CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

FIRST POSITION PAPER

of the Confederation of European Data Protection Organisations

(CEDPO)

on the European Commission Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

General Data Protection Regulation

COM(2012) 11 final

30th March 2012

AFCDP GDD APEP NGFG

France ***Germany*** ***Spain*** ***Netherlands***

I. INTRODUCTION

The Confederation of European Data Protection Organisations (CEDPO) was founded in 2011. Founding members of CEDPO are:

AFCDP *Association Française des Correspondants à la Protection des Données à Caractère Personnel (http://www.afcdp.net)*

APEP *Asociación Profesional Española de Privacidad (http://www.apep.es)*

GDD *Gesellschaft für Datenschutz und Datensicherheit (http://www.gdd.de)*

NGFG *Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (http://www.ngfg.nl)*

Together the above organisations represent the interests of private and public sector organisations, data protection officers (DPOs) and other data protection professionals from the four European Member States.

The main purpose of CEDPO is to promote the important role of the data protection officer (DPO) and balanced, practicable, and effective data protection in general. In addition, CEDPO aims to contribute to better harmonisation of data protection law and data protection practices in the European Union / European Economic Area. Based on the experiences gathered and shared by the national data protection organisations, the confederation plans to initiate and maintain constructive communications with competent European institutions. Harmonisation of data protection practices will also be achieved thanks to the interaction between the members of the different national associations.

CEDPO has published a comparative spreadsheet of the laws applicable to DPOs in 14 different countries which is a useful document to consider the future of the DPO. This document is available on the CEDPO website at www.cedpo.eu.

CEDPO would like to take the opportunity to comment on the Commission's proposal in general, and on the role and position of the DPO in particular as it does through this first position paper. CEDPO will further elaborate on additional aspects of the proposal in due course.

II. GENERAL COMMENTS ON THE COMMISSION PROPOSAL

CEDPO welcomes the Commission's initiative to harmonise and modernise the legal framework of data protection in the EU. CEDPO considers that it is essential to reduce administrative burdens bearing upon data controllers and processors. ***However, we feel that the Commission's proposal does not exploit the full potential of administrative simplification (see below IV).***

CEDPO shares the Commission's view according to which administrative simplification should not lead to an overall reduction of the data controllers' and data processors' responsibility in ensuring effective data protection. ***In this regard, the envisaged strengthening and harmonisation of the role***

and position of the data protection officer (DPO) meets the expectations of CEDPO as this is an important measure in order to intensify internal compliance.

Since a ***harmonised approach*** is essential in order to provide for a data protection regulation that is both, effective and economically reasonable, this approach should be ***consistent*** and must not be undermined. The envisaged regulation should provide for legal certainty. This includes a uniform application of the new data protection law in the Member States. In this regard CEDPO is concerned about Article 34 paragraph 2 point (b), which would allow the national DPAs to determine certain processing operations which are subject to prior consultation. Even though the national DPAs are supposed to communicate their findings to the European Data Protection Board according to Article 34 paragraph 4, this may lead to **different approaches in the Member States once again**. This would be detrimental to the Commission's goals, especially with regard to controllers / processors that are established in several Member States.

The proposal contains quite a few passages that would empower the Commission to adopt ***delegated acts*** in accordance with Article 87 for the purpose of further specifying certain data protection requirements (e.g. Art. 35 paragraph 11 concerning the designation and qualification of DPOs). The exercise of delegation includes certain rights of the European Parliament and the Council. According to the Commission Communication COM(2012) 9 final the Commission will also maintain close and transparent dialogue with all interested parties involving representatives from the private and public sector, throughout the adoption process and beyond, especially in the context of the implementation of the new legal instruments. CEDPO would be pleased to provide input to the Commission, for example, in further specifying the criteria and requirements for the core activities of the controller or the processor referred to in Article 35 paragraph 1 point (c) and the criteria for the professional qualities of the DPO referred to in Article 35 paragraph 5.

