agreed timeframe.

Tip: always check that the external DPO has no conflict of interest. If the external DPO also works as a DPO for a supplier or customer, a conflict of interest may arise. In other words, always check whether the candidate DPO acts for other companies in the information chain.

Several DPOs represent one company. Is that allowed?

It is possible to appoint several DPOs in the company, but only one of them will be the 'lead' DPO: the DPO acting as the single point of contact for the supervisory authority and for customers and suppliers. DPI has noticed that larger companies have several DPOs, each with a focus on a business process (for example, a DPO for HR and a DPO for marketing) or discipline (a DPO with a focus on information security versus a DPO with a focus on legal aspects). But you can only register one of these DPOs with the supervisory authority.

Attention: a DPO always has an overview of all business processes. The DPO will always have access to other business processes where personal data are processed (e.g. the processing of data concerning staff members). Appointing a DPO for a project or specific service is therefore not possible.

Often, internal DPO duties are supplemented by the services of an external DPO. The external DPO acts as a sounding board and an extra source of expertise. For instance, it happens that an internal DPO with more general knowledge is assisted by a DPO with a more legal background. In such cases, the internal DPO is (usually) appointed 'lead' DPO.

How much time is needed to fill the role of DPO?

The time the DPO needs to perform the duties has not been legally laid down. In itself, this is logical: the organisation's maturity plays a role (is GDPR already known, has the privacy policy been developed or not), but also the complexity (do you collect a lot of personal data or do you have many staff members) and the degree of innovation (do you use state-of-the-art track and trace technology or do you develop services whereby you profile or assess an individual in a smart way). This means the time to be spent in the performance of the duties is very variable. To give you an idea, here are a few examples:

Example 1: A marketing company guides its customers in the use of social media as a promotion channel. The company itself is an SME, but its customers are international. The marketing company appoints a part-time DPO.

Example 2: A regional hospital treats patients and is involved in scientific research projects with patient data. The hospital works with a full time internal DPO (lawyer) and a part-time external DPO with a more technical background.

Example 3: A bicycle shop measures the anatomy of customers to determine the right bike and bike position. Furthermore, personalised monthly newsletters are sent. Strictly speaking, appointing a DPO is not compulsory. Initially, an expert worked 5 days to ensure that the shop complies with the GDPR obligations and visits annually for an audit.

Example 4: A one-man business manages a platform for second hand items. The website monitors customers using cookies. This is how advertising space is sold. For 4 hours a month, an external DPO supports the manager, this consultant also handles questions from data subjects and monitors the platform's operation.

Conclusion

Correctly handling personal data is part of a modern company's value chain. A DPO helps organisations to draw up and implement a privacy policy. A DPO is necessary for public services and for companies that process personal data on a large scale, especially when customers or staff members are observed or when sensitive data is processed. This white paper provides more information on the criteria for appointing a DPO. The obligation to appoint a DPO applies to both companies that use the personal data for their own business operations and to suppliers that offer services related to the processing of personal data to these companies.

Increasingly, we notice a trend that companies which, strictly speaking, do not have to appoint a DPO, nevertheless employ a DPO or privacy expert. The explanation lies in the fact that appointing a DPO is just one of the many GDPR obligations. To comply with, and monitor, the (other) GDPR obligations, a staff member or consultant with the necessary expertise is still appointed.

The DPO has an independent position within the organisation. Both a DPO on the payroll and an external consultant can carry out the duties of a DPO. Both the DPO and the privacy expert need to have a sound knowledge of GDPR rules. Key to this is that the DPO must (at least) be able to inform the organisation about the correct application of the regulations, must be able to provide advice on this and must supervise the correct application of the legal provisions. In the case of the DPO, he/she has to be able to prove this knowledge. The **DPI certificate** for DPOs can help with this.

Annex 1: List of administrative obligations a company must meet in the context of GDPR and the DPO's role in this

As explained in the white paper, to be GDPR compliant, companies must implement a number of 'administrative' obligations. A list of these obligations is provided in the table below. The DPO can provide support with these obligations, but some obligations cannot be carried out by the DPO as this may lead to a conflict of interest. The table lists which duties the DPO can and cannot carry out.

GDPR obligation for a company	Duties the PO can and cannot carry out
Records of processing activities	The DPO can maintain the records. These records can serve as a dashboard or reference point for the DPO. The knowledge required to fill the records in terms of content will usually have to be obtained from company employees.
Data Protection Impact Assessment	The DPO cannot carry out this analysis: the DPO has an explicit advisory role in this risk analysis. However, the DPO can (help) establish the methodology and help determine the risk scales. The DPO can also provide training on how the analysis should be conducted.
Exercising the rights of the data subject	When a customer wants to view, access or delete data, the first thing to do is check whether the customer in question is in fact entitled to the requested action.

GDPR obligation for a company	Duties the PO can and cannot carry out
Exercising the rights of the data subject	. This usually requires a legal analysis in which the DPO can assist. The DPO must advise the management (this can be done based on case-by-case advice or framework agreements). However, the management can ignore a DPO's advice and, for example, refuse a request for access. In these situations, it is not evident that the DPO performs this duty. Conclusion: in practice, the DPO is often responsible for this, but proper coordination with the management is always necessary. In other words, giving this responsibility to the DPO is usually not best practice. Some duties, on the other hand, can be carried out by the DPO without any problems, for instance drawing up a privacy policy.
Notification of data breaches	For this obligation, the same reasoning applies as for exercising the data subject's rights. The DPO can assist with the administrative obligations of notification to the supervisory authority and the communication to the data subject in the event of a breach. The decision whether or not to do the notification and communication is made by the management, on the DPO's recommendation. In practice, it is often the DPO who notifies it. In practice, the communication is preferably made by a communications expert, following approval by the management and on the DPO's recommendation.

GDPR obligation for a company	Duties the PO can and cannot carry out
Information security and data protection by design and by default	The most technical task is information security. In practice, this often means the implementation of technical measures. In other words, the extent to which the DPO effectively secures the data or builds in security systems depends primarily on the DPO's knowledge. However, combining the position of DPO with the task of operational security expert is not recommended and even inadvisable. Preferably, the DPO's position is limited to informing, advising and monitoring.
Agreements with partners	The contractual arrangements to be made with a partner are often broader than data protection. In this table we only focus on the arrangements that deal with data protection: the processor agreement. In practice, the DPO will often personally negotiate this agreement with the suppliers. The DPO will ultimately advise the management whether or not to sign the agreement. In doing so, the DPO must also inform the data controller of any shortcomings. Once the agreement has been signed, it is important that it is also respected: here, the DPO can help in his role of data protection supervisor.