Deloitte.

The Role of the Data Protection Officer

Key points of the recent ODPC guidance and the Article 29 Working Group Guidance

September 2017

Introduction

Key points of the recent ODPC guidance, and the Article 29 working group guidance

The Article 29 Working Party (WP29) adopted guidance on the role of the Data Protection Officer (DPO) under the new General Data Protection Regulation (GDPR) last April 2017. In Ireland, the Office of the Data Protection Commissioner has recently issued (dated 14/08/17) their guidance on the appropriate qualifications for the DPO role. Under the GDPR, it is a requirement for certain data controllers and data processors to designate a DPO for their organisations. This designated DPO will play a leading and crucial role in implementing an effective data protection framework that complies with the new requirements as set out under the GDPR.

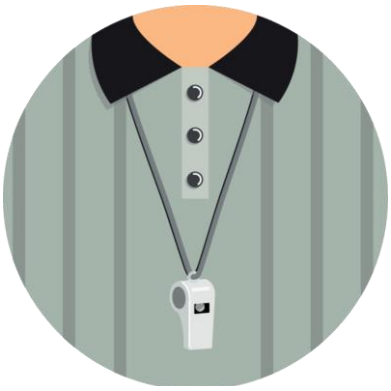
We summarise the key points of the guidance as follows:

Mandatory Designation

Under Article 37(1) of the GDPR, data controllers and processors must designate a DPO in any case where:

(a) The processing is carried out by a public authority or body except for courts acting in their judicial capacity;
(b) the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

The WP29 has clarified some of the key criteria around the mandatory designation of a DPO as follows:



1. Record

The WP29 has recommended that controllers and processors keep a record of the internal analysis carried out to determine whether or not a DPO is to be appointed in order to demonstrate that all relevant factors have been taken into account. Keeping this record also satisfies the accountability principle under the GDPR and must be considered an updateable and 'live' document.

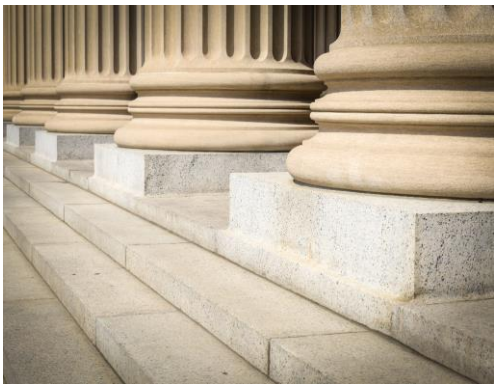
2. Public Authority or Body

The WP29 considers that what constitutes a 'public authority or body' is to be determined under national law and that these bodies must appoint a DPO. Furthermore, other natural or legal persons governed by public or private law (e.g. Public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulatory professions) are not obliged to appoint a DPO but the WP29 recommends it as good practice.

3. Core activities of the controller/processor

'Core activities of the controller or processor' is understood to relate to primary activities and key operations necessary to achieve the organisations goal (e.g. Hospitals using health data to provide healthcare or security companies carrying out surveillance) and does not relate to the processing of personal data as ancillary activities (e.g. Organisations processing payroll data of their employees).

4. Large Scale



The WP29 recommends the following factors in determining whether processing is 'large scale':

- Number of data subjects concerned
- Volume of data and/or range of different data items being processed
- Duration or permanence of the data processing activity
- Geographical extent of the processing activity

Some examples listed by the WP29 of large scale processing are called out as the 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.

5. Regular and Systematic Monitoring

'Regular and Systematic Monitoring' of data subjects is interpreted by the WP29 as meaning:

- *Regular:* ongoing or occurring at particular intervals for a particular period, recurring or repeated at fixed times, constantly or periodically taking place.
- *Systematic:* 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.

Some examples listed by the WP29 of regular and systematic monitoring are in relation to all forms of tracking, profiling and monitoring of the behaviour of data subjects such as targeted marketing activities, profiling and scoring for a risk assessment (fraud prevention AML controls, credit scoring, calculation of insurance premiums etc.), location tracking etc.

DPO for the Data Processor

The requirements under the GDPR apply to data controllers and data processors alike but it depends on who will fulfil the mandatory designation criteria above as to whether a DPO had to be appointed. The WP20 specifically states that even if it is only the data controller that fulfils the mandatory designation, it may be good practice for the data processor to appoint a DPO regardless.

Designation of a single DPO for several organisations

A group of undertakings may appoint a single DPO as long as that person is easily accessible from each establishment (see next point). In addition a single DPO can be appointed for several public authorities or bodies depending on their structure and size and with the help of a team if necessary.

Easily accessible from each establishment

The accessibility of the DPO, according to the WP29, refers to the actual tasks of the DPO as a contact point for data subjects and cooperation with the supervisory body. If there is to be a single DPO for a group of undertakings efficient communication and carrying out of key tasks is key across all languages if necessary. The personal availability of the DPO is also crucial to ensure data subjects can contact him/her. The WP29 recommends that the DPO be located within the European Union in order to be accessible but they do acknowledge that if the controller or processor is not established within the EU, it may be more effective the DPO carried out his/her activities outside the EU also.

