THE GENERAL DATA PROTECTION REGULATION IN THE SPANISH SYSTEM: THE DATA PROTECTION OFFICER

ROBERT RUBIÓ

PHD RESEARCHER, UNED

CÁTEDRA JEAN MONNET DE DERECHO PRIVADO EUROPEO

UNIVERSIDAD DE BARCELONA

WORKING PAPER

6/2018

WORKING PAPERS
JEAN MONNET CHAIR
EUROPEAN PRIVATE LAW

UNIVERSITAT DE BARCELONA

Abstract: The new General Data Protection Regulation (GDPR) is set to replace the Directive 95/46/EC, effective May 25, 2018. In accordance with the principle of primacy of the EU law, the GDPR shall be directly applicable in each Member State and will lead to a greater degree of data protection harmonization across EU Members.

The GDPR contains a number of new protections for EU data subjects and obligations, among them, a significant impact over national systems, as it requires in certain cases the mandatory designation of a Data Protection Officer (DPO). Thus, emphasis is put on the importance of the new position of DPO and consequences over the Spanish national system.

Title: The General Data Protection Regulation in the Spanish System: The Data Protection Officer.

Keywords: data protection officer, data protection, DPO, GDPR, LOPD, personal data, privacy.

Resumen*: El nuevo Reglamento General de Protección de Datos (RGPD) se establece para reemplazar la Directiva 95/46/CE, aplicable a partir del 25 de mayo de 2018. De acuerdo con el principio de primacía del derecho de la UE, el RGPD será directamente aplicable en cada Estado miembro y conducirá a un mayor grado de armonización en protección de datos entre los miembros de la UE.*

El RGPD contiene una serie de nuevas protecciones y obligaciones para los sujetos de la UE, entre ellas, un impacto significativo sobre los sistemas nacionales, ya que requiere en ciertos casos la designación obligatoria de un Delegado de Protección de Datos (DPO). Por lo tanto, se hace hincapié en la importancia de la nueva posición de DPO y las consecuencias sobre el sistema nacional español.

Título*: El Reglamento General de Protección de Datos en el sistema español: el delegado de protección de datos.*

Palabras clave: *datos personales, delegado de protección de datos, DPO, LOPD, privacidad, protección de datos, RGPD.*

Índice

I. Introduction

The right to protection of personal data is a fundamental right. It is different from, but closely linked to, the right to respect for private and family life.[1]

In this sense, the protection of personal data in the European Union (EU) has been always a field of discussion in practice. In the 1990s, protection of personal data was regulated by non-harmonized laws in the Member States. Although based on the same basic principles laid down in the Council of Europe Convention No. 108 on data protection,[2] these laws differed considerably in detail. Because this was considered to influence competition and thus the well-functioning of EU's internal market, pressure increased for a more harmonized environment.

This led to the adoption in 1995 of the Directive 95/46/EC[3]. It is the central piece of legislation on the protection of personal data in Europe. The Directive stipulates general rules on the lawfulness of personal data processing and rights of the people whose data are processed, and it was transposed into the Spanish system by means of the Organic Law 15/1999, of 13 December, on the Protection of Personal Data (LOPD).

With the new century, the General Data Protection Regulation (GDPR)[4] is set to replace the Directive 95/46/EC effective May 25, 2018. The GDPR constitutes a unitary and updated set of rules applicable to the processing of data of European citizens throughout the territory of the EU. It will thus avoid fragmentation of the market within the EU, resulting from the transposition of the Directive 95/46/EC into national system on data protection.

The main objectives of the GDPR is to facilitate cross-border business and corporate activity, the free movement of personal data and the greater guarantee of the fundamental rights and freedoms of European citizens. Among other aspects, the GDPR also requires public authorities – and, in some cases, private companies, to appoint a Data Protection Officer (DPO).

---

[1] This distinction is notably made in the EU Charter of Fundamental Rights - which mentions the two rights separately, although next to each other in Articles 7 and 8.

[2] Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data, 28 January 1981.

[3] European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of
Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 24 October 1995.

[4] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 27 April 2016 (General Data Protection Regulation).

The implementation of the GDPR will certainly represent new challenges for public authorities and companies in the EU when it comes to responding to the DPO requirement. It is precisely in a broad digital and technological horizon in which the DPO, designed by the GDPR, acquires full meaning and practical application relevant to the processing of personal data.[5]

II. The Data Protection Officer

1. Concept of DPO

The concept of DPO is not coetaneous to the EU framework, i.e. Directive 95/46/EC. [6]

In this regard, the idea of a data protection official, appointed by a controller[7] to ensure compliance with data protection requirements within the organization of the controller, is of German origin.[8]

Thus, although no EU regulation required any organization to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years as mentioned below.

