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

October 7, 2016

Dear Ms Chairwoman,

CEDPO and our associations representing Data Protection Officers and data protection delegates in several EU Member States would like to sincerely thank you for having given us the opportunity to share our views with representatives of Data Protection Authorities during the FabLab organized by the Working Party 29 on July 26, 2016.

As a follow up, we enclose an outline of matters prepared for discussion for this event and which we would like to bring to the attention of the Working Party 29, while it is preparing its guidance on the Data Protection Officer.

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 officers
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

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

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 position on the DPO in the GDPR

Follow-up of WP29 FabLab of July 26,2016

Appointment criteria

- "Core activities" must be construed in accordance with the description of the corporate purpose of the organisation 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 organisation nowadays must carry out for the purposes of (i) (cyber)security; (ii) protecting the organisation's systems and assets (including IP and confidential information as well as the personal data stored or otherwise processed by the organisation); and (iii) complying with laws and regulatory guidance (e.g., data protection duties, anti-fraud and anti-money laundering related activities).

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 organisation appointing a DPO must provide the DPO with resources including these different backgrounds.

Internal/external DPO

- The size and activities of each organisation as well as its private/public status are to be considered to determine whether an internal or external DPO is the appropriate decision from time to time. The choice between an internal or external DPO shall not be influenced by the employment protection of internal DPOs.
- External DPOs may include legal entities. Yet, appointing organisations should be offered some comfort, to the extent compatible with local laws, by having identified individual(s)performing DPO tasks.

Independence and conflict of interest

- Again, the size and scope of activities of each organisation should determine the most appropriate DPO structure. Regardless whether the choice is for an in-house, part-time DPO or an external DPO, specific safeguards would need to be in place to prevent, detect and mitigate any possible conflict of interest.
- The DPO's independence shall not be construed to convert the DPO in a (i) "mini-DPA"; (ii) the CEO's organisation; or (iii) the data subjects' representative. The DPO's independence shall be guaranteed with a DPO's integrity and loyalty. Likewise, his/her relationship with the organisation must be vested with the appropriate "potestas" (which requires an appropriate position sponsored by the decision-bodies of the organisation, 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 organisation with respect to his/her DPO responsibilities.
- The DPO needs clear confidentiality duties vis-à-vis the appointing organisation 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 organisation, as a "trusted counselor" is preserved.
- Risks of conflict of interest may appear, when the DPO is part of the Security, IT, HR or other department making decisions about data processing activities.

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 support (e.g., local privacy liaisons) would be the key elements to ensure effective protection.

Liability

- The DPO should not bear individual liability under GDPR. The appointing organisation is the one liable for any non compliance. The organisation 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 organisation has suffered (e.g., administrative fines, processing bans, etc.).

Tasks

- Record of processing activities. The DPO advises on the structure of the record of processing activities as well as on their maintenance rules. Then the DPO verifies, from

time to time, the completeness and accuracy of the record (supervision duty) and gives guidance to the relevant stakeholders, in this regard. The GDPR provides that the record must be maintained 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 shall not be considered as a conflict of interest.

- DPIA: DPIAs are carried out by the data controller. The DPO advises the data controller as to the need and methods of carrying out a DPIA. Then the DPO provides his/her opinion with respect to the relevance of the risk analysis, which resulted from the DPIA. Once the risks have been mitigated, the DPO provides an opinion on further mitigation measures to analyze the possibility to mitigate potential remaining risks.

Publication of DPO's contact details

- Organisations should be able to provide generic contact details of the DPO, such as dpo@company.com