CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Improve the protection of (our/your) data: 6 incentives for appointment of DPOs

At a time when EU Institutions seem to focus the debate on whether the Data Protection Officer ("DPO") should or should not be mandatory, CEDPO suggests stakeholders to go beyond this discussion and to focus on adopting effective measures which protect personal data by leveraging the role DPOs can play.

DPOs are key to ensure an effective implementation of complex data protection rules in an increasingly evolving technological environment[1]. Even in countries where DPOs are not mandatory, the number of DPOs appointed by organisations has grown, which signals the need of this function[2]. Still, data controllers and processors, especially in Europe are in need for motivations to appoint individuals assisting them in their compliance efforts. A DPO is not only a first and clear sign of making effective the accountability, privacy-by-design and privacy-by-default principles, but also an indispensable player to carry out privacy impact assessments (PIAs). In addition, the DPO is the appropriate interlocutor vis-à-vis the data subject, the management of the organisation and the Data Protection Authorities ("DPAs") as well as a positive image factor which helps creating trust.

In the regulation, steep fines are introduced as a 'stick' so that organisations are forced to take measures for data protection. CEDPO urges EU Institutions to review the draft regulation and EU Member States to reconsider their policies, in order to also create real incentives for controllers/processors to appoint DPOs. Such incentives will stimulate more DPOs to be appointed, resulting in better protection of personal data.

The following CEDPO proposals for introducing incentives ensure a better protection of personal data and give more chances to the rules to be implemented in practice. These proposals are based on long term experiences aggregated by "*Datenschutzbeauftragter"* in Germany, "*Correspondants Informatique et Libertés*" in France, "*Functionarissen voor de gegevensbescherming*" in the Netherlands and "*Responsables de seguridad*" in Spain.

The CEDPO proposals should by no means be regarded as DPOs replacing DPAs. DPAs will remain the ultimate supervising body on the national level for all organisations and their processing of personal data. By having DPOs assisting the organisations for which they work in ensuring data protection compliance, DPAs will be able to concentrate on providing guidance and carrying out enforcement actions.

CEDPO recommends that the regulation includes clear provisions which incentivise organisations to appoint a DPO. Member States, even those which currently do hot have data protection laws which mandating the designation of a DPO, should create advantages for organisations which appoint a DPO thereby promoting controllers/processors to have their own privacy enhancer. « *My wish is to convince those who would still doubt that the DPO is inevitable to make data protection compliance*

alive" declares Mireille Kalimbadjian, Board Member of AFCDP and Responsable Sécurité Protection Données Personnelles - Caisse d'Epargne PAC, who supports CEDPO's initiative.

Organisations appointing DPOs should be entitled to specific benefits for having taken this additional step towards being accountable over those who haven't made this organisational choice.

In view of the above considerations, CEDPO recommends the following:

1. Dispute resolution

Incentive: Creating a mechanism whereby data protection claims would be first brought to the attention of the DPO before being brought to DPAs or courts.

Role of the DPO: In the first place, the DPO should receive the claims from the data subjects and clarify the purpose of the claim. The DPO will then make the necessary investigations within the data controller/processor to understand the whereabouts and to assess the situation and get back to the data subject with a response and a solution.

"Entrusting the DPO with the task of a dispute resolver shows the data subject the importance of his/her request, while unburdening other departments of my organisation which are not familiar with data protection claims at the same time." Gabriela Krader, Corporate Data Protection Officer Deutsche Post DHL

Benefits: The data subject will be better heard by a professional who cares for data protection and who knows the internal organisation of the data controller/data processor. Giving DPOs the exclusive right to handle complaints in the first instance would reduce claims based on misunderstandings and petty claims going to the DPAs, hence their level of work, enabling them to focus their activities on more essential matters. The data controller/processor will avoid lengthy procedures for issues which may be resolved at an early stage of the dispute, which is very valuable at a time where collective action is being introduced in various countries (through consumer regulations or otherwise).

2. Reduction of bureaucratic burdens / more flexible procedures and formalities

Incentive: Data controllers/processors who appoint a DPO should be relieved from certain formalities with DPAs. An example can be in instances where the draft regulation requires prior consultation or prior authorisation[3]. Similar views have been expressed by MEP Jan Albrecht[4].

Role of the DPO: The DPO supervises the design of a data processing project and the documentation which will be put in place by the data controller/data processor. He/she verifies the project independently, using his/her technical and legal knowledge as well as the knowledge of the environment, in order to assess whether it meets data protection requirements.

