3/19/2019

Data Protection Office

Roles and Responsibilities of Data Protection Officer

Table of Contents

1. Designation of a data protection officer (DPO) 1

1.1. Mandatory designation 1

1.2. Can an organisation have more than one DPO? 1

1.3. Designation of a Data Protection Officer for each subsidiary/branch 1

1.4. Can the Data Protection Officer be an existing employee? 2

1.4.1. Conflict of interest 2

1.5. Can we contract out the role of the DPO 3

2. Qualifications of the data protection officer 3

Professional qualities and expertise 3

3. Roles of the data protection officer 3

4. What resources should be provided to the DPO by the controller or the processor? 4

5. Liability of a data protection officer 5

Is the DPO personally responsible for non-compliance with data protection requirements? 5

6. References 5

1. Designation of a data protection officer (DPO)

1.1. Mandatory designation

The designation of a data protection officer (DPO) is mandatory according to section 22(2)(e) of the Data Protection Act 2017 (DPA). Thus, this office encourages controllers and processors to appoint a DPO to inform and advise them as well as their employees on their obligations to comply with the DPA and other data protection standards.

The DPO will be the contact point with respect to data subjects, the Data Protection Office and internally within the organisation (controller).

1.2. Can an organisation have more than one DPO?

Organisations need to determine the best way to set up the DPO functions and whether this necessitates a data protection team. If the organisation has a team, it should clearly set out the roles and responsibilities of its team members and how it relates to the DPO.

1.3. Designation of a Data Protection Officer for each subsidiary/branch

The DPA does not specify whether a controller or processor needs to have a single or different Data Protection Officer(s) for its subsidiaries. It is the responsibility of the controller to determine same. For example, a single Data Protection Officer may be designated for several subsidiaries, taking account of their organisational structure and size.

If a single Data Protection Officer is designated, then he or she should be easily accessible from each subsidiary or establishment. The notion of accessibility refers to the tasks of the data protection officer as a contact point with respect to data subjects, the Data Protection Office but also internally within the organisation, considering that one of its roles is to inform and advise the controller and the processor and the employees who carry out processing of personal data of their

obligations under the DPA.

The Data Protection Officer, with the help of a team, if necessary, must be in a position to efficiently communicate with data subjects. The availability of a Data Protection Officer, whether physically on the same premises as employees, via a hotline or other secure means of communication, is essential to ensure that data subjects are able to contact the officer.

Given that the Data Protection Officer is in charge of a variety of tasks, the controller or the processor must ensure that a single Data Protection Officer, with the help of a team if necessary, can perform these efficiently despite being designated for several subsidiaries.

1.4. Can the Data Protection Officer be an existing employee?

A Data Protection Officer can be an existing employee as long as the professional duties of the employee are compatible with the duties of the Data Protection Officer and do not lead to a **conflict of interests**.

1.4.1. Conflict of interest

This means that the DPO cannot hold a position within an organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case. At the same time, the DPO should not be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

The European Data Protection Board (ex Article 29 Working Party) states that as a rule of thumb, conflicting positions within an organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the

organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

1.5. Can we contract out the role of the DPO

You can contract out the role of DPO externally, based on a service contract with an individual or an organisation. It is important to note that an externally appointed DPO should have the same position, tasks and duties as an internally appointed one.

2. Qualifications of the data protection officer

Professional qualities and expertise

A data protection officer is expected to have professional experience and knowledge of data protection laws and standards. The DPO should also have a good knowledge of the business sector of the controller that is how the operations are carried out, as well as the information systems, and data security and data protection needs of the controller.

Regarding personal qualities of a DPO, the latter for instance should be honest with high professional ethics. The DPO's main concern should be enabling compliance with the DPA. Thus, DPO should be chosen judiciously with regard to the data protection issues that arise within the organisation.

3. Roles of the data protection officer

The data protection officer should work within an **independent environment and manner**, report to the highest management level and have adequate resources to enable the controller or the processor to meet its obligations under the DPA.

The following illustrates the minimum tasks that a data protection officer should carry out. However, the controller/processor can add more tasks to meet their business

requirements:

- Inform and advise the controller/processor and its employees about their obligations to comply with the DPA and other data protection laws.
- Monitor compliance with the DPA and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- Be the first point of contact for the Data Protection Office and for individuals whose data are processed (employees, customers, amongst others).

Note: DPOs should not be dismissed or penalised by the controller or the processor for performing [their] tasks'. Example: a DPO may consider that a particular processing is likely to result in high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.

4. What resources should be provided to the DPO by the controller or the processor?

The Data Protection Officer must have the resources necessary to be able to carry out his or her tasks.

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources must be provided to the Data Protection Officer:

- active support of the Data Protection Officer's functions by senior management;
- sufficient time for Data Protection Officer(s) to fulfil their tasks;
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate;
- official communication of the designation of the Data Protection Officer to all staff;

- access to other services within the organisation so that Data Protection Officer(s) can receive essential support, input or information;
- continuous training.

5. Liability of a data protection officer

Is the DPO personally responsible for non-compliance with data protection requirements?

No. DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who is required to ensure and be able to demonstrate that processing is performed in accordance with the DPA. Data protection compliance is the responsibility of the controller or the processor.

Therefore, even though the data protection officer is responsible for assisting the controller or processor in monitoring the internal compliance, the officer is not personally responsible for any non-compliance with the Act by the controller or processor.

6. References

a. The Data Protection Act 2017
b. Article 29 Data Protection Working Party guideline on data protection officers and Article 38(2) of the GDPR