Guidelines on Data Protection Officers (DPO)

The European Data Protection Board (EDPB) on its first meeting (25th May 2018) endorsed the GDPR-related Article 29 Working Party Guidelines, including the Guidelines on Data Protection Officer (DPO)

This document summarises the main aspects of the guidelines.

INTRODUCTION

The GDPR establishes that certain controllers or processors must appoint a DPO: public authorities and bodies, and private organisations that as their core activities monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale (art. 37(1) GDPR). DPOs can also be designated on a voluntary basis.

The main function of the DPO is to facilitate compliance with the GDPR and to act as an intermediary between relevant stakeholders.

It is important to note that the DPOs are not personally responsible in case of non-compliance with the GDPR. It is the controller or processor who is required to ensure and to demonstrate that the processing is performed in accordance with its provisions (art. 24(1) GDPR)

DESIGNATION OF A DPO

Mandatory designation

The GDPR mandates to designate a DPO in three specific cases

a) processing carried out by a public authority or body (art. 37(1)(a) GDPR)

b) where the core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale (art. 37(1)(b) GDPR)

c) where the core activities consist of processing operations on a large scale of sensitive data or data relating to criminal convictions and offences (art. 37(1)(c) GDPR)

Controllers and processors should document the internal analysis carried out to determine whether or not a DPO is to be appointed. And if an organisation designates a DPO on a voluntary basis, arts. 37-39 GDPR will apply to the designation, position and tasks of the DPO.

Interpretation of key concepts

The notion of '**public authority or body**' is determined by national law. While it is not mandatory to designate a DPO where private parties carry out public tasks or exercise public authority, it is recommended.

'**Core activities'** of the controller or the processor refers to the primary activities and do not relate to the processing of personal data as ancillary activities (rec. 97 GDPR). They can also be referred as the key operations necessary to achieve the controller's or processor's goals. Activities where the processing of personal data forms an inextricably part of the controller's or processor's activity should not be excluded.

While there is no precise number to define '**large scale' processing operations**, the WP29 recommended controllers and processors to consider the following factors: a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b) the volume of data and/or the range of different data items being processed; c) the duration, or permanence, of the data processing activities; d) the geographical extent of the processing activities. Examples: processing patient data by a hospital, processing for behavioural advertising by a search engine, processing in the course of the regular business of an insurance company.

'**Regular monitoring'** should be interpreted as one or more of the following: a) ongoing or occurring at particular intervals for a particular period; b) recurring or repeated at fixed times; c) constantly or periodically taking place. '**Systematic monitoring'** should be interpreted as one or more of the following: a) occurring according to a system; b) pre-arranged, organised or methodical; c) taking place as part of a general plan for data collection; d) carried out as part of a strategy. Examples: email retargeting, data-driven marketing activities, loyalty programs, CCTV.

Special categories of personal data and data related to criminal convictions and offences. The text should be read as 'or' instead of 'and'.

Designation of a single DPO for several organisations. Localisation of the DPO

Art. 37(2) GDPR allows a group of undertakings to designate a single DPO provided that he or she is easily accessible from each establishment. The accessibility refers to the tasks of the DPO, and it is not mandatory physical availability.

The WP29 recommends that the DPO is located in the EU, regardless of the location of the controller or processor.

Expertise and skills of the DPO

The level of expertise must be commensurate with the sensitivity, complexity and amount of data an organisation processes. The GDPR does not require a specific degree, but DPOs must have expertise in national and EU data protection laws and practices and in-depth understanding of the GDPR. Knowledge of the business sector and of the organisation of the controller is useful. Likewise, knowledge of the processing activities carried out, and information on systems, data security and data protection needs of the controller. The DPO should act with integrity and high professional ethics.

The DPO can be exercised on the basis of a service contract with an individual or an organisation external to the controller's or processor's organisation.

Publication and communication of the DPO's contact details

Controllers and processors must publish the contact details of the DPO and communicate the contact details of the DPO to the relevant DPA. The DPO is bound by secrecy concerning the performance of his or her tasks.

POSITION OF THE DPO

Involvement of the DPO in all issues relating to the protection of personal data. Resources

It is crucial that the DPO is involved at the earliest possible stage in all issues relating to data protection. The controller and processor must provide the necessary resources to carry out its activities, including active support of his or her functions, even financial, sufficient time to perform its tasks, access to other services, continuous training.

Independency

The DPO must not receive any instructions regarding the exercise of his or her duties. The autonomy of the DPO does not mean that they have decision-making powers extending beyond their tasks pursuant art. 39 GDPR. The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance. If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear.

Dismissal or penalty for performing DPO tasks

The DPO cannot be dismissed or penalised for the performance of their tasks. This is a provision to strengthen the autonomy of the DPO

Conflict of interest

The organisation must ensure that any task and duty do not result in a conflict of interest. The absence of conflict of interest is closely related to the requirement to act in an independent manner. While DPOs are allowed to have other functions, they cannot hold a position within the organisation that lead them to determine the means and purposes of the processing of personal data. Conflicting positions could be: senior management positions, but also roles lower down in the structure if the position leads to the determination of the means and purposes of processing.

TASKS OF THE DPO

Monitoring compliance with the GDPR

As part of the monitoring of compliance with the GDPR DPOs may in particular

- collect information to identify processing activities,

- analyse and check compliance of processing activities,

- inform, advise, and issue recommendations to the controller or processor

Again, monitoring compliance does not mean responsibility for compliance, since the controller and processor are the responsible for compliance with the GDPR.

Role of the DPO in the DPIA

The controller must, under certain circumstances, conduct a DPIA. The DPO only assists the controller in this task providing their advice. In particular, the controller must seek the advice of the DPO to assess:

- whether the DPIA is necessary or not;

- what methodology to follow when carrying out a DPIA;

- whether to carry out a DPIA in-house or whether to outsource it;

- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interest of the data subjects;

- whether or not the DPIA has been correctly carried out and whether its conclusions are compliance with the GDPR;

If the controller must justify any disagreement with the advice of the DPO.

Cooperating with the supervisory authority and acting as a contact point

The DPO should cooperate with the supervisory authority and act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in art. 36, and to consult, where appropriate, with regard to any other matter (art. 39(1)(d) and (e) GDPR). The DPO acts as a facilitator with the supervisory authority. The duty of confidentiality does not prohibit the DPO to seek advice from the supervisory authority.

Role of the DPO in record-keeping

While the obligation of keeping a record of the processing activities lies on the controller or the processor (art. 30(1) and (2) GDPR), they can assign the DPO with the task of maintaining the record of processing operations under the responsibility of the controller or processor.

This briefing was prepared by Federico Marengo for QUBIT PRIVACY

QUBIT PRIVACY is a consultancy firm established in Italy that provides tailor-made services for individuals and companies to comply with the requirements established in the General Data Protection Regulation.

Qubit Privacy

Find more

https://qubitprivacy.com/

Federico Marengo is a lawyer, master in public administration (University of Buenos Aires), LLM (University of Manchester), and PhD candidate (Università Bocconi, Milano).
He currently provides data protection consultancy services for Qubit Privacy and also works as of counsel at Data Business Services.
He is the author of "Data Protection Law in Charts. A Visual Guide to the General Data Protection Regulation", e-book released in 2021, and authored several publications on international data transfers and international trade law.
As a PhD researcher, his research deals with the potential and challenges of the General Data Protection Regulation to protect data subjects against the adverse effects of Artificial Intelligence.
He is also teaching assistant at Università Bocconi.