Expertise and skills of the DPO

1. Expertise

According to the WP29 and the ODPC, the required level of expertise is not defined but it must be commensurate with the sensitivity, complexity and amount of data that the organisation processes. Expertise must also be taken into account if the organisation systematically transfers personal data outside of the European Union.

2. Professional Qualifications

Regarding professional qualifications, it is relevant that the DPO has expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. The DPO must also have knowledge of the business sector of the organisation and understand any processing activities, IT systems, and security and data protection needs of the organisation. The ODPC recommends that organisations should proactively decide on the qualifications and level of training required for the DPO and further recommends that the following non-exhaustive list be taken into consideration when selecting a training programme:

Non-exhaustive list of considerations when selecting a training programme:

–the content and means of the training and assessment;

–whether training leading to certification is required;

–the standing of the accrediting body; and

–whether the training and certification is recognised internationally

3. Ability to fulfil its tasks

Ability to fulfil its tasks refers to the integrity and high professional ethics of the individual named as DPO as well as enabling and fostering compliance with the GDPR and data protection through elements such as the principles of data processing, data subject rights, data protection by design and by default, record keeping of processing activities, security of processing and breach notification and handling.

4. Appointing the DPO on the basis of a service contract

Appointing the DPO on the basis of a service contract can be concluded with an individual or an organisation outside of the controllers or processors organisation ensuring that there are no conflicts of interests and that such individual is protected by the provisions of the GDPR. A team of individuals can also be structured in order to efficiently serve clients as long as there is clear allocation of tasks and a lead contact and person in charge for each client. These points should be covered under the service contract.

Publication and communication of the DPO's contact details

This requirement under GDPR ensures that the contact details of the DPO should include information allowing data subjects and the supervisory authority to reach the DPO easily (address, phone, email address, dedicated hotline or dedicated contact form on an organisation's website). The requirement does not extend to the DPO's name but it may be best practice and is for the DPO and the organisation to decide.

The WP29 recommends that an organisation informs the supervisory authority and employees of the name and contact details of the DPO as good practice.

Position of the DPO

The WP29 stresses that it is crucial that the DPO is involved from the earliest stage possible in all data protection matters. The DPO must be involved early in relation to data protection impact assessments. This is crucial to complying with the privacy by design requirement under GDPR. The DPO must also be part of any discussion or working groups dealing with data processing activities of the organisation. The WP29 recommend developing data protection guidelines or programmes that set out when a DPO must be consulted to ensure they are part of the decision making processes for privacy implications and that they are consulted promptly in the case of a data breach or any other privacy incidents.

Necessary Resources

The WP29 call out the following as being necessary resources:

- Active support of the DPO by senior management (such as board level)
- Sufficient time to fulfil their duties
- Financial, infrastructure and staff resources
- Official communication of the DPO appointment to all employees
- Access to stakeholders such as HR, Legal, IT, Security etc.
- Continuous training
- A DPO team depending on the size and structure of the organisation

Acting in an independent manner

DPO's must not be instructed how to deal with a matter according to the WP29 and they must not be instructed to take a certain view of a data protection issue. The controller or processor does remain responsible for compliance however, and must be able to demonstrate compliance. If they make decisions that go against the DPO's advice, the DOP must be able to make his opposing opinion clear.

Currently, data protection generally sits within compliance or other functions such as data governance or information security but the new requirements could prevent the DPO reporting into the heads of these functions due to a potential conflict of interest and the requirement for the DPO to act in an independent manner.

The DPO and these heads of functions could be the same person but the general thinking is that this could cause an independence and workload issue. There will therefore be some grey areas between these heads of functions and the DPO in terms of roles and responsibilities.

Conflicts of interests

The DPO may fulfil other tasks and duties however, these duties must not conflict with their data protection duties. The independence requirement is strengthened here and a DPO cannot hold a position within an organisation that leads him/her to determine the purposes and means of processing personal data.

Tasks of the DPO

The DPO must monitor compliance with the GDPR. In order to do this, the DPO may:

- Collect information to identify processing activities
- Analyse and check compliance of any processing activities
- Inform, advise and issue recommendations

Data Protection Impact Assessments: It is the task of the controller to carry out data protection impact assessments but the DPO must assist and provide advice to the controller in terms of whether or not to carry out an assessment, the risk-based methodology to use, mitigating controls and whether or not it has been carried out accurately and the conclusions comply with the GDPR.

Record-keeping: DPOs can be assigned the task of maintaining the record of processing activities under the responsibility of the controller. This record will be considered a tool to enable the DPO to perform its tasks of monitoring compliance and informing and advising the controller or processor.

For more information on the DPO requirements under the GDPR or for any data protection and privacy questions including tailored GDPR and DPIA assessments, please contact the Deloitte Ireland Data Privacy Services team.

Dismissal or penalty for performing DPO tasks

The DPO must not be penalised for carrying out his/her duties or giving advice that the controller or processor disagrees with.

Contact

Sean Smith
Partner| Risk Advisory
Email: seansmith1@deloitte.ie

Donal Murray
Director | Risk Advisory
Email: donmurray@deloitte.ie

Nicola Flannery
Senior Manager | Risk Advisory
Email: niflannery@deloitte.ie

Deloitte.