



# **SECOND EDITION THE DPO WHITE PAPER**



# DECEMBER 2025

Copyright: All rights reserved. You may download, store, use, or print the 2nd Edition of the DPO White Paper within the framework of the General Data Protection Regulation application by ISMS Forum, subject to the following conditions: (a) the guide may not be used for commercial purposes; (b) under no circumstances may the guide be modified or altered in any of its parts; (c) the guide may not be published without prior consent; and (d) the copyright notice must not be removed.

# AUTHORS

COORDINATION Carlos A. Saiz

REVIEW Javier Lomas

PARTICIPANTS Alberto Casaseca  
Alberto Ribes  
Araceli Fernández  
Aranzazu Herráez  
Esmeralda Saracibar  
Esther García  
Josep Bardallo  
María Jesús Casado  
Marta Cañas  
Óscar Antonio Sánchez  
Patricia Mendoza  
Pilar Pascual  
Rubén Cabezas  
Sonia Beulax

PROJECT MANAGEMENT Beatriz García

TRANSLATION Wasim Escribano

DESIGN/LAYOUT Lydia García

# CONTENTS

## CONTENTS

1. INTRODUCTION AND CURRENT CONTEXT	8
1.1. Evolution and Lessons Learned: Reasons for a Second Edition	8
1.2. Evolution and Lessons Learned: Reasons for a Second Edition	10
2. THE ROLE OF THE DATA PROTECTION OFFICER	12
2.1. Appointment of the Data Protection Officer	12
2.2. Tasks and Responsibilities of the Data Protection Officer	17
2.3. DPO Functions According to the AEPD Certification Scheme	19
3. ORGANIZATIONALS MODELS	21
3.1. Introduction	21
3.2. Type of Data Protection Officer: External, Internal, or Departamental DPO	24
3.2.1. External DPO	24
3.2.2. Departamental DPO (Collegiate Body or Committee	26
3.2.3. Internal DPO	27
3.3. Organizational Model	28
3.3.1. Model I: DPO and CISO	28
3.3.2. Model II: DPO and Compliance	30
3.3.3. Model III: DPO within the Legal Department	31
3.3.4. Modelo IV: Independent Area	32
4. RELATIONAL MODELS: REPORT AND RELATIONSHIP WITH THE REST OF THE ORGANIZATION	33
4.1. DPO Reporting	33
4.1.1. Purpose of Reporting	33
4.1.2. Reporting Frecuency	34
4.1.3. Reporting Methodologies	35
4.1.4. Factors Influencing the Choice or Reporting Methodology	40
4.1.5. Forms of Communicating the Report	41
4.1.6. Reporting Guidelines	45
4.1.7. Relationship with Other Areas of the Organization	46

4.1.8. Human Resources (HR)	46
4.1.9. IT Department (Information Technology)	46
4.1.10. CISO or Chief Information Security Officer	47
4.1.11. Marketing and Sales	47
4.1.12. Legal Department	47
4.1.13. Senior Management	48
5. PUBLIC SECTOR	49
5.1. Obligation to Appoint a DPO in the Public Sector	49
5.2. External DPO	50
5.3. Collegiate Body	50
5.4. Organizational Model	51
5.5. Data Protection and Information Security in the Public Sector: Towards a New Organizational and Relational Model	53
5.5.1.1. Responsabilidad compartida en materia de seguridad y protección de datos en el Sector Público	53
5.5.1.2. La comunicación electrónica entre entidades del Sector Público requiere de un trabajo colaborativo	54
5.5.1.3. Relación del DPO con otras áreas de responsabilidad en el Sector Público	55
5.6. Profile of the DPO in the Public Sector	59
6. PRIVACY GOVERNANCE	62
6.1. Duties and Responsibilities of Data Protection Governance	62
6.2. Data Protection Governance Model	64
6.2.1. Governance Layer	64
6.2.2. Supervision and Control Layer	64
6.2.3. Operational Layer	65
6.2.4. Personal Data Information Management System (PDIMS)	66
6.2.5. Integration with Others Compliance Functions	69
6.2.6. Continuous Training and Awareness	70

6.2.7. Promoting a Privacy Culture	70
6.3. Strategy Level – Political Data Protection	70
6.4. Organizational Level – Roles and Relationships	76
6.5. Practical Challenges of Data Protection Governance	79
7. MECHANISMS TO ENSURE INDEPENDENCE	84
7.1. Interference in the Performance of Duties	86
7.2. Practical Challenges to DPO Independence	86
7.2.1. The DPO's Rol in Safeguarding Corporate Sustainability	86
7.2.2. DPO Reporting and Hierarchical Independence	87
7.2.3. Conflict of Interest: A Constant Challenge	89
7.2.4. Resources and Training	90
7.2.5. Lack of Integration into Critical Processes	90
7.3. Mechanisms to Ensure DPO Independence	91
7.3.1. Reportar al más alto nivel de la organización	91
7.3.2. Separación de funciones	91
7.3.3. Recursos suficientes y autonomía presupuestaria	91
7.3.4. Participación activa en procesos de decisión	92
7.3.5. Políticas y transparencia	92
7.3.6. Comités de Privacidad	93
7.3.7. Auditorías independientes	93
7.3.8. Protección frente a despidos injustificados	93
7.4. Independence of the DPO and Decisions by Data Protection Authorities	94
7.4.1. Regulation of the DPO under the GDPR and LOPDGDD	95
7.4.2. Infringements Related to the DPO under the GDPR and LOPDGDD	95
7.4.3. Sanctioning Regimen under the GDPR and LOPDGDD	96
7.4.4. Decisions by Supervisory Authorities	96
7.4.4.1. Resoluciones de la AEPD	97
7.4.4.2. Resoluciones de otras autoridades de control europeas	97

8. THE DPO PROFILE	99
8.1. Legal Framework	99
8.2. Qualifications	100
8.3. Professional Experience	101
8.4. Personal Skills	101
8.5. Training	103
8.6. Duty of Confidentiality	103
9. THE DPO IN THE REGULATORY FRAMEWORK OF ARTIFICIAL INTELLIGENCE	108
9.1. Introduction	108
9.2. Defining the DPO's Role in Data Protection Law	109
9.3. Common Objectives of the Data Protection and Artificial Intelligence Regulatory Frameworks	109
9.4. GDPR and AI Act: Complementarity of the Legal Texts	110
9.5. Conclusions	117



# 1

## INTRODUCTION AND CURRENT CONTEXT

### 1.1. Evolution and Lessons Learned: Reasons for a Second Edition

More than five years have passed since the publication of the first edition of **The DPO White Paper**<sup>1</sup>, a period during which the role of the **Data Protection Officer (hereinafter, DPO)** has evolved and solidified its position within organizations. What was initially perceived as a new regulatory requirement has taken on a strategic dimension, becoming a key element in privacy management and regulatory compliance.

The context has changed not only from a regulatory or judicial standpoint. Digital transformation, the exponential growth of data volumes, and the emergence of artificial intelligence have redefined the challenges faced by the DPO. In this regard, the maturity of privacy programs and the growing need to integrate data protection into corporate governance models have also gained prominence.

Over the years, we have learned a great deal about the various organizational models for the DPO. From positioning within internal structures to outsourcing or forming collegiate teams, each organization has found its own path to ensure the effectiveness and independence of this function.

Moreover, decisions from data protection authorities and courts, both national and European, have begun to address key aspects affecting this role, offering interpretations that are redefining its place in privacy and data protection. Although still limited, these rulings are starting to more clearly define the boundaries and obligations of the DPO, providing guidance on independence, conflicts of interest, adequate resource allocation, the diligence required in fulfilling duties, and the risks associated with poor data protection management.