III. THE ROLE AND POSITION OF THE DATA PROTECTION OFFICER (DPO)

1. Current situation

Both, the European Commission (COM(2003) 265 final – Report, p. 18 and 24) and the Article 29 Working Party (WP 106, p.22 and 23) have already recommended the appointment of DPOs. In addition, the important and growing role of DPOs has been recognised globally in the "Madrid Resolution" on international privacy standards approved by data protection authorities from over 50 countries at the 31st International Conference of Data protection Commissioners in 2009. One of the most relevant chapters of the document is the one that refers to proactive measures. It includes the recommendation to appoint data protection or privacy officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately. Germany has made good experiences with the DPO in the past 30 years and DPOs are becoming increasingly accepted by Member States such as France and the Netherlands. In Spain, where the DPO role is not mandatory except for security measures regarding specific processing, it has become evident – at least for large companies – that this role is indispensable. In complex structures, the role of the DPO is developing from a mere compliance function to a more and more strategic position. For the Netherlands, where appointing DPOs is not mandatory, the NGFG has developed a checklist to help organisations decide whether or not to appoint a DPO[1] .

[1] NGFG. (2008, April). Am I the Lucky One. Den Haag, the Netherlands.

2. Designation of the DPO (Article 35)

a) Introducing incentives

Generally, the recognition of the DPO in Article 35 – 37 of the proposal is very welcome by CEDPO.

Nevertheless, the regulation should provide for ***incentives*** in favor of the appointment of DPOs by controllers and processors. It would make the measure better accepted in cases where the appointment is mandatory and in other cases it would encourage the appointment of DPOs.

Appointing DPOs has major advantages for data subjects, controllers / processors and DPAs. This is basically reflected by section 4 of Chapter IV of the proposal. An independent study commissioned by the Dutch Ministry of Justice found that organisations that have appointed a DPO have a higher degree of compliance awareness and knowledge[2]. CEDPO thinks that the recitals of the regulation should emphasize the advantages of appointing a DPO and stress its central role for compliance, especially in the light of the new duties of data controllers / processors aiming at more effective data protection, such as the necessity of data protection impact assessments, breach notification, privacy by default, and the training of staff. When promoting effective data protection as a competitive advantage, the Commission should mention the DPO. It should be emphasized that in many cases DPOs are good for business. Installing a competent and qualified privacy guardian is not only a first tangible sign of making effective the accountability principle, but also a positive image factor which helps creating trust.

CEDPO agrees with the Commission on the necessity of avoiding undue administrative burdens, particularly on small and micro-enterprises. Nevertheless, this must not lead to the conclusion that smaller organisations could not ***benefit from appointing DPOs***. For example, smaller start-up companies active in the information and communication sector may very well benefit from data protection officers as a competitive advantage. Looking at the remedies, liability and sanctions as described in Chapter VIII of the proposal, appointing a DPO may be a very useful proactive measure which can in fact not only save the controllers /processors money in the end but also provide more control on risks that may cause reputational damages. DPOs can contribute to make the personal information a valuable asset and not a source of concerns. For these reasons, the Commission should emphasize that also companies not having a legal obligation to appoint a DPO may considerably reduce the above risks and improve their business by making use of an optional appointment.

The regulation should provide for incentives for those controllers /processors who appoint a DPO and encourage Member States to create advantages (on tax or other charges) for those companies who appoint a DPO when this is only an option.

CEDPO recommends the following incentives:

[2] Brouwer-Korf, A. (2009). Rapport 'Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer'. Den Haag, the Netherlands.

Pro Facto (2008) H.B. Winter et. al *Wat niet weet, wat niet deert: Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*

Conclusion reached by the Second Chamber based on the research, “Evaluation of the Data Protection Act” (Tweede Kamer, vergaderjaar 2009-2010, 31 051, nr. 5, blz. 29.)

