ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 243

Guidelines on Data Protection Officers ('DPOs')

Adopted on 13 December 2016

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Table of content

1 Introduction

The General Data Protection Regulation ('GDPR'),[1] due to come into effect on 25 May 2018, will provide a modernised, accountability-based compliance framework for data protection in Europe. Data Protection Officers ('DPO's) will be at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR.

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO.[2] This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

The concept of DPO is not new. Although Directive 95/46/EC[3] did not require any organisation to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years.

Before the adoption of the GDPR, the WP29 argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.[4] In addition to facilitating compliance through the implementation of accountability tools (such as facilitating or carrying out data protection impact assessments and audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).

DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.

The controller or the processor also has a crucial role in enabling the effective performance of the DPO's tasks. Appointing a DPO is a first step but DPOs must also be given sufficient autonomy and resources to carry out their tasks effectively.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016).

[2] The appointment of a DPO is also mandatory for competent authorities under Article 32 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131), and national implementing legislation. While these guidelines focus on DPOs under the GDPR, the guidance is also relevant regarding DPOs under Directive 2016/680, with respect to their similar provisions.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[4] See http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks. The aim of these guidelines is to clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law, but also to assist DPOs in their role. The guidelines also provide best practice recommendations, building on the experience gained in some EU Member States. The WP29 will monitor the implementation of these guidelines and may complement them with further details as appropriate.

2 Designation of a DPO

2.1. Mandatory designation

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases:[5]

a) where the processing is carried out by a public authority or body;[6]
b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data[7] or[8] personal data relating to criminal convictions and offences.[9]

In the following subsections, the WP29 provides guidance with regard to the criteria and terminology used in Article 37(1).

Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.[10]

When an organisation designates a DPO on a voluntary basis, the same requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory.

This does not prevent an organisation, which does not wish to designate a DPO on a voluntary basis and is not legally required to designate a DPO, to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data. In this case it is important to ensure that there is no confusion regarding their title, status, position and tasks. Therefore, it should be made clear, in any

[5] Note that under Article 37(4), Union or Member State law may require the designation of DPOs in other situations as well.
[6] Except for courts acting in their judicial capacity.
[7] Pursuant to Article 9 these include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
[8] Article 37(1)(c) uses the word '*and*'. See Section 2.1.5 below for explanation on the use of '*or*' instead of '*and*.'
[9] Article 10.
[10] See Article 24(1).

communications within the company, as well as with data protection authorities, data subjects, and the public at large, that the title of this individual or consultant is not a 'DPO'. [11]

2.1.1 'PUBLIC AUTHORITY OR BODY'

The GDPR does not define what constitutes a '*public authority or body'*. The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.[12] In such cases, the designation of a DPO is mandatory.

A public task may be carried out, and public authority may be exercised[13] not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.

In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.

Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that:

- private organisations carrying out public tasks or exercising public authority designate a DPO and that
- such a DPO's activity should also cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

2.1.2 'CORE ACTIVITIES'

Article 37(1)(b) and (c) of the GDPR refers to the '*core activities of the controller or processor'*. Recital 97 specifies that the core activities of a controller relate to '*primary activities and do not relate to the processing of personal data as ancillary activities*'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.

However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, the core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these

[11] This is also relevant for chief privacy officers ('CPO's) or other privacy professionals already in place today in some companies, who may not always meet the GDPR criteria, for instance, in terms of available resources or guarantees for independence, and therefore, cannot be considered and referred to as DPOs.

[12] See, e.g. the definition of '*public sector body*' and '*body governed by public law*' in Article 2(1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, p. 90).

[13] Article 6(1)(e).

data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.

As another example, a private security company carries out the surveillance of a number of private shopping centres and public spaces. Surveillance is the core activity of the company, which in turn is inextricably linked to the processing of personal data. Therefore, this company must also designate a DPO.

