Considering appointing a DPO - Issues to consider?

This note sets out consideration that should be taken into account when appointing a Data Protection Officer ("DPO") under the General Data Protection Regulation ("GDPR") that comes into force on the 25th May 2018.

Mandatory or voluntary appointment

Mandatory

Article 37(1) of the GDPR defines three situations in which designation of a DPO is mandatory:

(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 the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the *core activities* of the controller or the processor consist of processing on a *large scale* of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Article 29 Data Protection Working Party in its Guidelines on DPOs adopted on 5 April 2017 ('WP29 Guidelines') provided guidance on the terms '*public authority or body', 'core activities', 'large scale' and 'regular and systematic monitoring'.*

'Public authority or body' has to be determined by national law. The concept includes national, regional and local authorities and a range of other bodies governed by public law[1].

'*Core activities'* are defined as key operations necessary to achieve the controller's or processor's goals, and are distinguished from *ancillary activities.* By way of example, core activities of a hospital include provision of health care and processing health data, such as patients' health records. Paying hospital employees or carrying out standard IT support activities are considered ancillary as they only support the core activities[2].

'Large scale' – the WP29 Guidelines recommend to take into account the following factors:

- 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.

For example, processing of patient data in the regular course of business by a hospital constitutes processing on a large scale while processing of patient data by an individual physician does not. Processing of personal data relating to criminal convictions and offences by an individual lawyer is also not considered to be the processing on a large scale[3].

'Regular and systematic monitoring' is interpreted in the WP29 Guidelines as follows:

[1] Para 2.1.1 of the WP29 Guidelines
[2] Para 2.1.2 of the WP29 Guidelines
[3] Para 2.1.3 of the WP29 Guidelines

'*Regular'* means 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[4].

'Systematic' means one or more of the following:

- Occurring according to a system;
- Pre-arranged, organized or methodical;
- Taking place as part of a general plan for data collection;
- Carried out as part of a strategy[5].

Examples provided by WP29 Guidelines include: 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; behavioral 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.

Voluntary

It is recommended therefore to conduct analysis based on the requirements of Article 37(1) of the GDPR to determine if the appointment of a DPO is necessary. It is conceivable however that after such analysis the controller or processor may not reach a definitive conclusion on whether or not the requirement to designate a DPO is applicable to them. In such a case it is probably prudent to designate a DPO considering that the fines for failure to designate a DPO, should it be deemed necessary by the supervisory authority, are up to EURO 10 million or 2 % of the previous year's total worldwide turnover[6].

There are certain advantages in designating a DPO even if the controller or processor is not required to do so, i.e. on the voluntary basis. The DPO plays a key role in fostering a data protection culture within the organization and helps to implement essential elements of the GDPR, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches[7]. However, it is important to note that any voluntary DPO appointments will need to comply with the requirements of Articles 37 to 39 of the GDPR.

If however the controller or processor decides against designation of a DPO it is recommended to document this decision including the rational for such decision in order to demonstrate compliance with requirements of the GDPR relating to data protection officers.

[4] Para 2.1.4 of the WP29 Guidelines
[5] Para 2.1.4 of the WP29 Guidelines
[6] Para 4(a) Article 83 of the GDPR
[7] Para 2.5 of the WP29 Guidelines

It is important to avoid referring to the individuals that are involved in the process of compliance as “data protection officers” because this would subject them to the requirements of Articles 37 to 39. To minimise the risk of being subjected to the requirements of Articles 37 to 39, an organisation may share the DPO’s responsibilities among a number of individuals or departments in relevant fields, i.e. legal department, compliance, HR, IT etc. It appears however that this would only work in a small size organisation or one with very simple operations and structure. Most organisations of medium or large size would find that they need to have a single point of coordination of GDPR compliance activities which would make this person(s) a *de facto* DPO.

DPO for a number of undertakings

Paragraphs 2, 3 and 4 of Article 37 of the GDPR permit the appointment of a single DPO for a number of undertakings:

- Paragraph 2 – for group companies;
- Paragraph 3 –for several public authorities or bodies;
- Paragraph 4 – for associations and other bodies representing categories of controllers or processors.