---

<sup>1</sup> [\*Libro Blanco del DPO – isms forum spain & data privacy institute\*](#)



One of the most significant milestones in this evolution has been the ***Certification Scheme for Data Protection Officers by the Spanish Data Protection Agency***<sup>2</sup> (hereinafter, AEPD-DPO Scheme), designed to help organizations select professionals whose competencies as DPOs have been certified by entities accredited by the **Spanish National Accreditation Body** (hereinafter, ENAC), thereby strengthening their professionalization and recognition within organizations. This step has enabled the establishment of clearer standards regarding their competencies and responsibilities, providing organizations with an objective criterion to assess the suitability of their DPOs and ensuring a higher level of qualification in the performance of their duties.

More recently, the entry into force of the **European Union regulation on Artificial Intelligence** (*Regulation laying down harmonized rules on artificial intelligence – RIA or Artificial Intelligence Act – AI Act*) has introduced new challenges in the management of personal data processing. The regulation sets specific criteria to ensure privacy in the use of AI, requiring greater oversight and additional compliance measures, further reinforcing the role of the DPO in this area.

In response to these developments, this second edition of the DPO White Paper is not merely an update of regulatory references or a review of what we already knew. **It is a reflective and practical guide on what we have begun to learn over these five years, the new challenges that have emerged, and the best practices that can help DPOs carry out their work successfully. And this is just the beginning.**

In this new edition, we don't only present the regulatory framework and the fundamental principles of the DPO's role but also incorporate practical experiences that have shaped the maturity of privacy governance models within organizations, both in the public and private sectors, consolidating the DPO as a key figure in the data protection ecosystem. This edition of the White Paper moves from the theoretical level to the organizational reality, where the DPO interacts with different lines of defense and where their positioning continues to be subject to analysis and evolution.

With this practical approach guiding the development of this guide, we have integrated tools and methodologies that help optimize DPO management. Notably, we include **a section dedicated to reporting methodologies, addressing the importance of Key Performance Indicators (KPIs) as an effective strategy to assess compliance levels, monitor the function, and provide senior management with key information for informed decision-making.** The consolidation of organizational models, the definition of roles, and the interaction of the DPO with other strategic areas of the organization are some of the aspects we have analyzed based on the experience of multiple entities.

Furthermore, in this edition we delve into the **mechanisms that ensure the independence of the DPO—not as an end itself, but as an essential means to guarantee that they can perform their duties effectively and without interference.** This analysis is reinforced by recent decisions from data protection authorities and European case law that have clarified the importance of preserving this independence, offering concrete examples of how it can be compromised and the consequences thereof.

**The role of the DPO is no longer unknown as it was five years ago. The experience gained has helped them to more clearly define their function and responsibilities.** However, the future presents new challenges. The emergence of artificial intelligence and its impact on personal data protection have opened a new scenario in which the DPO will be key to ensuring responsible development aligned with the principles of privacy and governance.

---

<sup>2</sup>[\*Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos\*](#)

The management of risks associated with AI, and the evolution of its regulation are shaping a field in which the role of the DPO will have increasing prominence.

With this update, the White Paper aims to provide a more comprehensive framework adapted to the current reality of the DPO. It highlights the evolution of the DPO over these years and emphasizes the importance of KPIs, organizational models, independence, and the impact of AI, thereby facilitating their work in an environment where privacy, data security, and regulatory compliance continue to evolve at a rapid pace.

We hope this publication will be a useful tool for all those who perform this role, as well as for those who work closely with them.

*“Privacy continues to evolve, and with it, the role of the DPO. It is time to keep learning and adapting to a constantly changing environment.”*

## 1.2. Regulatory Framework

The repealed Directive 95/46/EC referred to the figure of the DPO under the designation of “person in charge of personal data,” in relation to the exception of the obligation to notify files to the supervisory authority. This directive allowed Member States to incorporate this figure into their national legislation, although Spain did not adopt it, opting instead for the mandatory figure of the Security Officer, with different responsibilities and a distinct operational approach.

In fact, the first and unavoidable legislative reference to the DPO corresponds to **Regulation (EU) 2016/679 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 and on the free movement of such data (hereinafter “GDPR”)**, which regulates this role in **Section 4 of Chapter IV**, Articles 37, 38, and 39, along with **Recital 97**. While the GDPR did not invent the concept of the Data Protection Officer, it did impose new requirements at the EU level, establishing the conditions for their appointment, their powers, and their position within organizational structures.

At the national level, **Articles 34 to 37 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter, LOPDGDD)**, expand and refine what is established in the GDPR regarding this role, specifying aspects such as mandatory appointment scenarios and their relationship with public administration.

The evolution of the regulatory framework has been accompanied by key documents, such as the **WP243 Guidelines** from the **Article 29 Working Party** (hereinafter, **WP29**), which were later endorsed by its successor, the **European Data Protection Board (EDPB)**, in its first plenary meeting after its creation.

Before the GDPR came into force, the Article 29 Working Party (WP29) emphasized the role of what were then called **Data Protection Officers (DPOs)** as *“a cornerstone of accountability.”* Its **2017 Guidelines on DPOs** were later adopted by the European Data Protection Board (EDPB) after the GDPR came into effect, stating that these professionals would be *“the heart of the new legal framework for many organizations.”*

It is also essential to consider the guidelines, responses, opinions, and reports issued by the Spanish Data Protection Agency (AEPD), particularly **Report 164/2018**, which analyzes the incompatibility between the DPO and the Security Officer. Also noteworthy is the **coordinated action approved** by the EDPB in January 2023, focused on the designation and positioning of Data Protection Officers.

All of this constitutes a key reference that will be analyzed throughout this White Paper. While the GDPR and the LOPDGDD establish the core of the regulatory framework for the DPO, their scope of action is not limited to these regulations. In their daily work, other legal frameworks must also be considered, including:

- The **Law on Information Society Services and Electronic Commerce (LSSI)**.
- The **General Telecommunications Law (LGT)**, which transposes **Directive 2002/58/EC** (e-Privacy), currently under review to become a European regulation.
- **Directive (EU) 2016/1148** of the European Parliament and Council (NIS Directive), on the security of networks and information systems, which affects sectors where data protection is linked to cybersecurity

In addition, it is crucial to consider the **opinions, guidelines, and recommendations of the WP29 and the EDPB**, as well as the decisions and interpretative criteria of the **AEPD and regional data protection authorities**. **Judicial rulings** must also be considered, given the growing body of case law in the field of data protection.

Finally, we cannot overlook the impact of **international standards and regulations** on the DPO's role. In this regard, the work of the International Organization for Standardization (ISO) is key. The **ISO/IEC 27701:2021** provides guidelines on privacy management and the protection of personal information, enabling organizations to demonstrate regulatory compliance at a global level.

In the field of information security, it is also relevant to consider the studies and recommendations of specialized bodies such as:

- The **European Union Agency for Cybersecurity (ENISA)**.
- The **National Cryptologic Center (CCN-CERT)**.
- The **National Cybersecurity Institute (INCIBE)**.

All these elements form a dynamic and constantly evolving regulatory ecosystem that defines the DPO's framework of action and their role within organizations.

# 2

## THE ROLE OF THE DATA PROTECTION OFFICER

Currently, there seems to be no doubt that the role and function of the Data Protection Officer (DPO) is crucial for compliance with data protection regulations. Even before the GDPR came into force, the Article 29 Working Party described DPOs as **“a cornerstone of accountability”**; and the current European Data Protection Board (EDPB), following the implementation of the GDPR, stated that DPOs would be **“the heart of this new legal framework,”** recently affirming that we are at a point where, in light of the entry into force of numerous regulations related to the digital market (Digital Markets Act, Data Act, Digital Services Act, Artificial Intelligence Regulation, etc.), **“the role of DPOs appears to be changing,”** as they are increasingly being assigned new responsibilities related to artificial intelligence, ethics, data governance, and data spaces.

