CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Bonn, Den Haag, Dublin, Madrid, Paris, Vienna, Warsaw

DG Justice – Working Party 29
Office N° MO-59 02/013
European Commission
B-1049 Brussels BELGIUM

Attn: Isabelle Falque-Pierrotin, Chairwoman

By email: JUST-ARTICLE29WP-SEC@ec.europa.eu presidenceg29@cnil.fr.

February 15, 2017

Dear Ms. Chairwoman,

CEDPO members have read with great interest the Guidelines on Data Protection Officers ("DPOs") adopted on 13 December 2016 by the Working Party 29 (WP 243).

We are very appreciative of the clarification efforts made and of the thoroughness of the guidance given. At the same time, we understand that this is a living document and that it will be updated over time, as while implementing the new rules, new questions will arise for controllers, processors and data protection officers.

With respect to the current text, we would like to offer the attached comments which we hope will be taken into consideration in the update process of the Guidelines.

We remain at your disposal and at the disposal of each national Data Protection Authority, to continue the dialogue on this important topic.

Sincerely Yours,

Fintan Swanton
ADPO

Pascale Gelly
AFCDP

Cecilia Alvarez
APEP

Charlotte Schönherr
Arge Daten

Steffen Weiss
GDD

Paul Korremans
NGFG

Maciej Byczkowski
SABI

dpo.ie the association of data protection officer www.dpo.ie
AFCDP www.afcdp.net
apep www.apep.es
ARGE DATEN www.argedaten.at
GDD www.gdd.de
NGFG www.ngfg.nl
Stowarzyszenie Administratorów Bezpieczeństwa Informacji www.sabi.org.pl

About CEDPO:

CEDPO was founded in September 2011 by European Data Protection Organisations, namely, AFCDP (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*) of France, APEP (*Asociación Profesional Española de Privacidad*) of Spain, GDD (*Gesellschaft für Datenschutz und Datensicherheit*) of Germany, and NGFG (*Nederlands Genootschaap van Functionarissen voor de Gegevensbescherming*) of The Netherlands. The Confederation was soon joined by ADPO (Association of Data Protection Officers) of Ireland, ARGE DATEN of Austria and SABI (*Stowarzyszenie Administratorów Bezpieczeństwa Informacji*) of Poland.

CEDPO aims to promote the role of the Data Protection Officer, to provide advice on balanced, practicable, and effective data protection and to contribute to a better harmonisation of data protection law and practices in the EU/EEA.

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

1. **Appointment criteria**

- "Core activities" must be construed in accordance with the description of the corporate purpose of the organization and the P&L revenues.
- "Large scale" should be understood according to a risk-based approach (rather than using criteria such as number of employees or the "volume" of personal data processed in a certain period of time alone).
- "Monitoring of behaviour" shall exclude the IT monitoring activities that any organization nowadays must carry out for the purposes of (i) (cyber)security; (ii) protecting the organization's systems and assets (including IP and confidential information as well as the personal data stored or otherwise processed by the organization); and (iii) complying with laws and regulatory guidance (e.g., data protection duties, anti-fraud and anti-money laundering related activities).

2. **Professional background**

- In view of the tasks that are entrusted to the DPO, different skills are required, including legal, technical, program and risk management and communication abilities. The DPO must ensure that his/her functions are actually carried out by himself/herself and/or his/her team comprised of professionals of different backgrounds, including but not limited to individuals holding a law or computer science degree. The organization appointing a DPO must provide the DPO with resources having these different backgrounds.
- The GDPR requires that '*The DPO shall be designated on the basis … of expert knowledge of data protection law …*". The DPO function should be open to any person, whatever their professional or curricular background is, and that this requirement can be met even by professionals who do not have a law degree. The text should not be interpreted narrowly; otherwise the risk is that data controllers and data processors will consider hiring mainly lawyers as DPOs.

3. **Internal/external DPO**

- The size and activities of each organization as well as its private/public status would determine whether an internal or external DPO is the appropriate decision from time to time.
- There are instances in which it could make sense to share the same external DPO, such as small organizations and organizations dealing with similar data processing activities.
- External DPOs may include legal entities even though the client organization may expect certain stability, to the extent compatible with local laws, regarding the actual individual(s) ultimately assuming the outsourced DPO tasks.
- The choice between an internal or external DPO shall not be influenced by the employment protection of internal DPOs.

