A&L Goodbody

WP29 Guidance on DPOs

The Article 29 Working Party (**WP29**) has published **Guidelines on Data Protection Officers (DPOs).**

The guidelines aim to assist organisations with determining whether a DPO needs to be appointed, the professional qualifications a DPO should have, their tasks, and their potential liability. The guidelines will also help DPOs in understanding the scope of their role.

Mandatory Designation

The GDPR introduces a mandatory obligation for controllers and processors to appoint a DPO in three specific circumstances, including:

- If you are a public authority or body;
- If your core activities require regular and systematic monitoring of data subjects on a large scale; or
- If your core activities involve large scale processing of sensitive data or data relating to criminal convictions and offences (Article 37(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 by national law, and would typically include national, regional and local authorities, and other bodies governed by public law. The WP29 recommends, as good practice, that private organisations carrying out public tasks or exercising public authority should also appoint a DPO. Such a DPO's activity would cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty.

"Core Activities"

The recitals highlight that the *"core activities"* of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities (Recital 97). The WP29 considers that *"core activities"* are the key operations necessary to achieve the controller's or processor's goals.

"Large scale"

The GDPR does not define what constitutes *"large scale processing"*, but the WP29 recommends that the following factors are considered:

- The number of data subjects – either as a specific number or proportion of the relevant population;
- The volume of data and/or range of different data items being processed;
- The duration of the processing; and
- The geographical extent of the processing.

The WP29 gives examples of *"large scale processing"*, including:

- Processing of patient data in the regular course of business by a hospital;
- Processing of customer data in the regular course of business by an insurance company or bank;
- Processing of personal data for behavioural advertising by a search engine; or
- Processing of data (content, traffic, location) by telephone or internet service providers.

"Regular and systematic monitoring"

The notion of *"regular and systematic monitoring"* of data subjects is not defined, but the WP29 provides examples, including: data-driven marketing activities; profiling and scoring for risk-assessment purposes; location tracking; behavioural advertising; CCTV usage, and monitoring of fitness and health via wearable devices.

Do both the controller and processor need to appoint a DPO?

The GDPR requires both controllers and processors to appoint a DPO, depending on who fulfils the criteria for mandatory designation. In some cases only the controller or only the processor may need to appoint a DPO. The WP29 provides, as an example, a small family business (a controller) which uses the services of a processor whose core activity is to provide website analytic services and assistance with targeted advertising. The activities of the family business and its customers do not generate processing on a large-scale, considering its small number of customers and limited activities, and thus the family business does not need to appoint a DPO. However, the activities of the processor, having many customers like the small business, taken together, are carrying out large-scale processing. The processor must therefore appoint a DPO.

Voluntary Designation

Even when the GDPR does not specifically require the appointment of a DPO, organisations may find it useful to appoint a DPO on a voluntary basis to help facilitate compliance with the GDPR, and act as an intermediary with the supervisory authority, data subjects, and cross-functional teams within an organisation. The WP29 encourages such voluntary appointments of DPOs.

However, the WP29 highlights that when an organisation designates a DPO on a voluntary basis, the statutory obligations of a DPO set out in Articles 37 to 39 of the GDPR will apply as if the designation had been mandatory. Therefore, if an organisation does not wish a voluntary DPO to be subject to such statutory obligations, it should be made clear in communications within the organisation, as well as with supervisory authorities, data subjects and the public at large, that the title of the individual or consultant is not a DPO.

Qualifications and Tasks of DPO

The GDPR does not specify the professional qualities or level of expertise required for a DPO, but the WP29 states it should be commensurate with the sensitivity, complexity and amount of data an organisation processes.

A DPO may be a staff member or fulfil the role on the basis of a service contract (Article 37(6)). In the event that a DPO carries out other tasks and duties, they must not result in a conflict of interests. The WP29 notes, for example, that conflicting positions may include senior management positions, such as chief executive or chief operating officer, or head of marketing, Human Resources or IT departments. In addition, a conflict of interests may arise if an external DPO is asked to represent the controller or processor before the courts in cases involving data protection issues. The absence of conflict of interests is closely linked to the requirement for the DPO to act in an independant manner.

The GDPR sets out a DPO's tasks as, at the minimum, including:

- To inform and advise the controller or processor and employees who carry out processing of their statutory obligations under the GDPR and other relevant EU or national data protection law;
- To monitor compliance with the GDPR, and with other EU or national data protection obligations and with the data protection policies of the controller or processor, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and related audits;
- To provide advice on data protection impact assessments (DPIAs);
- Cooperate with the supervisory authority; and
- To act as a contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter (Article 39(1)).

Although the statutory obligation to maintain records of processing activities lies with the controller or processor (Article 30), the WP29 highlights that there is nothing preventing the controller or processor from assigning the DPO with that task. Such records may assist the DPO with monitoring an organisation's GDPR compliance.

In fulfilling their tasks, DPOs must not be instructed on how to deal with a matter, for instance, how to investigate a complaint or whether to consult a supervisory authority and must directly report to the highest management level (e.g. board of directors) (Article 38(3)). Organisations are required to provide DPOs with the necessary resources to complete their tasks and for their ongoing training (Article 38(2)).

Publication and communication of DPO's contact details

The GDPR requires the contact details of the DPO to be published and to be communicated to the supervisory authority, so that the DPO can be easily reached (Article 37(7)). In the WP29's opinion, the contact details which should be published include: the postal address, a dedicated telephone number, and/or a dedicated email address of the DPO, but not necessarily the name of the DPO. However, the name of the DPO should be communicated to the supervisory authority. As a matter of good practice, the WP29 also recommends that an organisation informs its employees of both the name and contact details of the DPO, on the company's intranet, internal telephone directory and organisational charts.

Group companies can appoint a single DPO provided he or she is easily accessible from each establishment (Article 32(2)). The WP29 recommends, where feasible, that the DPO be located within the EU, whether or not the controller or processor is established within the EU.

Liability

Data protection compliance is the responsibility of the controller or processor, and the WP29 helpfully clarifies that DPOs will not be personally responsible in the event of non-compliance with the GDPR.

Conclusion

It is vital that companies start considering now whether they are required to appoint a DPO, and if so, how best to recruit, train and resource the position, as the appointee will need to be in place by 25 May 2018.

In cases where it is not clear whether a DPO needs to be appointed, the WP29 recommends that controllers and processors document the internal analysis carried out to determine whether or not a DPO is required. Such documentation will assist companies with demonstrating to the supervisory authority that the relevant factors were taken into account.

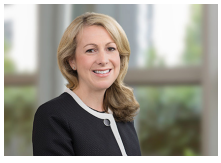
CONTACT US

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Claire Morrissey
Partner, Dublin
+353 1 649 2246
cmorrissey@algoodbody.com

Mark Rasdale
Partner
+353 1 649 2300
mrasdale@algoodbody.com



Davinia Brennan
Associate & Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com