### 2.1. Appointment of the Data Protection Officer

Recital 97 of the GDPR states: **“In monitoring internal compliance with this Regulation, the controller or processor should be assisted by a person with expert knowledge of data protection law and practices if the processing is carried out by a public authority,** except for courts or other independent judicial authorities acting in their judicial capacity; if the processing is carried out in the private sector by a controller whose **core activities** consist of large-scale processing operations that require regular and systematic monitoring of data subjects; or if the core activities of the controller or processor consist of large-scale processing of special categories of personal data and data relating to criminal convictions and offenses. In the private sector, the core activities of a controller are related to its primary operations and not to the processing of personal data as ancillary activities. The level of expert knowledge required should be determined in particular based on the data processing operations carried out and **the protection required for the personal data processed by the controller or processor.**”

Such Data Protection Officers, whether or not they are employees of the controller, must be able to perform their duties and tasks independently.

**Article 37.1 of the GDPR** establishes three criteria for which the appointment of a Data Protection Officer (DPO) is considered mandatory:

**a.**

The processing is carried out by a public authority or body, except for courts acting in their judicial capacity.

**b.**

The core activities of the controller consist of processing operations which, by their nature, scope, and/or purposes, require regular and systematic monitoring of data subjects on a large scale.

**c.**

The core activities of the controller or processor consist of large-scale processing of special categories of personal data in accordance with Article 9 of the GDPR, and of personal data relating to criminal convictions and offenses as referred to in Article 10 of the GDPR.

The **WP29 Guidelines** introduced several clarifications regarding different aspects or concepts of these criteria<sup>3y4</sup>:

- The concept of **“core activity”** should be interpreted as inclusive of all activities that, while not identical to the corporate purpose, are inseparable from it. It excludes support activities which, although necessary for the fulfillment of the core activity, are not inseparable from it.
- **“Large scale”** cannot be quantified in general terms but must be assessed based on factors such as the number of data subjects affected, their proportion relative to the relevant population, the volume and variety of data, the duration or permanence of the processing, and its geographical scope.
- **“Regular and systematic monitoring”**: The term “regular” should be interpreted with one of the following meanings: continuous, occurring at specific intervals over a defined period, recurring or repeated at predetermined times, or taking place constantly or periodically. As for “systematic”, it should be understood as something that occurs according to a system or is carried out in a pre-established, organized, or methodical manner.

---

<sup>3</sup> [\*Esquema certificación aepd \(punto 7.2. y 7.1.\)\*](#);

<sup>4</sup> [\*Informe Jurídico 2023-0038\*](#);

Without prejudice to what is established in the GDPR, Article 34.1 of the LOPDGDD provides a detailed list of entities that are required to appoint a Data Protection Officer (DPO). With the sole intention of facilitating access to this list, we proceed to enumerate them below:

- a) Professional associations and their general councils.
- b) Educational institutions offering instruction at any level established by legislation governing the right to education, as well as public and private universities.
- c) Entities that operate networks and provide electronic communications services in accordance with specific legislation, when they regularly and systematically process personal data on a large scale.
- d) Providers of information society services that carry out large-scale profiling of service users.
- e) Entities covered by Article 1 of Law 10/2014, of June 26, on the regulation, supervision, and solvency of credit institutions.
- f) Credit financial establishments.
- g) Insurance and reinsurance companies.
- h) Investment service companies regulated by securities market legislation.
- i) Distributors and marketers of electricity and distributors and marketers of natural gas.
- j) Entities responsible for common files for assessing financial solvency and creditworthiness or for managing and preventing fraud, including those responsible for files regulated by legislation on the prevention of money laundering and terrorist financing.
- k) Entities engaged in advertising and commercial prospecting activities, including market and commercial research, when they carry out processing based on data subjects' preferences or engage in profiling activities.
- l) Healthcare centers legally required to maintain patients' medical records. Health professionals practicing individually are excluded.
- m) Entities whose purpose includes issuing commercial reports that may refer to natural persons.
- n) Operators engaged in gambling activities through electronic, computer, telematic, or interactive channels, in accordance with gambling regulations.
- ñ) Private security companies.
- o) Sports federations when processing data of minors.



Without prejudice to what is established in the GDPR, Article 34.2 of the LOPDGDD refers to the possibility of **voluntarily appointing a Data Protection Officer (DPO)**, which in many cases may be advisable, at least for the following reasons:

- The **graduation of sanctions** based on the existence of a DPO within the organization, even when not mandatory (Article 76.h LOPDGDD).
- The **involvement of the DPO in resolving complaints**, both those submitted directly by citizens—when they choose this route before filing a complaint with the AEPD—and those that the AEPD decides to forward to the DPO prior to initiating a sanctioning procedure. In general, if the DPO manages to resolve the complaint, and without prejudice to the data subject later contacting the AEPD, no sanctioning procedure would be initiated (Article 37 LOPDGDD).
- The **greater assurance for the organization in terms of privacy compliance**, derived from having a specifically designated and regulated role within the organization dedicated to this activity.

Recently, the **European Data Protection Board (EDPB)** itself has stated that both controllers and processors may choose to appoint a DPO voluntarily. Having a data protection expert is extremely useful in the planning and decision-making processes of any company, as they assist with compliance with data protection regulations—especially with the principles of accountability, data protection by design and by default, and the obligation to implement appropriate technical and organizational measures to comply with the GDPR, among many others.

Furthermore, the **DPO must be appointed in accordance with Article 37.5 of the GDPR**, based on their professional qualities and, in particular, their expert knowledge of data protection law and practices, as well as their ability to perform the tasks referred to in Article 39 of the GDPR. The DPO may be internal or external (Article 37.6 GDPR). Additionally, Article 37.2 of the GDPR allows a group of undertakings to appoint a single DPO, provided that this officer is “easily accessible from each establishment.”

Regarding the procedure for appointment, designation, and dismissal, **Article 34.3 of the LOPDGDD** establishes that controllers and processors must notify the Spanish Data Protection Agency (AEPD) or, where applicable, the regional data protection authorities, within ten days. This obligation applies whether the appointment is mandatory or voluntary. Likewise, they must publish the DPO’s contact details and communicate them to the supervisory authority (Article 37.7 GDPR).

## 2.2. Tasks and Responsibilities of the Data Protection Officer

The tasks of the DPO, as established in **Article 39 of the GDPR**, include at minimum the following:

a.

**Inform and advise** the controller or the processor and the employees who carry out processing of their obligations under this Regulation and other Union or Member State data protection provisions.

b.

**Monitor compliance** with this Regulation, with other Union or Member State data protection provisions, and with the policies of the controller or processor regarding the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

c.

**Provide advice**, when requested, regarding data protection impact assessments and monitor their implementation in accordance with Article 35.

d.

**Cooperate** with the supervisory authority.

e.

**Act as a contact point for the supervisory authority** on issues related to processing, including the prior consultation referred to in Article 36, and consult, where appropriate, on any other matter.

Recently, the Spanish Data Protection Agency had the opportunity to comment, in **Legal Report 0038/2023**, on a series of extremely interesting issues relating to the functions of the DPO, **distinguishing between “decision-making” functions** (which correspond to the data controller) **and “advisory or supervisory” functions** (which correspond to the DPO), clarifying the following<sup>5y6</sup>:


- The DPO acts as an internal advisor and supervisor, and therefore **the position cannot be held by individuals** who also perform tasks involving decisions about whether data processing should occur or how it should be carried out (e.g., IT managers or information security officers).