In this sense, the DPO plays a fundamental role in ensuring respect of data protection requirements within the institution/body concerned. The DPO should be appointed by his institution to advise it on the application of the rules, but he/she is also required to ensure, in an independent manner, that the applicable data protection regulations are applied internally.

These responsibilities mirror those of privacy professionals elsewhere around the globe and signal a growth spurt for the profession in the EU according to the International Association of Privacy Professionals (IAPP).[9]

[5] International Association of Privacy Professionals, cited 2016: *Study, At Least 28,000 DPOs Needed To Meet GDPR Requirements*.

[6] Vide Germany, Federal Data Protection Act, 1 February 1977, where it stated in section 38 B*eauftragter für den Datenschuzt* that "*Die in & 31 genannten Personen, Gesellschaten und anderen Personenvereinigungen haben einen Beauftragten für den Datenschutz zu bestellen. Die Vorschriften über den Beauftragten für den Datenschuzt in && 28 und 29 gelten entsprechend.*".

[7] Controller means the institution, body, or any other organizational entity which alone or jointly with others determines the purposes and means of the processing of personal data.

[8] Vide Lee Riccardi, J.: *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?*, 6 B.C. Int'l & Comp. L. Rev. 243 (1983), http://lawdigitalcommons.bc.edu/iclr/vol6/iss1/8

[9] Vide Heimes, R.: *Top 10 operational impacts of the GDPR: Part 2 - The mandatory DPO*, International Association of Privacy Professionals, cited 2016.

2. The DPO in the Directive 95/46/EC

The idea of a DPO in the EU framework originates from Article 18.2 of the Directive 95/46/EC, which allows Member States to exempt controllers from notification of a processing operation to the national data protection authorities where the controller appoints a data protection official.

This alternative to notification provided by the Directive 95/46/EC was implemented in several Member States, such as Germany, the Netherlands, Sweden, Luxembourg and France.[10]

The consequence is that notification is then not required anymore; thus the DPO must maintain a register of processing operations containing the information that would have had to be made in case of notification.[11]

By contrast, Spain did not avail itself of the possibility to introduce any exemptions at all from notification for innocuous processing operations.

The point to be noted here is that - in spite of some similarities and parallels – the standards in the different Member States differ significantly in scope and detail.[12]

Even with respect to similar operations which, in different Member States, are subject to exemptions the norms are different. Leading to the situation that entities which want to harmonize such operations throughout their different establishments in the EU will therefore often not benefit from such "simplified norms" or exemptions.[13]

3. The DPO in the GDPR

The GDPR recognizes the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks.

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO. Thus, Article 37 of the GDPR states that DPOs must be appointed for all public

[10] Vide European Commission, cited 2003: *Commission's first report on the transposition of the Data Protection Directive - Analysis and impact study on the implementation of Directive EC 95/46 in Member States*.

[11] Indeed, the Article 29 Working Party argued that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses.

[12] For example, in Spain, there is the need for a security manager that must be appointed only when the processing concerns specific categories of data that deserve a reinforced security protection (including but not limited to sensitive data).

[13] Vide European Commission, cited 2003: *Commission's first report on the transposition of the Data Protection Directive - Analysis and impact study on the implementation of Directive EC 95/46 in Member States*.

authorities, and where the core activities of the controller or the processor involve "*regular and systematic monitoring of data subjects on a large scale*" or where the entity conducts large-scale processing of "*special categories of personal data*" (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and the like, defined in its Article 9).[14]

In this regard, a mention has to be made that although an early draft of the GDPR limited mandatory DPO appointment to companies with more than 250 employees, the final version has no such restriction.[15]

With regards to the DPO function, Article 37 does not establish the precise credentials DPO must carry but does require that they have "*expert knowledge of data protection law and practices*." The GDPR's recitals suggest the level of expert knowledge "*should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor.*"

In this way, the controller or the processor also has a crucial role in enabling the effective performance of the DPO's tasks.

Back to the DPO's tasks, they are also delineated in Article 39 of the GDPR to include:

a) Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.

b) Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits.

c) Advising with regard to data protection impact assessments when required under Article 35.

d) Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.

[14] The appointment of a DPO is also mandatory for competent authorities under Article 32 of Directive 2016/680 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, and national implementing legislation.

