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.