<sup>5</sup> [Esquema certificación aepd \(punto 7.2. y 7.1.\)](#);

<sup>6</sup> [Informe Jurídico 2023-0038](#);

- The list of functions in Article 39 of the GDPR is a **minimum list**, and other functions may be assigned to the DPO, such as keeping a record of processing activities; however, this must always be done while **respecting the advisory and supervisory nature of the DPO**, without implying direct intervention in decision-making regarding the purposes and means of processing, which would affect their independence and imply the existence of a conflict of interest.
- The DPO acts as an internal advisor and supervisor, **so this position cannot be held by individuals who also have tasks that involve decisions about the existence of data processing or how data will be processed** (e.g., ITC managers or information security managers).
- The DPO primarily assumes advisory and supervisory functions for the benefit of the controller or processor. However, as clearly stated in various provisions of the GDPR, **the controller remains fully legally responsible for any failures in this regard, and under no circumstances does this responsibility fall on the DPO**.
- The DPO must provide the controller or processor with all documentation resulting from the exercise of their functions. While the DPO's recommendations are not binding, it is advisable for the controller to document the reasons or rationale for deviating from the DPO's advice.
- There must be a clear separation between the DPO's advisory and supervisory functions and the management or governance functions related to privacy and data protection (which fall under the responsibility of the controller or processor). **These management functions may be assigned to a separate "Privacy and Data Protection Officer", distinct from the DPO role.**

The Spanish Data Protection Agency (AEPD), in the aforementioned report, also refers to the DPO's role in prior consultation with the supervisory authority, stating: *"The function of consulting the supervisory authority falls within the **DPO's own responsibilities, protected by their functional independence, which means they cannot receive instructions regarding its execution.** Thus, the controller or processor may request the DPO's advice, and if the DPO deems it appropriate, they may initiate consultation with the supervisory authority, but without receiving instructions on how to proceed."*



Finally, it is important to remember that the DPO assumes advisory, supervisory, and collaborative functions with the supervisory authority, whether these are assigned by the GDPR itself or voluntarily by the controller or processor. As noted by the AEPD, the DPO is expected to play a fundamental role in the new model of proactive accountability. To do so, they must act independently and with a clear focus on the risks associated with personal data processing, considering the nature, scope, context, and purposes of such processing, in accordance with Article 39.2 of the GDPR.

## 2.3. DPO Functions According to the AEPD Certification Scheme

According to **Section 7.2 of the Scheme**, the general functions of the DPO can be specified as advisory and supervisory tasks, among others, in the following areas:

1. Ensuring compliance with data processing principles, such as purpose limitation, data minimization, and accuracy.
2. Identifying the legal bases for data processing.
3. Assessing the compatibility of purposes different from those for which the data were originally collected.
4. Determining the existence of sector-specific regulations that may establish specific processing conditions different from those set by general data protection legislation.
5. Designing and implementing information measures for data subjects.
6. Establishing procedures for receiving and managing data subject rights requests.
7. Evaluating data subject rights requests.
8. Managing the engagement of data processors, including the content of contracts or legal instruments governing the controller-processor relationship.
9. Identifying appropriate instruments for international data transfers based on the organization's needs and characteristics, and the justification for such transfers.
10. Designing and implementing data protection policies.
11. Conducting data protection audits.
12. Establishing and managing records of processing activities.
13. Performing risk analyses of processing operations.
14. Implementing data protection by design and by default measures appropriate to the risks and nature of the processing.
15. Implementing security measures appropriate to the risks and nature of the processing.
16. Establishing procedures for managing data breaches, including risk assessment for the rights and freedoms of data subjects and notification procedures to supervisory authorities and affected individuals.

- 17. Determining the need for data protection impact assessments.
- 18. Conducting data protection impact assessments.
- 19. Managing relationships with supervisory authorities.
- 20. Implementing training and awareness programs for staff on data protection.

To carry out these tasks, according to Section 7.1 of the Scheme, the DPO must be able to:

- a) Gather the necessary information to determine processing activities.
- b) Analyze and verify the compliance of processing activities with applicable regulations.
- c) Inform, advise, and issue recommendations to the controller or processor.
- d) Collect information to monitor the record of processing operations.
- e) Advise on the application of data protection by design and by default.
- f) Advise on:
  - Whether a data protection impact assessment should be conducted and which areas or processing operations should be subject to internal or external audit.
  - The methodology to follow when conducting a data protection impact assessment.
  - Whether the impact assessment should be carried out internally or outsourced.
  - What safeguards (including technical and organizational measures) should be applied to mitigate any risks to the rights and interests of data subjects.
  - Whether the data protection impact assessment has been properly conducted.
  - Whether its conclusions (whether to proceed with the processing and what safeguards to apply) comply with the GDPR.
- g) Prioritize activities and focus efforts on issues presenting the greatest data protection risks.
- h) Advise on what internal training activities should be provided to staff and managers responsible for data processing, and which processing operations require more time and resources.
- i) Intervene in case of complaints before data protection authorities.

# 3 ORGANIZATIONAL MODELS

## 3.1. Introduction

Since there is no specific regulation governing this aspect, organizations have implemented various organizational and relational models for the DPO, based on diverse and internal criteria, as reflected in the results of the latest **Study on the Level of Maturity and Compliance with the GDPR in Spain\***.

The organizational and relational model regarding the DPO's position within the organization has a significant impact, as it largely determines whether the DPO can adequately fulfill their duties in accordance with the requirements set out in Section 4 of the GDPR. This includes timely and appropriate involvement in all matters related to data protection, having sufficient resources and access to personal data and processing operations, acting independently, avoiding conflicts of interest, and reporting to the highest hierarchical level of the organization.

This section will review the most common models in terms of:

- **Type of DPO:** Internal, External, or Departmental Team.
- **Organizational Models:** Position within the organizational chart.
- **Relational Model:** Reporting and relationship with the rest of the organization.

The GDPR does not regulate, nor even recommend, how public and private entities should or may structure their Organizational and Relational Model regarding the DPO. This grants flexibility to any entity in choosing its model, within its organizational freedom or public service framework, which may vary from one entity to another and will largely be determined by the following characteristics:

- The size of the organization and the type of activities, processes, products, and services

---

*\* Estudio sobre el Nivel de Madurez y Cumplimiento del RGPD en España.*

- Type of processing activities carried out by the entity.
- The prominence of new technologies and innovation in its activities.
- Geographic and cross-border locations (local, European, or multinational)ponderancia en sus actividades de las nuevas tecnologías y de la innovación.
- The complexity of processes and their interactions.

