Berlin, January 2017

Comments and Questions on the Guidelines on Data Protection Officers (WP243) of the article 29 working party

The German Professional Association of Data Protection Officers (BvD.e.V.) highly appreciates the effort to clarify the legislation on the role of the data protection officers (DPO) in the GDPR. We also see that the position is very close to what we published as the professional code of practice.[1] We currently especially see in Germany discussions about the position regarding the responsibilities trying to transfer the responsibilities of the controller to DPOs and to argue to hold data protection officers liable in an inappropriate way. Several statements within WP243 are therefore clarifying the role of DPO in companies and public bodies. In detail, we like to go through the guideline step by step and comment on various aspects with the hope, that it is useful to sharpen the guideline. Not in all commented aspects we think that we see instant options to improve the document.

With respect to the designation (section 2) we especially value the clarifications on various terms used in the GDPR. Within our Association, we already had discussions on the term “public authority or body”. In Germany this term now will be defined in the data protection act. With the clarification that performing public tasks leads to a requirement to designate a DPO it might also be argued for the private body being a public one. These discussions will not be very relevant in Germany but may raise questions in other countries.

The definition of “core activity” still seems confusing. The distinction of hospitals vs. medical practices as good examples is not easy to follow, whereas hospitals are required to designate and practices are not. The criterion of a core activity seems to also include an argument of scale - which is discussed as a different criterion in the WP243 as well. We also see the effort to also clarify this term, but from our perspective we still see a need of clarification.

The last paragraph of section 2.4 about DPOs designated on the basis of a service contract can be read as supporting a position that legal persons can be designated as DPO. We as the German Professional Association of DPOs would argue that the personal trust is essential for the position. The references of the GDPR to personal qualities and requirements lead to natural persons fulfilling these personal requirements. Our understanding is that natural persons need to be designated, even if a larger team supports the personally designated DPO. The DPO in person is the first contact and leading the team performing tasks of the data protection officer. We are unsure that the WP243 Guideline might be read differently and whether this is intended (section 2.4. last paragraphs).

[1] https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/bvd-allgemein/BEBI_EN_2016.pdf

Regarding expertise and skills we already published a position being part of the code of practice, which especially deals with the required professional skills. The WP243 Guideline expresses similar positions, like the coverage of the domains of legal, technical and organisational skills. The level of expertise is bound to the risks of the processing and domain of the controller. But we found the statements to be quite weak. We see great differences of the knowledge of data protection officers in Germany. Stronger statements to enforce regular trainings and statements about a level of absolutely required knowledge are needed from our point of view. “Authorities should promote training” - this does not fit with the requirement to designate a DPO, which is limited to cases which have a certain level of risk. Therefore we think it would be appropriate if the level of expertise needed would be stated more clearly and certified trainings as the foundation would be required.

Although the GDPR in general is oriented to certification, in the area of expertise this option is not mentioned. As well the GDPR states requirements to demonstrate the efforts, which might be appropriate with this regard as well. The value of the institution of DPOs is highly depending on the abilities of the DPO. Clear statements on professional backgrounds and levels of expertise are missing from our point of view.

Section 3.2 nicely gives hints on the necessary resources of DPOs. We have to accept that the statements cannot be made without the use of vague terms, although we would have a great interest in clear statements in most of the situations of conflict we see in practice.

An open question will be the role of DPOs in impact assessments (section 4.2). In practice this will create huge practical problems. The practical experience in Germany is that the expertise of assessing privacy impacts is limited to the DPOs. Every question about data protection is directed to the DPOs. That a company as controller or processor and its departments can create a DPIA, only with limited advice of a DPO, and which then finally might only be reviewed by DPOs, seems a bit unrealistic to be fulfilled in practice. The GDPR is clear with this respect but from our view we see various obstacles to bring this to life.

With respect to the ongoing discussions in Germany we see the clarification of great value that DPO are not responsible to ensure data protection (Introduction and section 4.1). But with some detailed arguments, we still see additional need for clarification. The descriptions of DPOs as facilitators of data protection, as intermediaries and the description of DPOs fostering a data protection culture fits with our view on DPOs in companies and public authorities. The current effort trying to hold DPOs responsible for data protection flaws is closely linked to the interpretation of the mandatory task of “monitoring”. Section 4.1 last paragraph of the WP 243 stresses that monitoring a specific processing does not lead to personal responsibility. We see a need for clarification that decisions about limiting the task of monitoring following what it also discussed as risk based approach is also not leading to personal responsibility. The GDPR never intended to require DPOs to monitor all processing activities in a full coverage. Nevertheless the WP 243 uses “may” describing the authority to monitor in the first place. Given this statements, one may still argue that a DPO has a duty to monitor, and if a problem of a certain level was not identified, a DPO is responsible and can be held liable. We see liability of DPO limited to cases where DPOs ignore known problems.

Finally the Professional Association of Data Protection Officials stresses that we see a great value in the WP243 Guideline on DPOs and the effort of the Article 29 Working party to support DPOs in the challenges we currently face every day and the ones we face with the implementation of the GDPR.

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
German Professional Association of Data Protection Officers

Budapester Straße 31
10787 Berlin

fon: +49 30 26367760
fax: +49 30 26367763
mail: bvd-vorstand@bvdnet.de
web: www.bvdnet.de

eingetragener Verein:
Amtsgericht Charlottenburg, VR 27190B
Chairman: Thomas Spaeing