The requirement of easy accessibility of the DPO for each establishment in such a joint appointment is set out in paragraph 2 but it should equally be applicable to paragraphs 3 and 4.

Internal or external appointment

Paragraph 6 of Article 37 gives flexibility to organisations to either employ a DPO or engage one on the basis of a service contract with an individual or an external organisation. This choice should be made based on the specific circumstances and requirements of the controller or processor.

Both internally or externally appointed DPOs are subject to the provisions of Articles 37 to 39 of the GDPR, including requirements for independence, competencies, absence of conflict of interests etc.

Individual or collective DPO

If an external organisation (as opposed to an individual) is engaged to exercise functions of a DPO then the likelihood is that they will have a number of qualified staff members working as a team that could perform a DPO’s functions more efficiently than a single individual.

Can an employer authorise several employees to perform the functions of a DPO? Yes. WP29 Guidelines provides that given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff)[8].

[8] Para 3.2 of the WO29 Guidelines

Where the functions of a DPO is performed by a group of people, either external organisation or an internal DPO team:

- for the sake of legal clarity and good organisation and to prevent conflicts of interests for the team members, there must be clear allocation of tasks and responsibilities[9][10];
- each member of that external organisation or the team must fulfil the requirements of Articles 37 to 39 of the GDPR, specifically on the conflict of interests[11].

In addition to the above, in case if an external organisation is performing the functions of a DPO:

- a single individual must be assigned as a lead contact for the client and person 'in charge'[12][13];
- all of the above points must be specified in the service contract[14].

Tasks of a DPO

DPO's obligations are set out in paragraph 1 of Article 39 of the GDPR and include the following:

- To inform and advise the organisation and its employees on their obligations in relation to the personal data processing;
- To monitor compliance, including the assignment of responsibilities, awareness raising, training of staff and related audits;
- To provide advice with regard to the data protection impact assessment;
- To cooperate with and to act as the contact point for the supervisory authority.

It is important to consider the role of a DPO during the stage of implementation of compliance with GDPR. While the organisation may be tempted to delegate the responsibility for the implementation to the DPO, it goes against the spirit of the GDPR.

Article 39 of GDPR indicates the DPO is acting in a consulting, advisory and monitoring capacity. Article 5.2 of the GDPR states that it is the controller's responsibility to comply and to demonstrate compliance with the principles of the GDPR on the processing of personal data. Presumably, the same applies to the processor. WP29 Guidelines add that the DPO helps to implement essential elements of the GDPR[15].

Depending on the size of the organisation and the level of their compliance with the existing data protection legislation it could be a very complicated project with large scope covering many functions and actions to be completed. It should be approached as a project with identified

[9] Para 2.5 of the WP29 Guidelines
[10] Para 3.2 of the WO29 Guidelines
[11] Para 2.5 of the WP29 Guidelines
[12] Para 2.5 of the WP29 Guidelines
[13] Para 3.2 of the WP29 Guidelines
[14] Para 2.5 of the WP29 Guidelines
[15] Para 2.5 of the WP29 Guidelines

stakeholders, established goals, defined deliverables, a project schedule, identification of issues and a completed risk assessment. A project team, e.g. consisting of a Steering Committee and a Working Group, should be set up in order to drive the project forward. The DPO shall be involved, properly and in a timely manner[16] as a member of the project team in order to give appropriate advice and monitor compliance with the GDPR but should not be in charge of implementation.

Competencies

Paragraph 5 of Article 37 of 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 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.

There is no formal education that prepares DPOs which makes the task of recruiting a DPO a difficult one. A legal professional is a suitable candidate provided he or she fulfils the requirements of the GDPR discussed below.

