October 19th, 2012

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
Recital 75 (on DPO)	Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitorinternal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently.	The presence of a qualified person by the side of the controller or the processor is highly beneficial to ensure awareness and compliance with this Regulation. Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a data protection officer should assist the controller or processor to monitor internal compliance with this Regulation. In other instances, Member States should provide for incentives in order to promote the appointment of data protection officers by controllers and processors. Data protection officers, whether or not an employee of the controller or processor, should be in a position to perform their duties and tasks effectively and independently. For this purpose, they should have access to any information and any person necessary to the performance of their mission, including	The recital must reflect the central role played by DPOs in the compliance with the obligations of the Regulation. In particular, it is important to list the processes where DPOs must be involved to make sure that controllers and processors associate DPOs to these processes. It is also necessary to stress that DPOs should not be designated only by organisations in instances where their appointment is mandatory but to open the possibility for organisations to appoint DPOs where they see advantages for their activity.

AFCDP — **France**

APEP — **Spain**

GDD — **Germany**

NGFG — **The Netherlands**

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
		in the following cases: handling of data subjects' requests (Articles 12, 15 and 19; e.g. design of process, assessment of requests); involvement in defining mechanisms to ensure the verification of compliance measures (Article 22.3; in order to carry out their mission effectively, data protection officers shall be given a central role in the performance of compliance audits); verification of guarantees provided by contractors and subcontractors (Article 26.1); assessment of appropriate security level (Articles 30.1 and 30.2); privacy impact assessment (Article 33.1); maintenance of the documentation (Article 28). The entry into force of this Regulation should not terminate the appointment of data protection officials appointed under the national law provisions implementing Article 18.2 of Directive 95/46/EC, as long as they fulfill the requirements set forth in the Regulation.	Several countries in the EU under national laws implementing the EC Directive 95/46 know the function of data protection official. The change from a Directive into a Regulation should not be a justification for controllers to terminate the appointment of existing data protection officials. As a consequence, if the appointed data protection officials meet the qualification requirements of the Regulation, they should be maintained in their functions, that is

AFCDP — **France**

APEP — **Spain**

GDD — **Germany**

NGFG — **The Netherlands**

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
			automatically become data protection officers.
Article 31 para. 1 *Notification of a personal data breach to the supervisory authority*	In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.	***Para. 1 unchanged but insertion of new para. 2 and 3:*** 2. The data protection officer shall be immediately informed of the suspected breach, and be involved in any assessment of the breach by the data controller and in the notification process to the supervisory authority, in accordance with Article 36 2. 3. As an exception to Article 31 1. above, where a data protection officer is appointed, the controller shall be exempted from notifying the supervisory authority, in case of minor breaches.	In addition to the list of tasks in Article 37, the role of the DPO regarding breach notification should be explicitly included in the Regulation. 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 and to be exempted from notification of minor breaches. This would be an acknowledgement of the added value of appointing a DPO. The DPAs would remain in a strong supervisory position as they can issue guidance and investigate the application of the criteria.
Article 34 para. 2 *Prior authorisation and prior consultation*	The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in	The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in	Where DPOs are appointed, monitoring of the implementation and application of the regulation within the organisation, are in place. 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

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
	particular to mitigate the risks involved for the data subjects where: (a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or (b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.	particular to mitigate the risks involved for the data subjects where: a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks. In case the controller or processor acting on the controller's behalf has designated a data protection officer, the controller or processor acting on the controller's behalf shall merely inform the supervisory authority of the above mentioned processing. ***Deletion of letter (b)***	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. After all, 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. 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. Letter (b) may be detrimental to harmonisation.
Article 35 *Designation of the data protection officer*	1. The controller and the processor shall designate a data protection officer in any case	***Insertion of new para. 1:*** 1. The data protection officer monitors the processing of personal data by the controller and the processor in order to advise the controller and the processor on compliance with this Regulation; he or she thereby assists in ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. The designa-	CEDPO recommends to add a general provision to specify the general role of the data protection officer: monitoring in order to advise the organisation on compliance with data protection rules. This provision 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.