[15] Vide Article 25.2 of the Proposal for a Regulation of the European Parliament and of 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).

e) Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

In fact, the GDPR borrows some concepts from Germany's Federal Data Protection Act, which already requires a DPO to be appointed by firms with at least nine people employed in the automated processing of personal data, or at least 20 people who are engaged in non-automated data processing. [16]

DPOs under the GDPR are expressly granted significant independence in their job functions and may perform other tasks and duties provided they do not create conflicts of interest. Job security is another perk; the GDPR expressly prevents dismissal or penalty of the DPO for performance of the tasks and places no limitation on the length of this tenure.

Thus, an entity with multiple subsidiaries (a "group of undertakings") may appoint a single DPO so long as she is "*easily accessible from each establishment*."

The GDPR also allows the DPO functions to be performed by either an employee of the controller or processor or by a third-party service provider, creating opportunities for consulting and legal firms to offer outside such DPO services.

However, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

III. The Data Protection Officer into the Spanish system

1. The DPO in Spain: a new player

With the entry into force of the GDPR, a new player has been further enshrined that is key for ensuring data protection compliance, the DPO.

[16] Vide Section 4f of the Germany, Federal Data Protection Act, 14 January 2003: "*Data Protection Official: (1) Public and private bodies which process personal data automatically shall appoint in writing a data protection official. Private bodies are obliged to appoint such an officer within one month of commencing their activities. The same shall apply where personal data are processed by other means and at least 20 persons are permanently employed for this purpose. The first and second sentences above shall not apply to private bodies which generally deploy a maximum of nine employees to carry out the automatic processing of personal data on an ongoing basis. In so far as the structure of a public body requires, the appointment of one data protection official for several areas shall be sufficient. In so far as private bodies carry out automated processing operations which are subject to prior checking or process personal data in the course of business for the purposes of transfer, anonymized transfer, or market or opinion research, they are to appoint a data protection official irrespective of the number of persons deployed to carry out automatic processing*."

Apart from the mandatory DPO designations as per Article 37 of the GDPR, it is also foreseen the possibility for the Spanish legislator to require the designation of DPOs in other situations as well as the opportunity for interested entities in designating a DPO on a voluntary basis.[17]

However, it must be noted that when an entity designates a DPO on a voluntary basis, the same requirements under Articles 37 to 39 of the GDPR will apply to his or her designation, position and tasks as if the designation had been mandatory.

Although this does not prevent an entity, which does not wish to designate a DPO on a voluntary basis and is not legally required to designate a DPO, to nevertheless employ staff or outside consultants with tasks relating to the protection of personal data.

In such a case, it is important to ensure that there is no confusion regarding their title, status, position and tasks as regards the DPO function.[18]

2. Basic conditionings

The DPO function requires certain basic conditionings for the proper enforcement of his functions that will be also required in Spain,[19] namely the DPO:

a) Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices;

b) May be a staff member or an external service provider;

c) Contact details must be provided to the relevant Data Protection Authority, i.e. AEPD[20];

d) Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge;

e) Must report directly to the highest level of management; and,

f) Must not carry out any other tasks that could results in a conflict of interest.

Noted the above-mentioned conditionings, I will also reflect below those aspects that may have a particular interest as per the existing practice in Spain.

[17] In this regard, the Article 29 Data Protection Working Party has encouraged these voluntary efforts.
[18] This clarity is required in order to avoid the collateral application of the DPO requirements, when its application is not desired.
[19] Vide Article 29 Data Protection Working Party, cited 2016: Guidelines on Data Protection Officers ("DPOs").
[20] Spanish Data Protection Agency

3. A new function

The new function of DPO will most probably require a lot of investment at the beginning in order to raise the awareness of staff and to ensure compliance in the field of notifications.

Both the public and the private sector are moving slowly to adapt the organizations to the GDPR and are giving the impression that they will arrive late to its proper compliance. This impression is giving without considering the possibility of the Spanish legislator to enlarge the obligation for the designation of a DPO to other situations not foreseen in the GDPR.

The AEPD, as main authority in the field, should recommend the appointment of a full-time DPO at least at the start of the function.[21]

As an alternative, a common/shared DPO could be a solution especially for small organizations where the appointment of a full-time DPO is not feasible.

However, the appointment of a "shared" DPO between organizations must be made conditional upon the fact that the institutions are closely connected both in their functioning and their geographical location or organization.

4. Compliance and liability

The GDRP entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR.[22]

The Recital 97 of the GDRP further specifies that the DPO "*should assist the controller or the processor to monitor internal compliance with this Regulation*".