- When a processing is on a list of processing subject to prior consultation of the DPA, the controller/processor should be subject to mere notification or no formalities at all when a DPO has been appointed. Indeed even among the most sensitive processing operations, some are routine (e.g. some uses of biometrics) and should not be subject to prior consultation when a DPO has been appointed, as the DPO will supervise their implementation and verify that they meet the data protection requirements.
- Making the DPO the cornerstone of data protection claims. This would reduce claims based on misunderstandings and the number of claims going to the DPAs. When a data subject has a claim, he/she should first attempt to get it solved at the DPO level before bringing it to courts or DPAs. This would require to set a procedure and a response time frame.
- The proposed regulation requires all security breaches to be notified to the DPA. Inevitably, the vast majority of the notified breaches will relate to minor incidents, unnecessarily overwhelming controllers/processors as well as DPAs. CEDPO assumes that certain criteria will be set in the future by the Commission, to differentiate minor breaches, not requiring the DPA's attention, from breaches, worthy of attention. In such cases, organisations with a DPO should be allowed to have him/her advise on the application of these criteria.

b) Appropriate threshold

Looking at the threshold number of 250 employees in Article 35 paragraph 1 point (b) CEDPO pleads for an opening clause allowing Member States to maintain / establish a lower threshold. It seems counterproductive to raise the threshold for appointment of a DPO so high in a country such as Germany where their use has been a success.

The number of persons employed for the purpose of processing personal data is only one of several factors that may be taken into account. After all, the risks to the rights and freedoms of the data subjects depend on the circumstances of the individual case. In its handbook *Are You The Lucky One,* the NGFG suggests 16 aspects to be taken into account, varying from data usage to types of data, to determine if an appointment of a DPO is recommendable[3]. CEDPO believes that the thresholds to be considered should take into consideration the risks presented by the processing.

Article 35 paragraph 1 point (c) takes into consideration the risk factor presented by a processing operation: the controller and the processor shall designate a data protection officer in any case where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects. This wording is inconsistent with recital 75 and item 3.4.4.4. of the Explanatory Memorandum. Correctly, recital 75 refers to the monitoring of ***processing operations***, whereas Article 35 merely refers to the monitoring of ***data subjects***. This makes quite a difference with regard to the obligation of appointing a DPO. It should be clarified that Article 35 applies to risky processing operations. The national translations should be checked accordingly. CEDPO suggests the text to be adjusted as follows in addressing this issue:

The controller or processor shall designate a data protection officer in any case where:

…

(c) the processing of personal data, particularly by virtue of their nature, their scope and / or their purposes, is of high risk to the protection of personal data or the privacy of the data subject.

[3] See footnote 1; the 16 aspects are available at http://www.ngfg.nl/producten_brochures.html

With regard to a possible obligation to appoint a DPO, CEDPO suggests to take into account the following criteria based on the risks presented by the activity.

- **Purpose of processing operations**

A higher risk potential could be attributed to companies which commercially carry out automated processing of personal data for the purpose of transferring them to other parties which require the data subjects' consent as a legitimate ground (e.g. companies trading mailing lists). The same applies to organisations processing personal data for market or opinion research purposes or for any processing that requires a data protection impact assessment.

Generally, the profiling of individuals – e.g. by credit agencies – involves specific risks for the rights and freedoms of the data subjects.

- **Sensitivity of data/data processing**

Naturally, the sensitivity of the data being processed has to be taken into account, e.g. according to the German Federal Data Protection Act (BDSG), the obligation to appoint a DPO applies in all cases where prior checking (in the Regulation, it would refer to "consultation") is required. That may include the processing of sensitive data according to Article 8 (1) of EU Directive (95/46/EC) unless this processing is required to comply with national law or merely incidental. In any event, CEDPO believes that evaluating the usefulness of appointing a DPO should be part of the individual data protection impact assessment of the controller.

- ***Amount of personal data being processed***

Companies processing large amounts of personal data are more likely to put the rights and freedoms of the data subjects at risk than companies only dealing with a minimum of personal data. Generally, companies where the processing of personal data is a major part of the overall business purpose (e.g. internet or telecommunication service providers) have a higher risk potential, because of the large amounts of personal data being processed.