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

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
	where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise employing 250 persons or more; or (c) 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. 2. (...) 3. (...) 4. (...) 5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. (...) 6. (...)	tion of a data protection officer does not discharge the controller and the processor from their obligations under this Regulation. ***Para. 1 letter (a) and (b) unchanged, but new wording letter (c):*** (c) the processing of personal data, particularly by its virtue of nature, its scope and/or its purposes, is of high risk to the protection of personal data or the privacy of data subjects. 5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, adequate knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. (...)	The wording of letter (c) 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. CEDPO recommends to replace the adjective “expert” by “adequate” in order to open the DPO position broadly enough, beyond the legal professions.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
	7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.	7.The controller and processor must inform the supervisory authority of the termination of the designation of the data protection officer. Data protection officers may only be dismissed, if they no longer fulfil the conditions required for the performance of their duties as data protection officers. Where the termination of the relationship between the controller or processor and the data protection officer relates to his or her tasks as data protection officer, the data protection officer may request the supervisory authority to investigate the grounds of termination.	The creation of a minimum period of designation 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. Particularly internal DPOs must be provided with protection from unfair dismissal to ensure their independence. The controller/processor must inform the DPA in case of termination. In case of termination at the initiative of the controller/processor, the DPO should be able to require the DPA to investigate the grounds for termination. 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.
	8. (...) 9. (...)		
	10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the	***Deletion of para. 10:***	The term "right" is not appropriate. The possibility to contact DPOs cannot be made a "right" at the same level as the data subject rights.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
	data subject's data and to request exercising the rights under this Regulation. 11. (...)		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. 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. 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.
Article 36 *Position of the data protection officer*	1. (...) 2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the	2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the	CEDPO 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 controller or processor at the highest representative level`. In the case of

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
	function. The data protection officer shall directly report to the management of the controller or the processor.	function. The data protection officer shall directly report to the controller or the processor at the highest representative level.	private bodies that could be at least one designated member of the directory board or the executive director. In public bodies, e.g. a governmental ministry, this may be the minister him/herself. The DPO should be given appropriate status and visibility within the organisation of the controller/processor in order to have its role recognized by data handlers.
		Insertion of new para. 3:	
		The data protection officer must ensure confidentiality of information obtained while performing his or her tasks, in particular as regards to information relating to complaints and information relating to the data processing activities of the controller or processor.	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.
	3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.	The controller or the processor shall support the data protection officer in performing the tasks and shall provide and bear the costs of staff, premises, equipment, continuous training and any other resources necessary to carry out the duties and tasks referred to in Article 37. These means shall be adapted to the size and needs of the organisation of the controller or processor; in particular	Especially with regard to the necessary qualification of the DPO, the regulation should explicitly mention the duty of the controller/processor to allow and pay for adequate training.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
		where a single data protection officer is appointed for a group of undertakings according to Article 35 paragraph 1.	
Article 37 *Tasks of the data protection officer*	1. The controller or the processor shall entrust the data protection officer at least with the following tasks: (a) - (c) (...)	***Insertion of new letter (a):*** to advise the data controller or the processor with regard to the overall data protection strategy;	The proactive management role of DPOs is not 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.
	(d) to ensure that the documentation referred to in Article 28 is maintained;	(d) to monitor that the documentation referred to in Article 28 is maintained;	The verb ´ensure` could be replaced by the verb ´monitor`. After all, Article 29 attributes the duty of maintaining the documentation to the controller / processor.
	(e) – (h) (...)	***Insertion of new letter (g):*** to act as the mediator for claims from data subjects before any claims are brought before the supervisory authority or the competent jurisdiction;	Making the DPO the cornerstone of data protection claims would reduce claims based on misunder-standings 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.

AFCDP — **France**

APEP — **Spain**

GDD — **Germany**

NGFG — **The Netherlands**

October 19th, 2012

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Article	Text Draft Regulation	Suggested Changes	Reasoning
Article 64 para. 2 *European Data Protection Board*	The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.	The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State, the European Data Protection Supervisor and at least one representative of a non-governmental European data protection organisation supporting data protection officers.	The involvement of DPO representatives / data protection practitioners should be secured. Indeed the EC Directive 95/46 and now the Regulation have given birth to both supervisory authorities and DPOs who are respectively experts in the protection of personal data. The European Data Protection Board should benefit from the experience of DPOs in the implementation of the rules deriving from the Regulation.
Article 73 para. 1 *Right to lodge a complaint with a supervisory authority*	Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.	Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. Where the controller or the processor, subject of complaint, has designated a data protection officer, the supervisory authority should first instruct the complaining party to lodge the complaint to the data protection officer.	See reasoning for insertion of new letter (g) above.