Thus, monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*".[23]

[21] Indeed, a preferable measure to determine the time needed to carry out the function and to determine appropriate level of priority for DPO duties is to encourage the organizations to draw up in advance an Audit and Compliance Plan. This Plan could also be a useful instrument in the evaluation of the DPO once designated.
[22] Vide Article 39 of the GDPR.
[23] Vide Article 24.1 of the GDPR.

According to the GDPR, the data protection compliance is the responsibility of the controller or the processor. However, we should also refer to the professional liability of the DPO and how it will affect the Spanish system.[24]

Thus, we should expect from the Spanish legislator specific provisions applying to the DPOs or, at minimum, further clarifications on its level of liability.

This clarification is of major importance for those DPOs on the basis of a service contract,[25] as such entities providing the service would also incur in 2 kinds of liability. The first one is of contractual nature, arising from the service relationship with the entity requesting the services, while the second one is of non-contractual nature as regards the damages that the service provided, and how it is provided, may cause to third parties i.e. the data subjects.[26]

On this topic, specific references and clarifications should be also made to the bound of secrecy and confidentiality foreseen in the GDPR, namely the possible linkage with the AEPD in order to ensure compliance with the regulation.[27]

Indeed, although the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, this obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the AEPD.

Therefore, the Spanish legislator should tackle this balance between secrecy or confidentiality and the good performance of its functions, in direct link with the professional liability I was referring above.

5. Dismissal

According to the Article 38.3 of the GDPR, the DPOs should "not be dismissed or penalised by the controller or the processor for performing his tasks".

This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks. Indeed, penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO.

[24] Specific references to DPOs in the public sector will be tackled afterwards.
[25] Accordingly, the function of the DPO could be exercised on the basis of a service contract concluded with an individual or an organization outside the controller's/processor's organization.
[26] Vide STS 7448/1998, of 10 December, that establishes regarding the auditors responsibility that "*La auditoría de cuentas es, por lo tanto, un servicio que se presta a la empresa revisada y que afecta e interesa no sólo a la propia empresa, sino también a terceros que mantengan relaciones con la misma, habida cuenta que todos ellos, empresa y terceros, pueden conocer la calidad de la información económico-contable sobre la cual versa la opinión emitida por el auditor de cuentas*."
[27] Vide Article 38.5 of the GDPR.

However, the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. In practice, this may lead in practice to a deviation in the way the DPO function is performed against an unfair dismissal.[28]

As best practice, the Spanish legislator should foresee that for a possible dismissal of a DPO or termination of the service contract, this action should require the prior notification to the AEPD.[29]

Indeed, the prior notification should also include the reasoning and justifications for taking such extreme measure against a professional that must always act in an independent manner.[30]

Based on the reasoning and the justifications, the AEPD could take action against such decision by means of conducting investigations on the due application of the regulations. In addition, in case of an unfair dismissal, there could be also specific provisions in the form of penalties.[31]

6. Differences with the "Security Manager"

With the incorporation of the DPO, the Spanish legislator might see it as a way to give greater strength to the existing role of Security Manager foreseen in the Royal Decree 1720/2007, of 21 December, which approves the Regulation implementing the LOPD.

The Security Manager is under the Spanish data protection regime the person formally designated by the controller to coordinate and control all applicable security measures.[32]

However, there should not be an automatic transition from Security Managers to DPOs.

Precisely, the role of the DPO requires an expertise and qualifications, including the availability to perform his duties, which were not required for the Security Manager in the above-mentioned Royal Decree 1720/2007.

Therefore, for sake of clarity, both the AEPD and the Spanish legislator should make clear the distinction between both roles, and in any case, avoid the confusion of functions or the automatic conversion of Security Managers into DPOs.

[28] i.e. Unfair contractual termination in case of a service contract.
[29] Vide Article 24.5 of the Regulation 45/2011.
[30] Here we should distinguish those aspects not foreseen in the contractual relationship from those aspects foreseen, i.e. conflict of interest.
[31] Vide Article 84 of the GDPR.
[32] Vide Article 5.2.l and 95 of the Royal Decree 1720/2007.

7. The role of the AEPD

Ensuring compliance with the GDPR will be influenced by the working relationship between the DPO and the AEPD.

Currently, under the LOPD framework implementing Directive 95/46/EC, controllers are required to notify their data processing activities to the AEPD.[33]

However, under the GDPR, the role of the DPO will come to replace some of the functions that up-to-now are inherent to the AEPD. In this regard, the DPO should not be seen as an agent of the AEDP, but as a part of the organization in which he/she works.