"GDD member organisations prefer having a DPO, someone in charge to give recommendations beforehand rather than dealing with possible legal sanctions afterwards. Also our DPAs welcome the preliminary work done by the DPO, someone who is familiar with the organisation and the relevant business processes at a very early stage of projects. New data processing projects should be implemented upon prior consultation of the DPO who knows the guidelines of our DPAs. Companies making this kind of effort should not have to wait with their data processing until the DPA has made a second review. New data processing projects should therefore be implemented upon prior

consultation of the DPO instead of the DPA." Christoph Klug, GDD Representative in charge of International Affairs

Benefits: The data subjects benefit from this arrangement as the prior verification will be carried out by someone (the DPO) who is on the field and who knows the environment in which the data processing is operated. The same person will also be able to answer specific questions related to a data processing project at a later date. DPAs will also benefit from such a provision, as it would limit the demand on their resources which they can focus on other activities, like providing guidance and investigations. DPAs should nevertheless still have the power to investigate the assessments and recommendations of the DPO. The organisations will also benefit from avoiding current bureaucratic burdens which are merely formal. In addition, the DPO as single point of contact with regard to data protection topics will rationalise the consultation process within the organisation.

3. Data breach notification

Incentive: Data controllers and data processors who have appointed a DPO should be exempted from notifying minor breaches to the DPA.

Role of DPO: The DPO will be involved by the data controller/processor at the very early stage of identifying that a breach has occurred and will advise them as to whether a breach is minor or not looking at all circumstances and its consequences, taking into consideration DPAs' and ENISA's guidance.

"What I have understood as head of the working group on security breach notification of AFCDP is that for business, functional and technical staff in various impacted departments, who are not familiar with detailed data protection requirements and guidance, it is often not clear when a security breach leads to the obligation of notifying a DPA. They appreciate the possibility of channelling incidents to the DPO. The management and the DPO then discuss the necessary actions. Pascale Gelly, Attorney – Board Member of AFCDP.

Benefits: 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. By giving the DPO a pivotal role in the data breach analysis[5], incidents will be filtered and the DPAs could therefore also limit the demand on their resources and focus on other activities like assessing serious breaches, providing guidance and carrying out investigations. DPAs do not lose control as they can still investigate to verify how the organisation has reacted, including the checking of the registry of data breaches and the analysis conducted by the DPO. The organisations will benefit from an adequate assessment issued by the DPO regarding privacy regulatory requirements. Furthermore the communication of a possible security breach can be coordinated by one competent internal authority. The data subjects will also clearly benefit from this situation as a qualified professional will be involved in the analysis of the breach and of the remedies that could be adopted, i.e., a DPO, who is often better placed than the DPAs to know the business, commercial and technical environment in which the data processing is operated and to rapidly react in order to minimize damages, if any.

4. Certification

Incentive: Allow controllers/processors the opportunity to either fast track the certification process, extend the period for which the certification is valid for, or, provide them with a certificate with

higher value, in case it has appointed a DPO. Indeed as pointed by JURI, *"Stricter accountability criteria need to be established for organisations which do not have a data protection officer or sufficient certification"*[6].

Role of the DPO: The DPO can play a pivotal role during the certification process. The DPO prepares for the audit by advising on necessary technical and organisational measures as appropriate.

"A well-structured data protection organisation is usually not visible from outside. By certifying business processes in the field of data protection, efforts to ensure effective data protection rules finally become transparent. This includes my work as a data protection officer." Thomas Muethlein, external data protection officer and member of the Board of Directors of the GDD

Benefits: As data protection seals and certificates become a sign of (commercial) trustworthiness, increasing numbers of organisations will be interested in becoming certified or accredited. This will be the case for processors handling personal data on behalf of a multitude of controllers, such as those offering cloud computing services, who are in need of certification mechanisms in order to demonstrate appropriate technical and organisational measures in favour of their clients, respectively the data subjects. The appointment of a DPO is the first sign of the existence of a data protection programme. Furthermore, businesses and institutions with designated and well-integrated DPOs increase their chances of obtaining the certification without major issues, since the DPO would have already checked for legal compliance, prior to the initial assessment by the certifying body. The appointment of a DPO will also allow for the proper maintenance of the standard of data protection over time, once the organization has been certified or accredited. In this sense, the period for which the certification is valid can be extended for controllers/processors with a DPO appointed.

5. Waiver / reduction of sanctions

Incentive: The proposed regulation should provide for the possibility to refrain from administrative sanctions. The presence of a DPO should at least be a mitigating factor when it comes to determining a certain fine since it is a visible sign that the organisation cares about data protection. In their Final Opinions, the IMCO and ITRE Committee of the European Parliament made similar recommendations[78], partially with the view to apply sanctions proportionally.

Role of DPO: The DPO formally examines the processing, which may include information listed in Article 28 of the proposed regulation. This in turn requires a considerable amount of time, effort, and resources to be committed by the controller/processor in ensuring compliance within the organisation. Therefore, the involvement of the DPO has to be taken into account when considering to impose a certain sanction on an organisation.