AFCDP
France

apep
Spain

GDD
Germany

NGFG
The Netherlands

October 19th, 2012

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

About CEDPO:

The Confederation of European Data Protection Organisations (CEDPO) was founded in 2011 and represents the interests of privateand 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 a better harmonisation of data protection law and data protection practices in the European Union / European Economic Area.

Based on the experience gathered and shared by the national data protection organisations (see below), the confederation has begun 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.

AFCDP
France

apep
Spain

GDD
Germany

NGFG
The Netherlands

October 19th, 2012

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

AFCDP,

AFCDP, Association Française des Correspondants à la Protection des Données, was created in 2004, following the modification of the Data Protection Act, which created the function of DPO («Correspondant à la protection des données à caractère personnel» also called CIL, « Correspondant Informatique & Libertés »). AFCDP is a wide forum which welcomes any person interested in the protection of personal data: CIL, data protection managers, lawyers, HR specialists, IT and IS experts, quality and compliance managers, professionals of the e-commerce and marketing sectors … Over 1200 individuals have joined so far this non profit association. AFCDP promotes discussion and information sharing on the protection of personal data in order to facilitate exchange among its members and to promote best practices. AFCDP maintains relationship with the French National Data Protection Commission (CNIL) and other authorities at French and European level involved in the protection of personal data.

Contact

Pascale Gelly, Director - International Affairs, international@afcdp.net - Tel: + 33(0) 6. 71. 61.56.58/ Bruno Rasle, Délégué Général - Tel: + 33(0) 6. 1234. 0884 – delegue.general@afcdp.net Website: www.afcdp.net

APEP

The Spanish Association of Privacy Professionals (Asociación Profesional Española de la Privacidad) was created in 2009 by and for different profiles related to data protection and privacy professional interests, of both the private and the public sectors: in-house lawyers and external legal counsels, IT, IS and CTI experts as well as academics. In 2010, it launches the APEP certification for accountable professionals in order to put in value the DP professional roles and thus to contribute creating trust in the dynamic and emerging privacy market. The APEP has established stable links with several DPAs as well as with privacy-related associations and institutions at the domestic, EU and international levels.

Contact

Ricard Martínez Martínez, E-mail: presidencia@apep.es; Cecilia Alvarez Rigaudias, E-mail: administracion@apep.es; Website: http://www.apep.es/

GDD

The German Association for Data Protection and Data Security (Gesellschaft für Datenschutz und Datensicherheit e.V., GDD) was founded in 1977 and stands as a non-profit organisation for practicable and effective data protection. With more than 2400 – mostly company – members the GDD is Germany`s leading privacy association. Besides offering various member services such as education, training and certification of Data Protection Officers, guides for practitioners and networking opportunities for data protection professionals all across Germany, the GDD also represents member positions at national and European level.

Contact

Christoph Klug, Tel.: +49 170 4878062; E-Mail: klug@gdd.de,Website: http://www.gdd.de

NGFG

Het NederlandsGenootschap van Functionarissenvoor de gegevensbescherming (NGFG) is the Dutch association of Data Protection Officers, a position specified in article 62 of the Dutch Personal Data Protection Act, the Wet beschermingpersoonsgegevens (WBP). WBP has a provision where businesses, branch organisations, governments and institutions are allowed to appoint an internal supervisor for protecting the rights of data subjects, i.e. Data Protection Officers. These individuals supervise the proper implementation, as well as ensuring compliance to applicable laws, regulations and professional codes of conducts, in the field of data protection within their organisation. Thanks to the statutory tasks, responsibilities and authorities, Data Protection Officers have the ability to act independently within their organisations. The appointment of Data Protection Officers is how WBP implemented the ‘ Data Protection Officials’ as referred to in article 18, second paragraph of the Directive 95/46/EC.

Contact

Dr. Sachiko Scheuing, E-mail: secretariat@ngfg.nl,Website: http://www.ngfg.nl

AFCDP
France

apep
Spain

GDD
Germany

NGFG
The Netherlands