As already mentioned in previous sections, the proximity *de-facto* puts the DPO in an ideal situation to ensure compliance from the inside and to advise or to intervene at an early stage thereby avoiding possible intervention from the supervisory body. At the same time, the AEPD can offer valuable support to DPOs in the performance of their function in the benefit of his/her organization.

Indeed, in the area of implementation of particular data protection measures, synergy potentials between the DPOs and AEPD emerge as regards the adoption of sanctions and handling of complaints and queries. As already mentioned, the DPOs have limited powers of enforcement. Here is where the AEPD should contribute to ensuring compliance with the GDPR, by taking effective measures in the field of prior checks and of complaints and other inquiries.

The AEPD should also, in the new scenario granted by the GDPR, support the idea of developing possible synergies with the DPOs, which would contribute to achieving the overall aim of effective protection of personal data within the organizations. However, those synergies require trust between the parties and the only way to obtain it is by means of responsibility.

8. The DPO in the public sector

When the GDPR requires the designation of a DPO "*where the processing is carried out by a public authority or body*", we must note that the GDPR does not define what constitutes a "*public authority or body*".

Accordingly, public authorities and bodies should include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.

[33] Vide Article 26 of the LOPD.

The main impact of the definition is that in such cases, the designation of a DPO is mandatory.

In this regard, in Spain we must refer to the Law 40/2015, of 1 October, on the Legal Framework of the Public Sector that in its Article 2 establishes the subjective scope, as follows:

1. *This Law applies to the public sector which includes:*
    a) *The General State Administration.*
    b) *The Administrations of the Autonomous Communities.*
    c) *The Entities that make up the Local Administration.*
    d) *The institutional public sector.*
2. *The institutional public sector is integrated by:*
    a) *Any public bodies and entities governed by public law linked or dependent on Public Administrations.*
    b) *Entities governed by private law linked to or dependent on Public Administrations that will be subject to the provisions of the rules of this Law that specifically refer to them, in particular to the principles set forth in article 3, and in any case, when exercising administrative powers.*
    c) *The public universities that will be governed by its specific regulations and supplemented by the provisions of this Law.*
3. *The General State Administration, the Administrations of the Autonomous Communities, the Entities that make up the Local Administration, as well as the public bodies and entities of public law provided for in letter a) of section 2, are considered as Public Administrations.*

As per the above subjective scope, we may understand that the designation of a DPO will be mandatory to the public sector as defined in the above Law 40/2015.

Here, it is also interesting to note that the DPO shall cover all processing operations carried out by the entities of the public sector as referred above, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

9. The DPO designation in the public sector

The question that arises once defined the concept of "*public authority or body*" is to which extend the DPO designation in the public sector will be subject to additional conditionings.

At this point, we must refer to the Royal Legislative Decree 5/2015, of October 30, approving the revised text of the Basic Statute of the Public Employee ("EBEP").

First, I must note that the EBEP is the law that establishes a homogeneous model for the Spanish Civil Service, whilst respecting the competences of the other regional and local administrations, it sets out the common rules applicable to the different categories of public employees.

Regarding the DPO function, I would point out Article 9.2 of the EBEP that establishes: *"2. In any case, the exercise of functions which involve direct or indirect participation in the exercise of public powers or in the safeguarding of the general interests of the State and of the Public Administrations are exclusively for civil servants, upon the terms established by the law of development of each Public Administration."*

The question is not trivial, as the understanding of the functions of the DPO, according to said Article 9.2, will establish the way public sector has to fill the DPO posts.[34]

However, there is no law in force in Spain that defines "*public powers"* or *"in the safeguarding of the general interests"*.[35]

To this effect, considering that those functions as per Article 9.2 of the EBEP are provided only to Spanish nationals,[36] the lack of a clear definition of "*public powers*" or *"in the safeguarding of the general interests"* has been addressed by the ECJ when balancing this restriction with the freedom of movement for workers, one of the founding principles of the EU.

