

ARTICLE 29 DATA PROTECTION WORKING PARTY

Attn: Isabelle FALQUE-PIERROTIN –
Chairman of Art. 29 Working Party

PUBLIC CONSULTATION

Latina/Rome, JANUARY 31, 2017

Communicated to: JUST-ARTICLE29WP-SEC@ec.europa.eu and presidencg29@cnil.fr

Re: Our Remarks and suggestions on the Guidelines on Data Protection Officer (“DPOs”)

We welcome the recent publication of the Guidelines on Data Protection Officer (“DPOs”) adopted by the Article 29 Working Party on 13 December 2016, we consider this document very important for a consistent interpretation and for uniform application of the General Data Protection Regulation.

We briefly introduce our association, our European Privacy Centre (EPCE) gathers mainly privacy specialists (lawyers and engineers), EPCE is non-profit and independent from any particular interest concerning companies as well as political parties, aiming mainly at the promotion of scientific knowledge about the privacy and the protection of personal data, identity theft and any subject concerning its statute; the organisation and the management of training courses, seminars, meetings, lectures, high training courses, university masters also abroad, using either traditional instruments and technologies providing web conferences and seminars with high qualified speakers (for more details please see our website: <http://www.europeanprivacycentre.eu/en/>).

In respect of the public consultation of the Guidelines, we regard that some aspects of the Data Protection Officer could be better clarified and for this purpose we provide some remarks and suggestions in order to improve the following points.

Public Authority

First of all, it should be noted that in order to determine the exact meaning of “Bodies govern by public law”, these Guidelines indicate in the footnote no. 12 as a mere example the definition and criteria provided by the article 2 (1) of the Directive 2003/98/EC, our suggestion is to mention this Directive not only in the a footnote but in the body of the text of the Giudelines.

Although the notion of “public authority or body” is to be determined under national law of each Member States, for the sake of legal certainty and also of consistent interpretation at European level, it could be very useful to give more relevance in text to criteria enshrined in the abovementioned article 2 (1) of the Directive.

Large-Scale Criterion

In respect of par. 2.1.3 on the notion of large scale, we suggest to mention more situations that fall under exclusion cases of large-scale processings. In particular, it should be considered very useful to provide indications weather or not little organisations of physicians or lawyers are also to be considered excluded by the notion of large-scale processing. In both cases, the nature of the data can be considered the same at individual and group level, in small organizations of few individuals (lawyers or physicians) also risks are very similar to situations relating to data processings of individual physicians and lawyers.

Conflicts of Interest

Lastly, with regard to the par. 3.5 on the conflict of interests and more in particular to conflicting positions indicated in the footnote no. 34, on one hand, we suggest to give more relevance to this notion in the text of the Giudelines and not only in footnote, on the other hand, according to our opinion the conflicting positions should be analysed always with regard to core activities of the data controller or the data processor as a suggested general criterion in the rule of thumb. This is because for instance the role of head of human Resources or the head of the IT Departments could be considered not always as conflicting positions with a Data Protection Officer role, as mentioned above a very useful criterion could be to take into account the nature of the core business of a data controller or a data processor in comparison with these relevant roles.

DPO of the processor

Being the processor “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”, in respect of par. 2.2, we consider still not clear the application of the article 37 to controllers and processors. The two examples described in this paragraph shows according to our viewpoint that the data processor, when it processes data on large scale is to be regarded as a data controller and not only as a data processor, because this situation is beyond the data processing relating to the small enterprise or data processing relating to the manufacturer.

As a matter of fact, the conclusion of the first example is that the processor is carrying out its own activity with its own customers, this should bring to the situation of a DPO designation by a data controller.

In the light of the above considerations, we suggest to clarify through more examples when a DPO can be designated by the data processor.

Continuous Training of the DPO

In respect of the continuous training indicated in the par. 3.2 relating to *necessary resources*, we suggest to provide indications on how national DPAs, universities, research centres and associations of privacy experts should be involved.

Road Map for Data Protection Authorities and National legislators

Within the margin of manoeuvre left by the General Data Protection Regulation, we suggest to provide a road map to both national legislators and DPAs for the adoption of acts necessary to give more legal certainties and to allow a consistent application of GDPR.

In respect of the remarks here mentioned EPCE President wishes to acknowledge the valuable contributions of two of our privacy professionals, Mauro Alovio, Emiliano Vitelli and Stefano Gorla.

Best regards,

Fabio Di Resta

President of European Privacy Centre (EPCE)