On the other hand, all organisations carry out certain activities, for example, paying their employees or having standard IT support activities. These are necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

2.1.3 'LARGE SCALE'

Article 37(1)(b) and (c) requires that the processing of personal data be carried out on a large scale in order for the designation of a DPO to be triggered. The GDPR does not define what constitutes large-scale, though recital 91 provides some guidance.[14]

Indeed, it is not possible to give a precise number either with regard to the amount of data processed or the number of individuals concerned, which would be applicable in all situations. This does not exclude the possibility, however, that over time, a standard practice may develop, for specifying in objective, quantitative terms what constitutes '*large scale*' in respect of certain types of common processing activities. The WP29 also plans to contribute to this development, by way of sharing and publicising examples of the relevant thresholds for the designation of a DPO.

In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

[14] According to the recital, '*large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk*' would be included, in particular. On the other hand, the recital specifically provides that '*the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer'*. It is important to consider that while the recital provides examples at the extremes of the scale (processing by an individual physician versus processing of data of a whole country or across Europe); there is a large grey zone in between these extremes. In addition, it should be borne in mind that this recital refers to data protection impact assessments. This implies that some elements might be specific to that context and do not necessarily apply to the designation of DPOs in the exact same way.

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

2.1.4 'REGULAR AND SYSTEMATIC MONITORING'

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but the concept of 'monitoring the behaviour of data subjects' is mentioned in recital 24[15] and clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising.

However, the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects.[16]

WP29 interprets 'regular' as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

WP29 interprets 'systematic' as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

[15] *'In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.*

[16] Note that Recital 24 focuses on the extra-territorial application of the GDPR. In addition, there is also a difference between the wording '*monitoring their behaviour'* (Article 3(2)(b)) and *'regular and systematic monitoring of data subjects'* (Article 37(1)(b)) which could therefore be seen as constituting a different notion.

Examples: operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

2.1.5 SPECIAL CATEGORIES OF DATA AND DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

Article 37(1)(c) addresses the processing of special categories of data pursuant to Article 9, and personal data relating to criminal convictions and offences set out in in Article 10. Although the provision uses the word 'and', there is no policy reason for the two criteria having to be applied simultaneously. The text should therefore be read to say 'or'.

2.2. DPO of the processor

Article 37 applies to both controllers[17] and processors[18] with respect to the designation of a DPO. Depending on who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).

It is important to highlight that even if the controller fulfils the criteria for mandatory designation its processor is not necessarily required to appoint a DPO. This may, however, be a good practice.

Examples:

- A small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large-scale', considering the small number of customers and the relatively limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b). At the same time, the family business itself is not under an obligation to designate a DPO.

- A medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c) provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

[17] The controller is defined by Article 4(7) as the person or body, which determines the purposes and means of the processing.

[18] The processor is defined by Article 4(8) as the person or body, which processes data on behalf of the controller.

As a matter of good practice, the WP29 recommends that the DPO designated by a processor should also oversee activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

2.3. 'Easily accessible from each establishment'

Article 37(2) allows a group of undertakings to designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects[19], the supervisory authority[20] but also internally within the organisation, considering that one of the tasks of the DPO is *'to inform and advise the controller and the processor and the employees who carry out processing of their obligations pursuant to this Regulation'*.[21]

In order to ensure that the DPO, whether internal or external, is accessible it is important to ensure that their contact details are available in accordance with the requirements of the GDPR.[22]

He or she must be in a position to efficiently communicate with data subjects[23] and cooperate[24] with the supervisory authorities concerned. This also means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned.

According to Article 37(3), a single DPO may be designated for several public authorities or bodies, taking account of their organisational structure and size. The same considerations with regard to resources and communication apply. Given that the DPO is responsible for a variety of tasks, the controller must ensure that a single DPO can perform these efficiently despite being responsible for several public authorities and bodies.

The personal availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO. The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority.

2.4. Expertise and skills of the DPO

[19] Article 38(4): '*data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this regulation*'.

[20] Article 39(1)(e): '*act as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 and to consult, where appropriate, with regard to any other matter*'.

[21] Article 39(1)(a).

[22] See also Section 2.5 below.

[23] Article 12(1): *'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'*

[24] Article 39(1)(d) *: 'to cooperate with the supervisory authority'*

Article 37(5) provides that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'. Recital 97 provides that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

- **Level of expertise**

The required level of expertise is not strictly defined but it must be commensurate with the sensitivity, complexity and amount of data an organisation processes. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. There is also a difference depending on whether the organisation systematically transfers personal data outside the European Union or whether such transfers are occasional. The DPO should thus be chosen carefully, with due regard to the data protection issues that arise within the organisation.