The level of expertise must be commensurate with the sensitivity, complexity and amount of personal data an organisation processes[17]. In other words, the more complex the processes in the organization the higher level of expertise is required. Based on the WP29 Guidelines, a good candidate for a DPO role is expected to have the following competencies:

- Expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR;
- Knowledge of the business sector and of the organisation of the controller (or the processor);
- Good understanding of the processing operations carried out;
- Good understanding of the information systems, and data security and data protection needs of the controller (or the processor);
- In case of a public authority or body, a sound knowledge of the administrative rules and procedures of the organization;
- Integrity and high professional ethics[18].

The DPO is required to promote a data protection culture within the organization, provide advice to the organization[19], training to the employees[20], act as the contact point for the supervisory authority[21], therefore, in addition to the competencies recommended in WP29 Guidelines, the following are also important:

[16] Para 1 of Article 38 of the GDPR
[17] Para 2.5 of the WP29 Guidelines
[18] Para 2.5 of the WP29 Guidelines
[19] Para 1(a) Article 39 of the GDPR
[20] Para 1(b) Article 39 of the GDPR
[21] Para 1(d) Article 39 of the GDPR

- Excellent communication skills;
- Organisation and management skills;
- Ability to read, interpret and apply the legislation, Codes of Conducts and recommendations relating to the protection of personal data;
- Excellent drafting skills;
- Attention to details;
- Systematic approach to resolution of issues.

Independence

Paragraph 3 of Article 38 states the controller and processor shall ensure that the DPO does not receive any instructions regarding the exercise of the tasks referred to in Article 39. Recital 97 reinforces this statement by adding that the DPO should be in a position to perform their duties and tasks in an independent manner. It is important however not to interpret this too widely. WP29 Guidelines make it clear that the autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39[22].

Conflict of interests

Some organisations may wish to combine functions of a DPO with another role. Paragraph 6 of Article 38 allows the DPO to fulfil other tasks and duties. It also stresses that the controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests. WP29 guidance adds that DPO cannot hold a position within the organization that leads him or her to determine the purposes and the means of the processing of personal data. Such conflicting positions may include chief executive, chief operating, chief financial, chief medical officer, head of marketing, head of Human Resources, Head of IT[23].
An in-house counsel position may also lead to conflict of interest as it would be difficult to separate the DPO's duties from other duties of the in-house counsel. An in-house counsel is acting on instructions of the employer on various matters that could affect personal data processing, e.g. drafting employment contracts, representing the Company in litigation against employees or customers). If a member of an in-house Legal Department is considered for a role of the DPO, it would be advisable to ensure that such employee's duties are carefully separated from any duties that may create a conflict of interest. It also must be made clear which duties are subject to instructions from the employer and which are not. It appears therefore that the DPO's functions would be better undertaken by financial controllers, compliance officers or internal auditors, i.e. roles that perform monitoring functions and enjoy a degree of independence.

Reporting

Paragraph 3 of Article 38 states that the DPO shall directly report to the highest management level of the controller or the processor. For most companies this would mean the board of directors or the Chief Executive Officer ('CEO'). However, depending on the organizational

[22] Para 3.3 of the WP29 Guidelines
[23] Para 3.5 of the WP29 Guidelines

structure of the controller or the processor the DPO may report e.g. to the Head of a Risk Committee, Head of Compliance or Head of Internal Audit, provided that they belong to the highest management level and themselves report to the board of directors or the CEO. It may be prudent to document this decision including the rational for such decision in order to demonstrate compliance with requirements relating to data protection officers under Article 38 of the GDPR.

Support

Paragraph 3 of Article 38 of the GDPR imposes an obligation on the controller and the processor to support the DPO by providing resources necessary to carry out the DPO's tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

WP29 Guidelines provides a non-exhaustive list of essential resources that should be provided to the DPO:

- active support of the DPO's function by senior management;
- sufficient time for DPOs to fulfil their tasks;
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate;
- official communication of the designation of the DPO to all staff;
- access to other services within the organisation such as Human Resources, Legal, IT, security etc.[24] so that DPOs can receive essential support, input or information from those other services;
- continuous training[25].

[24] Para 3.2 of the WP29 Guidelines
[25] Para 9, Annex to the WP29 Guidelines