The same applies to companies processing personal data on behalf of their clients. CEDPO agrees with the Commission that internal control mechanisms are especially important "in those increasingly common cases where data controllers delegate data processing to other entities (e.g. processors)." Even if the controller remains responsible in such cases, it is essential to have a knowledgeable contact person within the processor.

c) Qualifications of the DPO

Only DPOs who are adequately qualified can do their important job properly.

A study of the German Association for Data Protection and Data Security (GDD) revealed the following criteria:

- sound knowledge of data protection law
- sound knowledge of IT standards
- the ability to establish a proper data protection management, based on an adequate knowledge of business related economics and a specific knowledge of the company`s inner structures and processing operations

The results of the study have recently been confirmed by German DPAs[4] . Based on more than 30 years of experience, the GDD has developed an educational program for data protection professionals, including a certification program for DPOs (GDDcert). APEP also offers in Spain a specific certification programme, which is particularly needed in view of the absence of a specific official DPO degree in the current Bologna Plan.

With reference to Article 35 paragraph 5 1st sentence CEDPO recommends the following wording replacing the adjective "expert" by "adequate" in order to open the DPO position broadly enough, beyond the legal professions:

*"The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, **adequate** knowledge and practice of data protection law and practices and ability to fulfill the tasks referred to in Article 37."*

In order to ensure the necessary qualification of the DPO, the regulation should explicitly mention the duty of the controller/processor to allow and pay for an adequate education (including continuing education) of the DPO. The Commission shall be empowered to adopt in accordance with Article 87 the criteria for the professional qualities of the DPO.

The CEDPO member organisations are experienced with the education of DPOs in their relevant countries. CEDPO would therefore welcome the opportunity to assist the Commission in determining such criteria.

d) Designation of DPO

Both, ***internal*** and ***external*** DPOs can perform their job properly, as long as they are adequately qualified, familiar with the internal structures and processing operations of the controller / processor, and sufficiently available for the controller/processor.

CEDPO welcomes the proposal allowing for a single DPO being in charge of a ***group*** of undertakings. The function as group DPO may actually improve the effectiveness and harmonisation of data protection practices in the entire business group. In such cases the DPO naturally needs local assistance. In this context the regulation should **confirm the application of Article 36 paragraph 3** according to which the controller / processor shall provide the necessary resources, including staff. Depending on the individual structure of the business group assistance can be provided by local assistants, a data protection committee or team. The issue of appointment of a single DPO for a group of undertakings raises several questions in particular with regard to the proximity with data handlers/subjects in language, culture and knowledge of DPA`s decisions (e.g. prior consultation, security breach). CEDPO will consider the practical implementation aspects and may provide further comments on the matter.

e) End of designation

CEDPO thinks that the creation of a minimum period of designation in Article 35 paragraph 7 ***may put the DPO's independence at risk.***

If the DPOs would depend on the controllers´ / processors´ good will when the two year term has ended, this could clearly interfere with their independence. They might be tempted to take instructions from the controller / processor, although they are not supposed to do so according to Article 36 paragraph 2.

[4] Düsseldorfer Kreis, Beschluss vom 24./ 25. November 2010

Therefore, CEDPO thinks that the Regulation should not address the issue of the term of the DPO's appointment. Still, particularly internal DPOs must be provided with protection from unfair dismissal to ensure their independence. The controller/processor must provide the DPA with the name and contact details of a DPO[5]. The Regulation could also provide that, in case of termination of the mission at the initiative of the data controller/processor, the controller/processor must inform the DPA. DPOs may request the DPAs to ask the controller/processor to inform them of the reasons for dismissal. In case the DPO has another function, this request may only be made when the grounds for termination are based on the fact that the person no longer fulfils the conditions required for the performance of his/her duties as DPO[6]. Fines should be due in case the controller / processor fails to inform the DPA.