- **Professional qualities**

Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs should have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs.

Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have sufficient understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller.

In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.

- **Ability to fulfil its tasks**

Ability to fulfil the tasks incumbent on the DPO should be interpreted as both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR, such as the principles of data processing[25], data subjects' rights[26], data protection by design and by default[27],

[25] Chapter II.
[26] Chapter III.
[27] Article 25.

records of processing activities[28], security of processing[29], and notification and communication of data breaches.[30]

- **DPO on the basis of a service contract**

The function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation. In this latter case, it is essential that each member of the organisation exercising the functions of a DPO fulfils all relevant requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract for activities as DPO but also no unfair dismissal of any individual member of the organisation carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.

For the sake of legal clarity and good organisation it is recommended to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be useful to specify these points in the service contract.

2.5. Publication and communication of the DPO's contact details

Article 37(7) of the GDPR requires the controller or the processor:

- to publish the contact details of the DPO and
- to communicate the contact details to the relevant supervisory authorities.

The objective of these requirements is to ensure that data subjects (both inside and outside of the organisation) and the supervisory authorities can easily, directly and confidentially contact the DPO without having to contact another part of the organisation.

The contact details of the DPO should include information allowing data subjects and the supervisory authorities to reach the DPO in an easy way (a postal address, a dedicated telephone number, and a dedicated e-mail address). When appropriate, for purposes of communications with the public, other means of communications could also be provided, for example, a dedicated hotline, or a dedicated contact form addressed to the DPO on the organisation's website.

Article 37(7) does not require that the published contact details should include the name of the DPO. Whilst it may be a good practice to do this, it is for the controller and the DPO to decide whether this is necessary or helpful in the particular circumstances.[31]

As a matter of good practice, the WP29 recommends that an organisation informs the supervisor authority and employees of the name and contact details of the DPO. For example, the name and

[28] Article 30.
[29] Article 32.
[30] Articles 33 and 34.
[31] It is notable that Article 33(3)(b), which describes information that must be provided to the supervisory authority and to the data subjects in case of a personal data breach, unlike Article 37(7), specifically also requires the name (and not only the contact details) of the DPO to be communicated.

contact details of the DPO could be published internally on organisation's intranet, internal telephone directory, and organisational charts.

3 Position of the DPO

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

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO be *'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'*.

It is crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.[32] Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, ensure a privacy by design approach and should therefore be standard procedure within the organisation's governance. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she is part of the relevant working groups dealing with data processing activities within the organisation.

Consequently, the organisation should ensure, for example, that:

- The DPO is invited to participate regularly in meetings of senior and middle management.
- His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
- The DPO must be promptly consulted once a data breach or another incident has occurred.

Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.

3.2. Necessary resources

Article 38(2) of the GDPR requires the organisation to support its DPO by *'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'.* The following items, in particular, are to be considered:

- Active support of the DPO's function by senior management (such as at board level).
- Sufficient time for DPOs to fulfil their duties. This is particularly important where the DPO is appointed on a part-time basis or where the employee carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a

[32] Article 35(2).

percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.

- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- Official communication of the designation of the DPO to all staff to ensure that their existence and function is known within the organisation.
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- Continuous training. DPOs should be given the opportunity to stay up to date with regard to developments within data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.
- Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.

In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out.

3.3. Instructions and 'acting in an independent manner'

Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers/processors are required to ensure that the DPO '*does not receive any instructions regarding the exercise of [his or her] tasks.*' Recital 97 adds that DPOs, '*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*'.

This means that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.

The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.

The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.[33] If the controller or processor makes decisions that are incompatible

[33] Article 5(2).

with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to those making the decisions.

3.4. Dismissal or penalty for performing DPO tasks

Article 38(3) also requires that DPOs should *'not be dismissed or penalised by the controller or the processor for performing [their] tasks'*.

This requirement also strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.

Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a 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.

Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.

As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).