In this regard, the **Spanish Data Protection Agency (AEPD)**, in its **Legal Report 38/2023**, has determined that the structuring of the DPO is an organizational matter that can be freely adopted by any entity—provided it aligns with the advisory and supervisory nature of the DPO’s functions. The only limitation is that the DPO’s position within the organization must meet all the requirements established in Article 38 of the GDPR:

**1.** Participate in a timely and appropriate manner in all matters related to personal data protection.

**2.** Having the necessary resources to perform their duties.

**3.** Perform their duties independently.

**4.** Not being dismissed or penalized for performing their duties.

**5.** Report to the highest hierarchical level of the organization.



***“Organizations should expect increased scrutiny and investigation by the AEPD in the coming years regarding the position of the DPO.”***

For this reason, it is recommended to consider the needs and capabilities of each entity when choosing the model that best suits it, with the aim of ensuring that the DPO function is properly embedded within the organization. Once all these aspects are clearly defined, entities should explicitly specify the most important elements of the DPO’s Organizational and Relational Model within their internal procedures—preferably through an Internal DPO Regulation or a service provision contract, in the case of an external DPO:

- Type of DPO
- Appropriate location and position within the organization
- Reporting level to senior management, procedures, and communication channels
- Operational procedures for interaction with other areas of the company
- Privacy governance model, identifying the different roles and responsibilities in data protection matters

In the same vein, the **European Data Protection Board** has established a series of **recommendations and key considerations** regarding the DPO role—applicable to both public and private sectors—which organizations should consider regardless of their organizational and relational model:

- Adopt standards, internal policies, and best practices that demonstrate compliance with the DPO’s obligations under the chosen model.
- Clearly assign internal functions, particularly ensuring the DPO is not tasked with responsibilities involving decisions about the existence of data processing or how data is processed, as this would compromise their functional independence.
- Promote the DPO’s role within the organization and ensure their involvement in all matters related to personal data protection.
- Document the analysis regarding the designation or non-designation of a DPO, especially if the conclusion is that appointment is not mandatory.
- Verify the resources made available to the DPO, analyzing on a case-by-case basis what resources are necessary—such as the number of data subjects whose data is being processed by the organization.
- Encourage ongoing training for DPOs so they can keep their knowledge up to date and stay informed about the latest developments (e.g., digital or AI regulations).

---

<sup>7</sup> [\*Coordinated Enforcement Action, Designation and Position of Data Protection Officers\*](#)

- Ensure that the DPO is able to fulfill the tasks assigned under the GDPR.
- Justify that the DPO does not assume responsibilities that could lead to a potential conflict of interest, nor is their independence compromised—especially when they perform other functions within the organization.



This section presents various reflections on the different types of DPOs, as well as the relational model of the role within the organization. All of this is approached with respect for the different models that exist across organizations, and with the understanding that there is no perfect or pure alignment between the regulatory requirements of the role and the widely adopted “three lines of defense” model present in many organizations.

## 3.2. Type of Data Protection Officer: External, Internal, or Departmental DPO

### 3.2.1. External DPO

**Article 37 of the GDPR** allows for the appointment of an external DPO, as part of a service provision contract with a natural or legal person. This is a residual option and is declining, as observed in the latest Study on the **Level of Maturity and Compliance with the GDPR in Spain**, with fewer than 3% of cases.

According to the Guidelines on DPOs from the Article 29 Working Party (now EDPB), this option allows the DPO tasks to be carried out by a team from the service provider. However, in such cases, all team members must meet the requirements to perform DPO functions. Additionally, a designated primary contact must be appointed to fulfill the DPO accessibility requirement.

This type of arrangement requires, as previously mentioned, **a service provision contract**. To avoid conflicts of interest, prevent gaps in the scope of responsibilities, and ensure compliance with the requirements outlined above, it is recommended that the contract includes at least:

- A detailed description of the tasks assigned to the external DPO team.
- Responsibilities of the organization itself, both in those tasks and in any that may be assumed internally.
- Designation of the primary contact person and the project manager for coordination with the organization.
- And of course, a Data Processing Agreement, since the DPO team will access personal data as a processor, under the responsibility of the client.

As stated by the EDPB in its **January 2024 Report** on the designation and position of the DPO, controllers and processors must carefully verify that the DPO has sufficient resources to adequately perform their duties. In some cases, when an external DPO is employed, this may require controllers and processors to check how many clients that DPO has, to ensure they have enough time and capacity to meet the relevant obligations under the GDPR.

The decision to hire an external DPO service largely depends on the company's data governance and privacy management strategy, as well as its size and ability to internally appoint someone with the appropriate profile to assume the role.

This model is probably not the most suitable for **large organizations** that have the capacity to establish dedicated Data Protection areas and appoint a properly trained DPO. An internal DPO will find it easier to understand the organization, its sector, and to participate effectively in its day-to-day operations—something that may be essential in organizations with numerous, varied, and constantly evolving personal data processing activities. On the other hand, **in smaller organizations**, outsourcing may be appropriate due to the inability to internally appoint a suitable DPO.

## PROS

- Reduced structural costs by outsourcing the function and the ability to allocate resources based on specific needs through the service contract.
- Access to professionals with extensive knowledge across all necessary areas of Data Protection.
- Lower risk of conflicts of interest compared to other roles within the company.

## CONS

- Limited knowledge of the organization and its sector.
- Difficulty in participating in all activities related to the organization's data processing, especially when these are numerous and complex.
- Risk of insufficient resources from the provider if they manage too many clients.

### 3.2.2. Departmental DPO (Collegiate Body or Committee)

According to the previously mentioned survey, a significant percentage of organizations have opted to create working teams to assume the functions of the DPO, representing 30% of the cases. However, this option is declining in favor of appointing a dedicated internal DPO.

Although neither the GDPR nor the Spanish Data Protection Law (LOPDGDD) provides a clear indication against appointing a multi-person body as a DPO, the Spanish Data Protection Agency (AEPD) includes in its Guide for Communicating the DPO some instructions on how to report a collegiate body or working group as such. Nevertheless, reasonable doubts arise in this area, as the wording of the legislation seems to be oriented toward a natural person rather than a multi-person body—especially considering that this possibility is specifically established for the case of an external DPO. Furthermore, the Guidelines from the Article 29 Working Party (now EDPB), when providing guidance for working group cases, refer exclusively to external DPOs.

In any case, given the lack of clear indications to the contrary, if this solution is chosen, the guidelines provided by the Article 29 Working Party for external DPOs appear to be an essential starting point for an interdepartmental team, where applicable: en el caso de un equipo interdepartamental en lo que aplica:

- **All members must meet the requirements to serve as a DPO.**
- **Clearly specify the tasks assigned to each team member.**
- **Define a single point of contact, both for the organization and for data subjects.**
- **Appoint a single person as the reporting contact with the Data Controller.**

This model is based on cross-functional collaboration within the organization and can offer significant advantages in organizations that are already mature in this type of structure, provided that the appropriate areas are properly represented. It is a model that extends the interdepartmental approach used in security management—based on committees or commissions with operational authority, which already exist in many organizations—to the realm of privacy.

## PROS

- Ensures cross-functional collaboration throughout the organization if committee members are properly selected.
- Guarantees that the body possesses all the knowledge and skills required of a DPO.
- **Resource Optimization:** Each department contributes to specific resources—both technical and human—that can be optimized in privacy management. This collaboration reduces the burden on the DPO and allows the organization to better manage its resources in terms of privacy and security.
- **Improved Risk Identification and Management:** Each department handles data with varying levels of sensitivity and different processes, so having representatives from each allows for the detection of specific risks and the adoption of appropriate preventive measures for each context.

## CONS

- Certain DPO functions are personal and require a very clear assignment of responsibilities within the committee.
- There is a higher likelihood of conflicts of interest, as each represented area brings its own; although managing these is easier due to the need for joint decision-making.
- **Challenges in Accountability:** With multiple individuals responsible for data protection matters, clarity over who makes final decisions or is accountable for specific areas may be diluted. This can lead to a lack of responsibility in cases of non-compliance or incidents.

### 3.2.3. Internal DPO

According to the **Study on the Level of Maturity and Compliance** with the GDPR in Spain, this is the most **widely adopted solution (over 55%)**, either as a newly defined exclusive role or as a new responsibility assigned to existing functions and/or departments within the organization.

