contrast

YOUR BUSINESS • FEBRUARY 2021

Time to rethink the appointment of your DPO?

What you need to know.

If your company processes as its main activity and on a large scale either sensitive and/or judicial data, or regularly and systematically monitors data subjects (e.g. online via cookies), you must appoint a Data Protection Officer (DPO). As long as he has the necessary expertise in legislation and practice, your DPO can be either an internal staff member or an external consultant. In addition, your DPO must perform his tasks in complete independence. Amongst other things, this means that he may not receive instructions regarding the exercise of those tasks, that he is protected against any sanctions or dismissal, and that he is bound by secrecy or confidentiality.

The appointment of an internal DPO offers many advantages: the DPO is familiar with the company and also knows its (commercial) interests. In that case, however, safeguarding independence and avoiding conflicts of interest between the position of DPO and any other functions is not always obvious. According to Working Party 29 (WP29), your DPO can indeed not hold a position that leads him to determine the purposes and the means of the processing of personal data.

It is therefore not possible to combine the position of DPO with that of head of a department which the DPO must supervise, for example the audit, risk and compliance department. A manager's position unquestionably entails determining the purposes and means of the processing of personal data within the relevant department.

What you need to do.

Most companies are not obliged to appoint a DPO. Whether you engage a DPO because this is required by law or you decide to do so voluntarily, you should know that the appointment of a DPO comes with far-reaching obligations.

For example, you must **document** your decision on whether or not to appoint a DPO. Keeping track of your decision-making process follows, amongst other things, from the accountability principle imposed by the GDPR. If this decision stipulates the appointment of a DPO, the document must also

demonstrate the DPO's expertise (DPA - [*currently only available in Dutch*]). If a person is found, during the selection procedure, to be the "most suitable" candidate, this does *not* automatically mean that he is also a "sufficiently" suitable candidate (DPA). In addition, it is advisable to also include in this document (i) the tasks and (ii) the absence of a conflict of interest and to regularly re-evaluate this analysis and update the document.

In addition, you must make **all resources available** to your DPO so that he can perform his tasks in complete independence. This includes e.g. active support of the DPO by senior management, access to certain services, continuous training, sufficient time to perform his duties and adequate financial resources, infrastructure and personnel. The more complex or sensitive the processing operations are, the more resources must be allocated to the DPO (DPA). A formal communication within your company regarding the appointment of your DPO, to ensure that the existence and function of the DPO are known, also falls under this obligation.

In order for your DPO to perform his duties, you must **involve him properly and in a timely manner** in all issues, which relate to the protection of personal data. Merely informing the DPO about a decision afterwards is insufficient. In other words, you are obliged to involve your DPO as early as possible, so that he can act as an adviser (WP29 and DPA).

You must also enable your DPO to **report** to the highest management level of your company. This may not be limited to an annual report, as this obligation also applies to *ad hoc* information and advice on obligations for specific intended processing operations (DPA).

Finally, you must also **disclose the contact details** of your DPO to both the competent data protection authority and to the data subjects. The DPO is the first point of contact for both the authority and the data subjects. If they address your company, the DPO is expected to answer.

These obligations ensure that your DPO can correctly carry out his duties (i.e. informing and advising on data protection obligations, monitoring compliance with the GDPR, providing advice on a data protection impact assessment where applicable, cooperating with the authorities and acting as a contact point).

Clearly, the (voluntarily) appointment of a DPO should not be a frivolous decision. Did you appoint a competent DPO when the GDPR first came into force, but does he also head a department? Or is he not getting involved in the analysis of a possible data breach? Or is he not reporting to the board of directors? Then your company is in breach of the GDPR and therefore exposed to the risk of being sanctioned by the authority. Time to rethink the appointment of your DPO?