Privacy Interviews with Experts
November 2015

Ricard Martínez Martínez

President
Spanish Association of Privacy Professionals (APEP)
Madrid, Spain

Cecilia Álvarez Rigaudias

Vice-President
Spanish Association of Privacy Professionals (APEP)
Madrid, Spain

The Role of Data Protection Officer in the new General Data Protection Regulation.

Ricard Martinez is Data Protection Officer and Associate Professor of Constitutional Law at the Universitat de València. He also chairs the Spanish Association of Privacy Professionals (APEP) and has previously been in charge of the Research Department of the Spanish Data Protection Agency (AEPD). Martinez is the author of numerous publications that provide guidance to companies on addressing these topics.

Cecilia Álvarez is the Pfizer European Data Protection Officer Lead. She is the Vice –President of the Spanish Association of Privacy Professionals (APEP) as well as a member of Confederation of European Data Protection Organizations CEDPO and the Steering Committee of The Sedona Conference. Cecilia is the author of several publications on data protection and regularly conducts workshops and conferences on this field.

Nymity: Which provision of the current European Directive (95/46/CE) regulates the role of the Data Protection Officer (DPO)? What are the powers assigned to this role?

Álvarez: The Directive 95/46/EC gave European Union member states the possibility to introduce into their national law the appointment of a Data Protection Officer (DPO). The relevant provisions are arts. 18(2) and 20(2).

Art. 18.2 Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

> *- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive*
>
> *- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),*
>
> *thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.*

Article 20

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

Nymity: How have the different European countries adopted the European Directive with regard to the role of the DPO?

Álvarez: Some Member States have imposed a DPO in their local data protection regulations. As a result thereof, the DPO role and tasks are not harmonised. For example, in Spain, the "mandatory" DPO is actually a mere security officer that must be appointed only when the processing concerns specific categories of data that deserve a reinforced security protection (including but not limited to the sensitive data). CEPDO undertook in 2012 a comparative analysis on the different DPO roles among the EU Member States that may be found here: http://www.cedpo.eu/wp-content/uploads/2015/01/CEDPO_Studies_Comparative-Analysis_DPO_20120206.pdf

Nymity: What are the differences between the roles of a Data Protection Officer and Data Security Officer (DSO)? Is the appointment of a DSO mandatory for companies operating in European countries?

Álvarez: The DSO concept may be deemed linked to the security provisions included in article 2(4) of the Directive 2009/136/EC amending Directive 2002/58/EC. However, this only applies to providers of publicly available electronic communication services. Under this provision, the DSO would be deemed responsible for protecting data against their unauthorized disclosure, takeover by an unauthorized person, or any change, loss, damage or destruction. He / she also supervises the implementation of technical and organizational measures to protect the personal data being processed, appropriate to the risks and category of data being protected.

Leaving aside this specific provision, in my opinion, the DSO would be the person in charge of any physical and logical security matters (including cyber security issues), and irrespective of whether the security risks or breaches refer to personal data or other kind of information.

The DPO would be assisting the organisation in the design, implementation and supervision of an effective personal data protection programme adapted to the specific data protection risks of the organisation. The security chapter is only one (and very important) of the elements of a data protection programme.

Nymity: Which provisions of the new General Data Protection Regulation (GDPR) regulate the role of DPO? Does this regulation make it mandatory for companies operating in Europe to appoint a DPO?

Álvarez: The approach of the institutions involved in the dialogue is divergent. In particular, it does not seem that the Council is in favour of the mandatory role. Irrespective of whether the law imposes the DPO or not, there is no controversy on the fact that (under the current Directive 95/46/EC and the future GDPR) the data controller and a data processor are and will be legally obliged to ensure (and be accountable for an) effective personal data protection. This cannot be achieved without a data protection culture embedded in the organisations lead by an expert on the field.

Nymity: What is the Confederation of European Data Protection Organizations (CEDPO) and what is its approach on this issue?

Álvarez: 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 Functionarissen voor de Gegevensbescherming) of the Netherlands. In February 2014, ADPO (The Association of Data Protection Officers) of Ireland, ARGE DATEN of Austria, and SABI (Stowarzyszenie Administratorów Bezpieczeństwa Informacji) of Poland joined CEDPO.

CEDPO aims to promote the role of the Data Protection Officer, to provide advice on balanced, practicable, and effective data protection and to contribute to a better harmonisation of data protection law and practices in the EU/EEA. In this light, position papers on the mandatory role of the DPO and on suggested incentives for his/her appointment have been

produced and presented to representatives of the EU Commission, the Parliament and the Council. They may be found at **www.cedpo.eu.**

Nymity: As a member of the CEDPO, what are the concerns of the Spanish Association of Privacy Professionals (APEP) regarding the role of a DPO in the GDPR?

Martínez: Through CEPDO, we have supported the mandatory role of the DPO taking into account processing risk-based criteria and we also suggested amendments to the GDPR in order to ensure that the DPO has sufficient tools and power within the organisation to effectively contribute to an effective and balanced data protection. Assuming that it could be the case that the DPO is not a mandatory role in the final text, we also think that the GDPR should include incentives for the organisations to appoint DPOs as further explained in the paper "Improve the protection of (our/your) data: 6 incentives for appointment of DPOs" accessible at http://www.cedpo.eu/wp-content/uploads/2015/01/CEDPO_Position_Paper_Incentives_DPO_20130924.pdf .

We must go beyond the superficial and inaccurate idea that a DPO is *only* a cost!

APEP would very much welcome that the DPO becomes mandatory in the GDPR. Indeed, an "official" recognition of the role, tasks and reporting line helps to raise privacy awareness within the organisations and is key for them to be able to approach privacy in balanced and expert manner, which is essential in the digital economy. In addition, it would also enable to create a true pan-European market of privacy professionals who may compete under the same conditions, irrespective of the jurisdiction. If this role is not made mandatory in the GDPR, we expect the DPAs, including the Spanish DPA, supporting and promoting this role, in particular, in case the fact that it becomes or not mandatory is left to the Member States' discretion.

Nymity: How is the role of DPO regulated in Spain? In practice, how are companies operating in Spain currently dealing with the implementation of this role?

Martínez: The "legal" role in Spain is limited to the monitoring of the compliance with the duties on the security measures that are listed in the law.

However, in practice, the DPO plays a larger role to the extent he/she advises the organisation in how to integrate privacy in the business culture, and this goes beyond security. In such a case, it is not unusual that the DPO forms part of the legal department or his/her tasks are actually divided into the legal and IT departments. He/she uses to play a privacy compliance role but when the organisation really pays attention on privacy, his/her role is close or embedded in the organisation's top management.

Nymity: What are the top 5 recommendations that you would give to companies operating in Europe in connection with appointing a DPO?

Álvarez and Martínez:

As it was said in the most recent CEDPO event that took place during the 37Th International Conference of Privacy and Data Protection Commissioners (https://www.privacyconference2015.org/the-dpo-in-times-of-expanding-data-driven-world/), a DPO should be a smart individual making smart decisions and in the right place of the organisation. This would mean, in our opinion, that a DPO job description must consider the following 5 features:

- Data protection expertise;
- As a general rule, appropriate knowledge of the business and time availability (to be adapted to the actual privacy needs of each organisation);
- Managerial and social skills (the role requires leadership and to be able to "sell" the privacy argument);
- Not working on a "silo" and, in particular, included in the business projects from the start; and
- Strongly supported by the organisation leadership (the DPO's independence of criteria and effectiveness may only be ensured if the individual at hand has effective powers and resources within the organisation).