## PROS

- An internal DPO is familiar with the organization's structure, culture, processes, and systems, which facilitates the identification of specific risks and the implementation of context-adapted measures. Being part of the organization, the internal DPO is always accessible to respond to questions, incidents, or training needs, enabling agile and continuous privacy management.

## CONS

- The internal DPO faces the challenge of needing to engage in continuous training to stay up to date with regulations and privacy practices, which can be demanding in terms of resources.

## 3.3. Organizational Model

### 3.3.1. Model I: DPO and CISO

Based on the pre-GDPR model in which there was no equivalent figure to the DPO in Spain—but there was an obligation to appoint a Security Officer—many companies have opted to assign this role to the CISO. However, assigning both functions to the same person can present challenges, particularly regarding **potential conflicts of interest**, depending on the type of CISO within the organization.

This combination of roles is not uncommon today. In fact, according to the latest Study on the Level of Maturity in the Application of the GDPR (February 2024), **21% of surveyed DPOs also hold the position of CISO**. In many organizations, this model offers significant synergies from an operational, cultural, and people management perspective.

In its document “**2023 Coordinated Enforcement Action. Designation and Position of Data Protection Officers<sup>8</sup>**”, the EDPB emphasizes the issue of multitasking DPOs, noting that a significant percentage of DPOs hold additional roles within their organizations, which may lead to conflicts of interest. Only 45.82% of DPOs work full-time in their role, while 33.97% are shared across multiple organizations. Moreover, many DPOs are involved in activities that may conflict with their primary role, compromising their independence.

The role of the CISO is not generally regulated by law, although more recent cybersecurity regulations do include the role of a Security Officer for critical infrastructure environments, important and essential entities, etc. (e.g., the NIS2 Directive). Organizations therefore exercise their business freedom to establish a cybersecurity governance model, which varies widely and results in many different scenarios. Some CISOs focus on operations and mitigating technological risks, others have a more strategic role in policy definition; some are closely tied to business operations, while others focus on control and oversight. Some work in highly regulated environments under supervisory authority, while others operate in less regulated markets. Some have large teams with diverse profiles, while in other cases, the department consists solely of the CISO.

For all these reasons, **each organization must assess the coherence and alignment with the principles mentioned above when deciding whether to assign the roles of DPO and CISO to the same person or function.**

---

<sup>8</sup> [2023 Coordinated Enforcement Action. Designation and Position of Data Protection Officers](#)

The DPO must be involved from the outset in assessing the lawfulness and proportionality of data processing activities, even before technological solutions are defined. This is a key point in protecting the fundamental rights of data subjects, and it may fall outside the scope of a CISO whose role is focused exclusively on security measures.

Both the AEPD in 2018 and the Catalan Data Protection Authority (APDCAT) in 2024 have expressed **similar** views regarding the overlap of DPO and CISO functions in the same individual. **The AEPD emphasizes that data protection is a fundamental right, whereas information security is a corporate obligation aimed at ensuring an adequate level of protection.** Therefore, **a clear separation between the two roles must exist.** However, the AEPD acknowledges that, exceptionally, in small organizations or those with limited resources, it may be permissible for one person to assume both roles, provided that a series of key requirements are met.

These requirements include ensuring the DPO's independence, avoiding conflicts of interest, and establishing clear organizational mechanisms to separate responsibilities. Additionally, the individual must meet the training and qualification requirements set out in the GDPR. Both the AEPD and APDCAT agree on the need to guarantee the DPO's independence, especially when they perform other functions within the organization, such as that of a security officer. The AEPD highlights that, in exceptional cases where one person holds both roles, it is essential to adopt "all necessary organizational measures," which must be "properly reflected in the information security policy," to ensure there are no conflicts of interest and that the DPO maintains their independence.

For its part, **APDCAT reinforces this idea by stating that the DPO's appointment must be "properly documented" and that the measures to guarantee their independence must be clearly reflected in the organization's security policy.** Moreover, APDCAT goes a step further by recommending the adoption of specific internal measures, such as explicitly defining roles that are incompatible with that of the DPO, to prevent potential conflicts of interest.

Both authorities emphasize the need for an organizational structure that ensures the DPO can perform their duties without interference or conflicts with other responsibilities that may compromise their autonomy.

The AEPD and APDCAT both agree that **combining the roles of DPO and CISO should be an exceptional measure**, subject to case-by-case evaluation.

The AEPD stresses that, in cases where it is not possible to maintain a separation between the two functions, it is essential to document the DPO's appointment, detailing the reasons why separation is not feasible, and the measures adopted to ensure their independence. These may include the use of separate email addresses, budgets, resources, and reporting lines.



### 3.3.2. Model II: DPO and Compliance

A significant number of companies have identified synergies between the roles of Compliance Officer and DPO, as both positions aim to ensure regulatory compliance within the organization—whether in data protection or other legal areas.

Since the implementation of the GDPR, this model has evolved notably. Many organizations have found benefits in integrating data protection into their broader compliance programs. This trend has been observed in studies highlighting increased adoption of this model, especially among small and medium-sized enterprises (SMEs) that lack sufficient resources to maintain these functions separately. Furthermore, both data protection and compliance have adopted a risk-based approach, which facilitates the integration of these roles.

However, several aspects must be considered when implementing this model:

- **Differentiation of Approaches:** The Compliance Officer focuses on managing risks that affect the organization from a regulatory standpoint, while the DPO is concerned with protecting the rights and freedoms of data subjects in relation to data processing. Therefore, specialization in each role is crucial to avoid potential conflicts of interest and ensure effective oversight.
- **Adequate Training:** It is essential that the individual responsible for both functions has appropriate training in both areas, including regulatory, technical, and legal aspects.
- **Organizational Placement:** This model may allow the DPO to benefit from the organizational structure of the Compliance Officer, who typically reports directly to senior management. This connection can not only support the DPO's independence but also enhance their visibility within the organization, promoting greater integration of their functions.
- **Risk Alignment:** This model is particularly suitable for organizations where data protection risks are closely tied to business processes. Integrating both roles can be effective if risk assessment is prioritized based on business activities and data processing operations.



However, **the Belgian Data Protection Authority (APD), in its substantive Decision 18/2020, warns that combining these roles is only appropriate if strong measures are implemented to manage conflicts of interest.** Otherwise, as occurred in the case analyzed, the lack of segregation between the responsibilities of the DPO and other departments can lead to situations of self-control and lack of objectivity in the supervision of personal data processing.

Organizations must conduct a thorough analysis of the compatibility between the roles of Data Protection Officer (DPO) and Compliance Officer, clearly defining the scope and responsibilities of each role. It is crucial to prepare a report detailing how potential conflicts of interest will be managed and documented. This may include establishing specific policies to prevent conflicts, implementing a rigorous selection and training process for candidates, and creating communication mechanisms to identify any links that could compromise impartiality in the performance of their duties.

### 3.3.3. Model III: DPO within the Legal Department

Another common position is to assign the role of Data Protection Officer to a member of the Legal Department. However, in recent years, there has been a growing trend toward not combining the DPO role with other functions, with nearly half of DPOs (46.81%) now dedicated exclusively to their duties. Still, a significant percentage (17.02%) continue to hold additional responsibilities within the legal area.

The synergies in legal knowledge related to data protection are evident, particularly in the advisory function, provided this does not create a conflict of interest. For example, a conflict may arise if the DPO holds an executive role within the organization that involves making decisions about the purposes and means of personal data processing. In such cases, the DPO would be required to evaluate, examine, and potentially criticize the processing independently. Likewise, if the DPO performs an executive function, they cannot supervise compliance with data protection regulations, as self-monitoring contradicts the DPO's independent role in ensuring compliance within the organization.