In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

3.5. Conflict of interests

Article 38(6) allows DPOs to '*fulfil other tasks and duties'*. It requires, however, that the organisation ensure that '*any such tasks and duties do not result in a conflict of interests'*.

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the 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.[34]

[34] As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources

Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:

- to identify the positions which would be incompatible with the function of DPO
- to draw up internal rules to this effect in order to avoid conflicts of interests
- to include a more general explanation about conflicts of interests
- to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement
- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.

4 Tasks of the DPO

4.1. Monitoring compliance with the GDPR

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO '*should assist the controller or the processor to monitor internal compliance with this Regulation*'.

As part of these duties to monitor compliance, DPOs may, in particular:

- collect information to identify processing activities,
- analyse and check the compliance of processing activities, and
- inform, advise and issue recommendations to the controller or the processor.

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.

4.2. The DPO's role in a data protection impact assessment

According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller '*shall seek advice'* of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to '*provide advice where requested as regards the [DPIA] and monitor its performance*'.

---

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.

The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others [35]:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the 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 interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account[36].

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.

4.3. Risk-based approach

Article 39(2) requires that the DPO '*have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing*'.

This article recalls a general and common sense principle, which may be relevant for many aspects of a DPO's day-to-day work. In essence, it requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks. This does not mean that they should neglect monitoring compliance of data processing operations that have comparatively lower level of risks, but it does indicate that they should focus, primarily, on the higher-risk areas.

This selective and pragmatic approach should help DPOs advise the controller what methodology to use when carrying out a DPIA, which areas should be subject to an internal or external data protection audit, which internal training activities to provide to staff or management responsible for data processing activities, and which processing operations to devote more of his or her time and resources to.

---

[35] Article 39(1) mentions the tasks of the DPO and indicates that the DPO shall have '*at least'* the following tasks. Therefore, nothing prevents the controller from assigning the DPO other tasks than those explicitly mentioned in Article 39(1), or specifying those tasks in more detail.

[36] Article 24(1) provides that '*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure **and to be able to demonstrate** that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*'.

4.4. The DPO's role in record-keeping

Under Article 30(1) and (2), it is the controller or the processor, not the DPO, who is required to '*maintain a record of processing operations under its responsibility*' or *'maintain a record of all categories of processing activities carried out on behalf of a controller'*.

In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.[37]

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.

[37] Article 24(1)(d), Regulation (EC) 45/2001.

WP243 ANNEX - FREQUENTLY ASKED QUESTIONS

The objective of this annex is to answer, in a simplified and easy-to-read format, some of the key questions that organisations may have regarding the new requirements under the GDPR to appoint a DPO.

Designation of the DPO (Article 37)

1 Which organisations are required to appoint a DPO? (Article 37(1))

The GDPR requires the designation of a DPO in three specific cases:

- where the processing is carried out by a public authority or body (irrespective of what data is being processed);
- where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; and
- where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Note that Union or Member State law may require the designation of DPOs in other situations as well. Finally, when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

For more information, see section 2.1 of the Guidelines.

2 What does the notion of 'core activities' mean? (Article 37(1)(b) and (c))

'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms as inextricable part of the controller's or processor's activity. For example, processing health data, such as patient's health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs.

On the other hand, all organisations carry out certain supporting activities for example, paying their employees or having standard IT support activities. These are necessary support functions for the organisation's core activity or main business. Even though these activities are necessary or essential, they are usually considered ancillary functions rather than the core activity.

For more information, see section 2.1.2 of the Guidelines.

3 What does the notion of 'large scale' mean? (Article 37(1)(b) and (c))

The GDPR does not define what constitutes large-scale. The WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

For more information, see section 2.1.3 of the Guidelines.

4 What does the notion of 'regular and systematic monitoring' mean? (Article 37(1)(b))

The notion of regular and systematic monitoring of data subjects is not defined in the GDPR, but clearly includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment.

WP29 interprets 'regular' as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

WP29 interprets 'systematic' as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

Examples: operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring,

establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.

For more information, see section 2.1.4 of the Guidelines.