According to the ECJ's case-law, the concept of public service must be given uniform interpretation and application throughout the EU and cannot therefore be left entirely to the discretion of the Member States.[37]

The ECJ stated that: "*The Community meaning of public service must, according to the Court's case-law, be interpreted strictly as being a derogation from a fundamental principle of Community law and be limited to what is strictly necessary for safeguarding the interests […] It is to be understood in a functional way: what is important is that the activity is typically associated with rights exercised under powers conferred by public*

[34] This question could be also addressed by law, as per Article 9 of the EBEP, declaring the DPO function exclusively for civil servants. In the absence of such a law, the understanding of the DPO functions as per Article 9.2 becomes of major importance.
[35] Vide Cantero Martínez, J.: *Funcionarios y Laborales (A Propósito del ejercicio de Potestades Públicas en la Administración y de la Reserva Funcionarial),* VI Congreso Internacional sobre Gestión de Recursos Humanos en la Administración Pública - June 2010, Vitoria.
[36] Vide Article 57.1 of the EBEP.
[37] Vide Cases C-152/73 *Sotgiu* and C-149/79 *Commission v Belgium*.

law, while at the same time responsibility for safeguarding the general interests of the State is vested in the person holding the post."

Hence, in my opinion, the functions of the DPO are safeguarding in the concerned institution both the public interest and a fundamental right – the right to protection of data.[38] In addition, we could also refer that the data processing by the public sector is in numerous cases linked to a legal mandate.

In this sense, we may refer to Article 24 of the Regulation 45/2001 establishing the need for appointing "*at least one person as data protection officer*" or the conditions for dismissal "*He or she may be dismissed from the post of Data Protection Officer by the Community institution or body which appointed him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties*".[39] Both aspects reinforce the idea of the DPO as civil servant safeguarding the general interest of its organization in an independent manner.

Based on this reasoning, the DPO as external service provider in the public sector would not be possible under the Spanish legal framework.[40]

In addition, the filling of the DPO post thus would require the accomplishment of the selection procedures as stated in the EBEP (i.e. competition).[41]

In any case, there should collaboration mechanisms between the various levels of DPOs in relation to the existing configuration and balances of the public sector.

Ultimately, noting the difficulties to fill the DPO posts in due time, the Spanish legislator should include either in a possible draft reform or as a transitional provision in another law, the mechanisms to fill the DPOs posts in the public sector.

IV. Conclusions

The GDPR shall affect all entities and institutions that collect and process personal data in Spain. In practice, this means nearly the entire scope of institutions as nowadays, it

[38] Here we could limit the scope to those public-sector entities that are processing data related to the performance of a public task or exercise of official duty.

[39] European Union, Regulation (EC) 45/2001 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of such Data, 18 December 2000.

[40] In this regard, we may refer to the provisions of the Regulation 45/2011 where it requires a person, excluding the possibility for an external service provider *"1. Each Community institution and Community body shall appoint at least one person as data protection officer."*

[41] Vide Article 55 et seq. of the EBEP.

is almost universal that all organizations and companies have databases of contacts, customers, employees, members, suppliers, etc.

Among the technical differences foreseen in the GDPR vs Directive 95/46/EC, the GDPR introduces:

1. An enlarged territorial scope;
2. A new Data Protection Impact Assessment as a mean to identify high risks to the privacy rights of individuals when processing their personal data;
3. Strengthened conditions for consent;
4. Mandatory breach notifications;
5. The concepts of Data protection by design and by default;
6. The accountability of both controllers and processors:
7. An increase of administrative fines that may apply to;
8. The possibility of data portability and the right to be forgotten; as well as,
9. The value of privacy on the ground by requiring the designation of a DPO in certain cases.

Therefore, the GDPR contains a number of new protections for EU data subjects and obligations, among them, a significant impact over the Spanish national system, the designation of the so-called DPO.

The GDPR also recognizes the DPO as a key player in the new data governance system and lays down conditions for his appointment, position and tasks. In this regard, the GDPR also foresees, within its margin of manoeuvre for Member States, the possibility for the Spanish legislator to require the designation of DPOs in additional situations as well as the opportunity for interested entities in designating a DPO on a voluntary basis.

Thus, the characteristics of the DPO function under the Spanish system are pending to be further defined according to the margin of manoeuvre foreseen in the GDPR.

Indeed, the new function of DPO will most probably require a lot of investment at the beginning to raise the awareness of staff and to ensure compliance in the field of notifications.

In fact, both the public and the private sector in Spain are moving slowly to adapt the organizations to the GDPR and are giving the impression that they will arrive late to its

proper compliance. This impression is giving without considering the possibility of the Spanish legislator to enlarge the obligation for the designation of a DPO to other situations not foreseen in the GDPR.

In conclusion, the applicability of the GDPR and the functions of the DPO over the Spanish system shall have to be further assessed and, in that context, the Spanish data protection regime in force as a whole has to be revisited.