Another potential conflict of interest may arise when the DPO, either directly or as a member of the legal department, represents the controller or processor before the courts in matters related to data protection. This conflict is mentioned by the Article 29 Working Party in its guidelines, although only in the case of external DPOs. A similar issue may occur when representing the controller or processor before the supervisory authority in matters beyond the duty to cooperate—such as in defense proceedings. The AEPD has addressed this, stating that submitting arguments on behalf of the data controller constitutes a function that goes beyond internal advisory, involving active defense and a declaration of position in a sanctioning procedure. This may compromise the DPO's independence and create a conflict of interest.

In any case, determining whether a conflict of interest exists must be done on a case-by-case basis, based on an assessment of all relevant circumstances—particularly the organizational structure of the controller or processor and in light of all applicable regulations, including any internal policies. To this end, **it is advisable for organizations to define the DPO's functions in a way that allows them to act independently and avoid potential conflicts of interest.** This could be done, for example, through a DPO Charter approved by senior management or an "engagement letter." The list of DPO functions is not exhaustive, so there is nothing preventing the DPO from assuming other roles, such as legal advisor, as long as the controller or processor ensures that these functions do not create a conflict of interest.

### 3.3.4. Model IV: Independent Area

Regardless of its hierarchical placement within the organization, the trend from previous years continues, with **nearly 50% of DPOs identified as belonging to an independent area within the organization.**

This model allows the organization to define the DPO's position from the outset, as well as the way in which their functions are carried out. However, its effectiveness in meeting the requirements for performing these functions also depends heavily on the hierarchical dependency and the level of reporting defined for the role.

In principle, this model does not present conflicts of interest, but it requires the organization to have the capacity to establish a dedicated area with sufficient resources and capabilities for the DPO.

# 4

## RELATIONAL MODELS: REPORTING AND RELATIONSHIP WITH THE REST OF THE

### 4.1. DPO Reporting

*“Reporting by the DPO to the highest hierarchical level is a key element to ensure that the organization’s strategic decisions regarding data protection are made based on a proper understanding of the risks.”*

Likewise, it must be noted that direct reporting by the DPO to the highest hierarchical level of the controller or processor is a **legal requirement established in Article 38.3 of the GDPR, and therefore**, this task must be facilitated for the DPO.

To ensure effective reporting, certain principles must be followed, and the structure must allow for a clear understanding of the situation during each reporting period, the challenges faced, and the actions to be taken by the organization. **It is not only important what is reported, but also how the report is presented**, as the format and clarity of the information can determine how effectively senior management understands and acts upon the risks and recommendations presented by the DPO.

#### 4.1.1. Purpose of Reporting

The main objective of the DPO’s report should be to provide senior management with a comprehensive view of the organization’s data protection compliance status, identified risks, necessary corrective measures, and areas requiring greater attention. This enables management to assess the maturity level of the data protection management system and make informed decisions on key issues such as resource allocation and risk management.

The DPO’s report should fulfill several key purposes:

- Ensure that senior management is aware of the **organization’s level of compliance** with data protection legislation, or any other sector-specific legislation impacting data protection, depending on the environments and countries in which the company operates. Management should be informed

not only of compliance levels but also of goal achievement and any deviations, both quantitatively and qualitatively.

- Advise senior management on the most relevant **risks associated with the organization's personal data processing activities**. These risks may include potential data breaches, failures in internal controls, or risks arising from technological processes that could affect the rights and freedoms of data subjects—whether employees, customers, users, or any other third party whose personal data is processed by the organization.
- **Report any personal data breaches that occurred during the reporting period, including their impact on affected individuals, actions taken to mitigate the consequences, and corrective measures needed to prevent similar future incidents.**
- Go beyond reporting the current status; the DPO should be able to present **strategic recommendations to improve compliance and minimize risks**. However, it is ultimately the controller who must make executive decisions regarding data protection. The DPO cannot and should not make decisions on behalf of the controller, as this would constitute a clear conflict of interest.

### 4.1.2. Reporting Frequency

The frequency with which the DPO reports to senior management will depend on several factors, such as the size of the organization, the complexity of personal data processing, the sector in which it operates, and the level of risk involved. Generally, **periodic reporting is recommended, with a minimum frequency of once per year**. However, in contexts where personal data processing is central to the company's activities, more frequent reporting may be necessary—semi-annually or even quarterly. In organizations with high volumes of personal data or operating in high-risk sectors such as finance or healthcare, more frequent reporting may be required to keep senior management continuously informed of data protection risks. In less exposed sectors or smaller companies, reporting may be less frequent but should still occur at least annually to ensure management is aware of the data protection status.

In addition to periodic reports, the DPO must be prepared to deliver **ad hoc reports when significant events occur, such as serious data breaches or regulatory changes** that require immediate organizational response (e.g., new guidelines issued by the European Data Protection Board or any Supervisory Authority).

### 4.1.3. Reporting Methodologies

The DPO may adopt various models to structure their reports, depending on the organization's needs and the type of information most relevant to senior management. Among the different reporting methodologies, the DPO should choose the one that best suits the information needs and organizational characteristics, ensuring clear and effective communication that supports informed decision-making. Factors such as the complexity of personal data processing, reporting frequency, and the level of detail required by senior management should be considered when selecting the appropriate model. The most common models include:

#### i. KPI-Based Reporting

**A KPI-based model provides senior management with a quantitative view of the data protection status.** KPIs allow for performance measurement of the data protection management system over time and offer a clear view of progress or setbacks in key areas. It is essential that KPIs go beyond absolute figures and include comparisons with previous periods to identify trends, goal achievement, deviations, etc. **Appendix 1 outlines some of the most useful KPIs a DPO can apply to measure organizational compliance.**



This model is recommended for smaller organizations or those with less complex data processing, or when senior management prefers a quick and precise overview of key compliance areas. It is particularly useful in low-risk environments where numerical indicators provide sufficient insight.

#### PROS

- KPIs provide quantitative data that enable objective evaluation of the data protection system's performance.
- They facilitate tracking of progress or setbacks over time, helping identify trends and areas for improvement.
- They offer a solid foundation for strategic decision-making, based on concrete and verifiable metrics.

#### CONS

- KPIs may not provide enough context about the underlying causes of deviations or goal achievement, potentially leading to misinterpretations.
- They may focus too heavily on quantitative aspects, overlooking important qualitative factors that also affect data protection.
- Collecting and analyzing KPI data may require significant resources in terms of time and technology.

## ii. Risk-Based Reporting

In this model, the DPO structures the report around identified risks, prioritizing those that pose the most immediate or significant threats—both from a corporate perspective and in relation to the rights and freedoms of data subjects. Senior management often focuses on risks with significant organizational impact, rather than those affecting individuals. However, **the DPO must clearly communicate that risks severely affecting data subjects' rights and freedoms—such as identity theft or misuse of sensitive data—can lead to administrative sanctions by supervisory authorities**, as well as legal actions and claims for damages by affected individuals.

A clear and well-explained presentation of the risks faced by the organization is essential for senior management to fully understand their magnitude and potential consequences, enabling more effective mitigation measures and informed decisions that protect both the organization and the data subjects.



**This type of reporting is recommended in high-risk sectors or where personal data processing may significantly impact individuals' rights and freedoms.**

For example, in organizations handling sensitive data such as those in the healthcare sector, this model prioritizes critical risks, allowing senior management to focus on the most urgent threats.

### PROS

- Enables senior management to focus on the most critical risks and make informed decisions to mitigate them.
- Provides a clear and structured view of risks, their impacts, and mitigation measures.