5 Can organisations appoint a DPO jointly? If so, under what conditions? (Articles 37(2) and (3))

The GDPR provides that a group of undertakings may designate a single DPO provided that he or she is '*easily accessible from each establishment*'. The notion of accessibility refers to the tasks of the DPO as a contact point with respect to data subjects, the supervisory authority and also internally within the organisation. In order to ensure that the DPO, whether internal or external, is accessible it is important to ensure that their contact details are available in accordance with the GDPR. The DPO must be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned. The personal availability of a DPO (whether physically on the same premises as employees, via a hotline or other secure means of communication) is essential to ensure that data subjects will be able to contact the DPO.

For more information, see section 2.3 of the Guidelines.

6 Is it possible to appoint an external DPO (Article 37(6))?

Yes. According to Article 37(6), the DPO may be a staff member of the controller or the processor (internal DPO) or 'fulfil the tasks on the basis of a service contract'. This means that the DPO can be external, and in this case, his/her function can be exercised based on a service contract concluded with an individual or an organisation.

If the DPO is external, all the requirements of Articles 37 to 39 apply to such a DPO. As stated in the Guidelines, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the DPO tasks as a team, under the responsibility of a designated lead contact and 'person in charge' of the client. In this case, it is essential that each member of the external organisation exercising the functions of a DPO fulfils all relevant requirements of the GDPR.

For the sake of legal clarity and good organisation, the Guidelines recommend to have, in the service contract, a clear allocation of tasks within the external DPO team and to assign a single individual as a lead contact and person 'in charge' of the client.

For more information, see sections 2.3, 2.4 and 3.5 of the Guidelines.

7 What are the professional qualities that the DPO should have (Article 37(5))?

The GDPR requires that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'.

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

The necessary skills and expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR
- understanding of the processing operations carried out
- understanding of information technologies and data security
- knowledge of the business sector and the organisation
- ability to promote a data protection culture within the organisation

For more information, see section 2.4 of the Guidelines.

Position of the DPO (Article 38)

8 What are the resources that should be provided to the DPO to carry out her/his tasks?

Article 38(2) of the GDPR requires the organisation to support its DPO by *'providing resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain his or her expert knowledge'.*

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- Active support of the DPO's function by senior management
- Sufficient time to for DPOs to fulfil their duties
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- Official communication of the designation of the DPO to all staff
- Access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- Continuous training

For more information, see section 3.2 of the Guidelines.

9 What are the safeguards to enable the DPO to perform her/his tasks in an independent manner (Article 38(3))?

Several safeguards exist in order to enable the DPO to act in an independent manner as stated in recital 97:

- No instructions by the controllers or the processors regarding the exercise of the DPO's tasks
- No dismissal or penalty by the controller for the performance of the DPO's tasks
- No conflict of interest with possible other tasks and duties

For more information, see sections 3.3 to 3.5 of the Guidelines.

10 What are the 'other tasks and duties' of a DPO which may result in a conflict of interests (Article 38(6))?

The DPO cannot hold a position within the 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.

As a rule of thumb, conflicting positions 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.

For more information, see section 3.5 of the Guidelines.

Tasks of the DPO (Article 39)

11 What does the notion of 'monitor compliance' with the GDPR encompass (Article 39(1)b)?

As part of these duties to monitor compliance, DPOs may, in particular:

- collect information to identify processing activities,
- analyse and check the compliance of processing activities, and
- inform, advise and issue recommendations to the controller or the processor.

For more information, see section 4.1 of the Guidelines.

12 Is the DPO personally responsible for non-compliance with the GDPR?

No, DPOs are not personally responsible for non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation' (Article 24(1)). Data protection compliance is the responsibility of the controller or the processor.

13 What is the role of the DPO with respect to the data protection impact assessment (Article 37(1)(c) and the record of processing activities (Article 30)?

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:

- whether or not to carry out a DPIA;
- what methodology to follow when carrying out a DPIA;
- whether to carry out the 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 interests of the data subjects;
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

For more information, see section 4.2 of the Guidelines.

As far as the record of processing activities is concerned, it is the controller or the processor, not the DPO, who is required to maintain a record of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

For more information, see section 4.4 of the Guidelines.