"*Our efforts in improving the data protection business culture must be taken into account. In Spain, where the DPA has actively exercised its enforcement powers, the existence of an accountable data protection programme, which obviously requires the active and prominent involvement of a DPO, was introduced in the law as a criteria –among others– to fix the final sanction. More proportionate sanctions are now imposed.*" Ricard Martínez, DPO of the University of Valencia, Spain

Benefits: If data controllers/processors have implemented processes involving a DPO's review, and if they have followed their DPO's recommendations, their intention and efforts should be taken into account when considering to impose sanctions. This would encourage the spreading of good practices among organisations in Europe and help for better data protection.

6. Accompanying DPA investigations

Incentive*:* The proposed regulation should provide that the DPAs should inform the DPO about upcoming investigations as appropriate. Obviously, there would be exceptions to prior information in case of emergency or if circumstances so require. The DPO should also have a say in the investigation: being a counterpart in the supervision, he should be heard by the DPA. In addition, an appropriate and adequate involvement of the DPO in the investigation process should be secured.

Role of the DPO: The DPO will be the interface between the data controller and the DPA in order to ensure smooth completion of the investigation and common understanding of the DPA`s requests. The DPO will be the knowledgeable person for the investigated organisation enabling the DPA to carry out its investigation more efficiently.

"Data controllers/processors should not be treated de facto as offenders. We have seen in several instances that when prior notice was given by the CNIL, DPOs were given a chance to present the CNIL investigation positively to the data controller/processor and to gather documents in advance and get better staff availability and cooperation, than if the CNIL investigators had come in the morning unannounced". Xavier Leclerc, external Data Protection Officer, Board Member – AFCDP

Benefits: DPO supported investigations will be conducted efficiently. Professional judgment of the DPO will be made available. In addition, the controller/processor will be better assured that business sensitive information will be treated with appropriate care during the inspection.

Please note: CEDPO has developed its original position in a First Position Paper dated 30th March 2012 and has made amendment suggestions to the draft regulation in a Redlined Text dated 19th October 2012. The relevant papers including an Executive Summary are available at www.cedpo.eu. These documents include *CEDPO`s* views on the mandatory appointment of DPOs.

On this topic, since the debate is not yet closed, CEDPO considers that the Regulation must at least preserve the mandatory appointment of DPOs which exists under the current national data protection laws which implemented the European Data Protection Directive.

Bonn, Den Haag, Madrid, Paris 24, September 2013

About CEDPO:

The Confederation of European Data Protection Organisations (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 Genootschap van Functionarissenvoor de Gegevensbescherming) of the Netherlands.

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.

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: secretaariat@ngfg.nl,Website: http://www.ngfg.nl

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

[1] 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. 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.*

"DPOs are a vital tool in protecting personal data and helping modern firms comply with data protection rules." European Commission Vice-President Viviane Reding explicitly referred to CEDPO when advocating in favour of DPOs and flexibility before the Irish Council Presidency (http://europa.eu/rapid/press-release_SPEECH-13-209_en.htm) on 8March 2013.

"The rapporteur welcomes the proposed shift from notification requirements to the Data Protection Authorities (DPAs) to practical accountability and corporate Data Protection Officers (DPOs). The proposed regulation can be simplified by merging information rights and documentation requirements essentially being two sides of the same coin. This will reduce administrative burdens for data controllers and make it easier for individuals to understand and exercise their rights (articles 14, 28).", report of LIBE Committee of 17.12.2012.

[2]Since its creation in 2000, the IAPP, International Association of Privacy Professionals has seen the number of members grow beyond 10 000 worldwide.

[3] E.g. Article 34. Par 2.

[4] Approach supported by European Parliament Rapporteur Jan Albrecht in his Draft Report: *"Instead of consulting the supervisory authorities prior to data processing that involves specific risks, the data controller should make use of its own data protection officer, if it has appointed one. This takes unnecessary burdens from the authorities while strengthening the role of the data protection officer."*

[5]The proportionality analysis and the risk based approach is already known in France and Spain in the financial sector which is bound to appoint a correspondent with anti-money laundering authorities to dialog when there is a suspicion of anti-money laundering activity. Impacted entities are used to draw maps of risks defining various vigilance levels (light, normal, reinforced), according to the risk and to interact with authorities and make decisions whether or not to notify. The correspondent plays an important role here for the interaction.

[6]JURI final opinion on Article 28 2nd paragraph.

[7] IMCO Doc. 2012/0011(COD), p. 107.

[8] ITRE Doc. 2012/0011(COD), p. 161, 162.