4. Independence and conflict of interest

- Again, the size and activities of each organization should determine the most appropriate DPO structure. If in-house but part-time DPO, as well as if external DPO, is the chosen solution, specific safeguards would need to be in place to detect and advance alternative solutions if a conflict of interest arises.
- The DPO's independence shall not be construed to convert the DPO in a (i) "mini-DPA"; (ii) the CEO's organization; or (iii) the data subjects' representative. The DPO's independence shall be guaranteed with a DPO with integrity and loyalty. Likewise, his/her relationship with the organization must be vested with the appropriate "potestas" (which requires an appropriate position sponsored by the decision bodies of the organization, functional reporting line and resources). The DPO must be given a direct reporting line to the Board or to a Board Member - or equivalent body - of the organization with respect to his/her DPO responsibilities.
- The DPO's confidentiality duties vis-à-vis the organization that appointed him/her must be clarified in order to ensure that (i) the DPO's loyalty to his/her employer (if in-house) or to his/her client (if external) is not compromised; and (ii) his/her appropriate integration with the organization as a "trusted counsellor" is preserved.
- Risks of conflict of interest may be seen in positioning the DPO in the Security, IT, HR or other departments making decisions about processing activities.

5. Position

- Art. 38 (3) stipulates the DPO shall directly report to the highest management level of the controller or the processor. This demand strengthens the autonomy and significance of DPOs and requires the controller's or the processor's organization to link DPOs to the highest management level (such as to the Board or to a Board Member). For example, the organizational structure could ensure that:
  - The DPO has direct and unfiltered access to the top management and there is no intermediate level between the DPO and the top management. This helps to ensure that DPOs have no conflict of interests with regard to their function as DPO and therefore enjoy sufficient protection in performing their tasks.
  - The respective Board or Board Member is acting as functional and administrative supervisor of the DPO with responsibilities for all DPO's personnel and budget matters.
  - The DPO's reporting line to the top management can be clearly identified (for example in an organizational chart).

6. Location

- Specific physical location regarding Group DPOs or DPOs of a single organisation with several establishments seems to be irrelevant nowadays. His/her accessibility, an appropriate business involvement and a good local "network" (e.g., local privacy liaisons), would be the key elements to take into account to ensure effective protection.

- The DPO's accessibility is not necessarily dependent only on his/her own skills but rather on the combination of his/her skills and those of his/her local "network", e.g., local privacy liaisons to ensure appropriate local legal and language knowledge when required. The Working Party recommends that in order to ensure accessibility "*communication must take place in the language or languages used by the supervisory authorities and the data subjects concerned*". This recommendation may raise practical concerns if it is not further precised. The GDPR cannot expect that any Group DPO speaks all the 24 EU languages of each EU establishment of the Group. We therefore suggest to add, that it is not required that the DPO himself/herself speaks the languages of all countries where the controller/processor is established but that in practice this need can be met through translations of documents/media and resorting to local contacts assisting the DPO. The GDPR is another piece of how the EU internal market is built and should not impose any restriction to the freedom of movement of the DPO professionals and services within the EU. The language(s) requirement should not be a barrier to the construction of the EU.

7. Liability

- The DPO should not have an individual liability for a processing under the GDPR: The organization is the one liable for any non-compliance. The organization may decide to take actions, according to local law, against a negligent DPO as it would be the case regarding any other employee or contractor who may be held ultimately responsible for the damages that the organization has suffered (e.g., administrative fines, processing bans, etc.).

8. Tasks

- Record of processing activities. The DPO advises on the structure of the required record of processing activities as well as on the record maintenance rules. Then the DPO verifies from time to time the completeness and accuracy of the record (supervision duty) and gives guidance to the data controller, respectively to various departments to correct what is incorrect.
- The GDPR provides that the record must be filled in by the data controller or by its representative (Art. 30). The DPO may then be charged to maintain the record as a controller's representative. This is not a case of conflict of interest.
- DPIA: DPIAs are carried out by the data controller. The DPO advises the data controller as to the obligation or opportunity to carry out a DPIA. Then the DPO provides his/her opinion as to the relevance of the risk analysis made. Once risks have been mitigated, the DPO provides an opinion on mitigation measures to analyze the possibility to mitigate potential remaining risks.
- One of the tasks of the DPO which could be added as a recommendation and which is a good accountability practice is the drafting of an annual report provided to the highest level of management.

9. Training

- DPOs must be given the opportunity to stay up to date with regard to developments relating to data protection in the broadest sense of the term, including regulations updates, new technologies, international matters, audit techniques … The level of expertise of DPOs has to be constantly increased by participating in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc. The WP29 should make clear that this kind of continuous professional development by DPOs is actually an implicit mandatory requirement pursuant to Art. 37(5) and Art. 38(2). Also, to comply with the spirit of the Art. 5(2) requirement for accountability, DPOs should record evidence of their continuing professional development.

10. Publication of DPO's contact details

- Organizations should be able to provide generic contact details such as dpo@company.com. The organization must be able to decide the level of information to be provided in order to ensure smooth communication with external stakeholders (including but not limited to data subjects) and respect for the DPO's privacy: We may suggest the following wording:

  "Article 37(7) does not require that the published contact details should include the name of the DPO. It is for the controller and the DPO to decide whether this is necessary or helpful in the particular circumstances.