3. Tasks of the DPO

CEDPO welcomes the description of the DPO`s tasks in Article 37, but thinks that it would be important to add a general statement either before the list of tasks or at the beginning of section 4 to specify the general role of the data protection officer: monitoring in order to advice the organisation on compliance with data protection rules. This statement should also specify that the appointment of a data protection officer does not discharge the controller / processor from its obligations as ultimate compliance bears upon them.

This would provide more legal certainty and a better harmonisation of the DPO´s activities in the member states.

The wording used in the proposal (inform, advise, monitor, ensure, act as contact point for DPA) characterizes the advisory and supervisory functions of the DPO. It implies that the DPO is not the decision maker. It is the controller /processor who remains responsible / accountable and who will be held liable in the first place. In this context the verb ´ensure` in Article 37 paragraph 1 point (d) could be replaced by the verb ´monitor` or ´supervise`. After all, Article 29 attributes the duty of maintaining the documentation to the controller / processor. The controller / processor is responsible for the implementation, not the person who monitors the implementation.

In addition, the proactive management role of DPOs may not be sufficiently reflected. In practice, DPOs are not merely in charge of keeping the controller / processor up to date and to internally monitor compliance with data protection law. They are also (co-)shaping internal data protection policies (e.g. according to Article 22 paragraph 1), they become involved in drawing up and establishing Binding Corporate Rules (BCRs), and they are asked to review data protection contracts. Also the strategic role of the DPO should explicitly be mentioned in the regulation, as it considerably contributes to the value of the DPO to the benefit of all parties involved, especially the data subjects and the controllers / processors themselves. Therefore, CEDPO recommends adding a new point (a) to Article 37 which could have the following wording:

´to advise the data controller or the processor with regard to the overall data protection strategy;`

4. Position of the DPO

a) Timely involvement and access to resources

CEDPO explicitly welcomes the duty of the controller / processor to ensure a proper and timely involvement of the DPO according to Article 36 paragraph 1.

[5] Article 35 paragraph 1
[6] Article 35 paragraph 7

This enables the DPO to effectively play a proactive role to the benefit of all parties involved (see above 3.). According to Article 79 paragraph 6 point (j) the supervisory authority shall impose a fine between 1,000 EUR and 1,000,000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37.

In order to provide for legal certainty, it should be clarified that administrative sanctions may also be imposed, if the DPO is not properly or timely informed about data protection issues of the controller / processor.

In addition, the DPO must be solicited in the framework of the assessment of whether the controller / processor has fulfilled its obligation, as referred to in the first paragraph of article 36. The regulation should provide more precisely for a right of the DPO to timely obtain access to information, data processing and people as needed to perform his/her mission.

b) Direct reporting line

CEDPO also welcomes the direct reporting line according to Article 36 paragraph 2, but for clarification purposes recommends to ***replace the wording ´report to the management` by ´report to the highest representative of the controller or processor`.*** In the case of private bodies that could be at least one designated member of the directory board or the executive director.

The DPO should be given appropriate status and visibility within the organization of the controller/processor in order to have its role recognized by data handlers.

c) Independent Status

aa) Eligibility for educational support

CEDPO welcomes the obligation of the controller / processor to support the DPO according to Article 36 paragraph 3. With regard to the DPOs qualification the controller should have the obligation to allow for an adequate education, including continuing education. As technology and legal requirements and organisations evolve, this maintaining up-to-date knowledge is essential in effective protection of personal data. CEDPO recommends the following wording, accordingly:

´The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment, ***continuous education*** *and any other resources necessary to carry out the duties and tasks as referred to in Article 37.`*

bb) Confidentiality

A confidentiality clause is important for both data subjects as well as data controllers/processors. For instance, when the DPO carries out an investigation into sensitive areas, such as concrete security arrangements and or on sensitive data, such information must be kept under utmost confidentiality. The Data protection Act in the Netherlands, for instance, provides protection in such instances through a specific confidentiality provision.[7]

[7] Wet bescherming persoonsgegevens Article 63 point 4.

5. Right to contact the DPO

Data subjects are guaranteed the right to data deletion, access and correction, and the right to be informed about data breaches. CEDPO regards a "right" given to data subjects to contact DPOs, referred to Article 35, paragraph 10, as problematic.

First of all the term "right" is not appropriate. The possibility to contact DPOs cannot be made a "right" at the same level as the rights mentioned above, it is a possibility offered to the data subject. There are situations where DPOs are practically unable to fulfil the duty of providing the unconditional right to be contacted. Where the controller/processor failed to provide appropriate resources in dealing with numerous contacts from the data subjects, such as after a security breach, DPOs are deem to be out of compliance.

Secondly, DPOs have advisory and monitoring tasks, not implementing tasks, as referred to article 37 which belong to the data controller. In instances where answers on behalf of the organisation must be given, DPOs are not in the position to be the point of contact and represent the data controller/processor. Most data protection requests today are adequately handled by assisting departments, such as consumer relations departments or the HR department, so that DPOs can focus their attention on issues that make greater difference in terms of compliance with the protection of personal data within the organisation. For example, in the Netherlands, where 'privacy officers' are appointed alongside the DPO, these officers play an important supporting role of the DPO.[8] Data subjects certainly reserve the possibility to contact the DPOs, for instance in cases of data protection claims that cannot be dealt with by the delegated persons. However, direct contact with individuals must not be disproportionate, to the extent that the DPOs cannot reasonably carry out their other important tasks.

Thirdly, Article 35, paragraph 10 seems redundant and out of place. Looking at Article 37 point (c), DPOs are expected to have direct contact with the data subjects. Furthermore, Article 35 sets the rules for the designation of a DPO, and is not about the rights of data subjects.

CEDPO would recommend Article 35 point 10 to be deleted from the proposed regulation.

IV. FURTHER REDUCTION OF UNNECESSARY ADMINISTRATIVE BURDEN

The reduction of unnecessary administrative burdens and the enhancement of the data controllers` / processors` responsibility and accountability belong to the most important goals of the Commission. This approach is welcome by CEDPO. Nevertheless, from a CEDPO point of view, it is questionable whether the Commission proposal does exploit the full potential in order to achieve these goals. Overlapping responsibilities should be avoided.

Where DPOs are appointed, monitoring of the implementation and application of the regulation within the organisation, are in place. Despite this, DPAs would still have to be consulted in advance in each and every case where they believe that specific risks are likely to be attached to certain

[8] According to the Explanatory Memorandum to the Police Data Act, House of Representatives, 2005-2006, 30 327, No. 3, p 92, The Netherlands: privacy officers, for instance support the (police) organisation with its controlling and monitoring of the processing of the data, as well as respecting data subjects' access and correction of data – practically carrying out some of the tasks of the DPO.

processing operations (Article 34 paragraph 2 point (b). Depending on the result of the data protection impact assessment, the DPAs would also have to be consulted in other cases (Article 34 paragraph 2 point (a). Irrespective of the question whether or not the DPAs would have sufficient resources to adequately respond to the controllers / processors, this kind of procedure is not entirely in line with the above goals of the Commission.

Therefore, it may be worthwhile to explore the option to replace formal consultation of the DPA by an obligation to merely inform the DPA about processing operations involving specific risks, when a DPO has been appointed.

This way, controllers would be able to execute processing operations without undue delay and unnecessary administrative burdens. The DPAs remain in a strong supervisory position, because they generally have the right to monitor the application of the regulation based on the documentation prescribed by Article 28. An obligation to formally consult the DPA should only apply in cases of doubt.

In Closing

Should there be specific points raised in this paper which require further discussion, please do not hesitate to contact CEDPO.

CEDPO would be delighted to share its experience and know how in the future. Together we strive towards a common goal: balanced and effective protection of personal data.

Bonn,

Den Haag,

Madrid,

Paris,

30th March 2012