### CONS

- Senior management may feel overwhelmed by the detailed information on each risk.
- By focusing on specific risks, a broader view of the overall data protection status may be lost.



### iii. Compliance Section-Based Reporting

A reporting methodology focused on compliance sections is based on the systematic review and evaluation of key regulatory areas that the organization must comply with in terms of data protection. This type of report emphasizes the organization's level of compliance with specific points of the GDPR and other sector-specific regulations.



**It is ideal for large organizations with complex data protection processes, where senior management requires a comprehensive and detailed view of each area of the compliance program.**

For example, in a multinational company managing large volumes of customer data, this model allows for a thorough evaluation broken down by compliance areas.

The first step in structuring a compliance section-based report is to identify the key areas to be reviewed. The report is organized into sections, each covering one of the identified compliance areas.

Each section may be structured as follows:

1.

**Description of the Compliance Area:** A brief explanation of the legal obligations the organization must meet in that specific area. For example, in the section "Transparency and Data Subject Rights," a summary of the obligations derived from Articles 12 to 22 of the GDPR is included.

2.

**Compliance Status:** This part of the report should assess the current level of compliance. The DPO may use a rating system (compliant, partially compliant, non-compliant) or a percentage scale to indicate the degree of conformity in each area.

3.

**Required Corrective Actions:** If non-compliance or deficiencies are identified, the report should propose corrective actions to achieve satisfactory compliance.

## PROS

- Provides greater clarity on which specific compliance aspects require attention, allowing senior management to easily identify where the organization is falling short and what actions need to be taken.
- Offers a more holistic view of the organization's compliance status. Instead of focusing only on isolated risks or KPIs, this model provides a thorough review of key regulatory obligations.
- Since each area is evaluated individually, it is easy to detect which sections are non-compliant. This allows for prioritization of corrective actions and more efficient resource allocation.
- This methodology can be adapted to any type of organization, regardless of size or sector, as regulatory compliance aspects apply broadly to any data controller or processor.

## CONS

- By focusing solely on compliance, this methodology may not give sufficient attention to risk prioritization. For example, an organization may be compliant with regulatory provisions but still face high risks to data subjects' rights and freedoms.
- Creating a detailed report for each regulatory area can generate a significant administrative burden for the DPO and their team. Additionally, this type of report may become too lengthy and complex, making quick decision-making difficult for senior management.
- Without clear numerical indicators to support the compliance sections, it may be difficult to objectively assess the level of compliance and compare performance over time. The absence of quantitative data may also limit senior management's ability to make evidence-based decisions.

### iv. Combined Information Reporting (Compliance, Metrics, Risks)

The combined reporting model brings together the strengths of the previously described approaches, integrating structured sections on regulatory compliance, key performance indicators (KPIs), and detailed risk analysis.

This hybrid approach provides senior management with a comprehensive view of the organization's personal data protection status, ensuring that decision-makers can act based on both objective metrics and qualitative and risk-based analysis, minimizing the limitations of individual models.



**It is suitable for organizations that require an integrated view combining risk analysis, quantitative metrics, and qualitative evaluation of key data protection areas—especially useful in large companies with high volumes of personal data processing activities.**

a.

**Executive Summary:** This section is essential to provide a clear and concise overview for senior management members who may not be interested in operational details but need a general understanding for quick and effective decision-making. It should include a summary of the main compliance risks faced by the organization, measures requiring immediate implementation, and a selection of the most relevant KPIs for the reporting period.

b.

**Key Performance Indicators (KPIs):** This section presents the main performance indicators related to personal data protection. To avoid data overload, it is essential to prioritize KPIs that have a direct impact on risk management and continuous improvement of the system.

c.

**Current Risks:** Here, the DPO should outline the main risks facing the organization, both from a corporate perspective and in relation to the rights and freedoms of data subjects. A clear presentation and explanation of these risks is essential for senior management to fully understand their magnitude and potential consequences, enabling more effective mitigation measures and informed decisions that protect both the organization and the data subjects.

d.

**Compliance Status Information:** As previously explained, compliance block reporting is based on the systematic review and evaluation of key regulatory areas the organization must comply with in terms of data protection. This section should focus on the organization's level of compliance with specific points of the GDPR and other applicable sectoral regulations impacting data protection.

The choice of reporting model used by the DPO will depend on several key factors within the organization's context and the specific characteristics of personal data processing. The DPO should consider aspects such as the type of data processed, the size of the organization, available resources, hierarchical structure, and senior management's needs to select the methodology that best facilitates informed decision-making and regulatory compliance.

#### 4.1.4. Factors Influencing the Choice of Reporting Methodology

1.

**Type of organization and sector:** Companies that handle large volumes of sensitive data (such as those in the healthcare and social services sectors) may benefit more from risk-based reporting, as proper management of risks affecting data subjects' rights is crucial in these sectors. In smaller organizations or those dealing with less critical data, a KPI-based report may be sufficient to provide a clear view of compliance without overwhelming senior management with information.

2.

**Complexity of data processing:** In companies with complex data processing operations involving multiple areas and systems, section-based reporting is ideal. It allows each aspect (audits, data breaches, training, etc.) to be broken down, providing in-depth analysis of each processing area. In organizations with more standardized processing activities, KPIs may offer a sufficient overview of performance without the need for a highly detailed report.

3.

**Available resources:** If the organization has limited technological and human resources, it may opt for a KPI model, which is easier to manage and allows for quick evaluation. In environments with greater resources, the DPO could implement a mixed or risk-based model to provide a comprehensive assessment, which requires more effort in terms of risk and contextual analysis.

### 4.1.5. Forms of Communicating the Report

The DPO can choose from various methods to communicate information to senior management. Each method has its pros and cons, and the choice will depend on senior management's preferences, the organizational culture, and the nature of the information to be presented.

#### Detailed Written Report

This is one of the most traditional reporting formats in which the DPO prepares a comprehensive document that includes all relevant details about the state of data protection within the organization.

#### PROS

- Allows the DPO to present detailed information on every aspect of data protection. Senior management can review the report at their own pace and use it as a long-term reference.
- Provides a formal record of the compliance status and identified risks at a specific point in time. This is useful for audit purposes and for tracking progress over time.
- The DPO has the opportunity to structure the report clearly and logically, with separate sections for each relevant topic (compliance, risks, incidents, etc.).

#### CONS

- Detailed reports can be lengthy, which may discourage senior management from reading them in full. Sometimes, executives may not have time to delve into all the details and could overlook critical aspects. For this reason, it is always recommended to include an executive summary highlighting the most critical points.
- A written report does not allow the DPO to clarify doubts or answer questions immediately, which could lead to misunderstandings or lack of attention to certain points if there is no opportunity for the DPO to explain unclear aspects.

## Graphical and Visual Presentations

Using tools such as charts, tables, and diagrams is an effective way to convey information concisely and in a visually appealing manner. These presentations are usually shorter than written reports and focus on key points.

### PROS

- Charts and visuals condense large volumes of information into simple, easy-to-interpret representations. This helps senior management quickly identify areas of highest risk and recommended actions.
- Visual presentations are more effective in highlighting trends, comparisons, and key metrics. A well-designed chart can have a more lasting impact than a paragraph of explanatory text.
- Since graphical presentations are typically shorter, they force the DPO to prioritize the most important points, which can help avoid information overload when communicating with senior management.

### CONTRAS

- While graphical presentations are useful for providing an overview, they may lack the detail needed for senior management to fully understand more complex issues.
- The success of a graphical presentation depends on the DPO's ability to use data visualization tools effectively, which may not always be the case.
- Although charts and diagrams provide a good general overview, they may require additional explanations or context to fully understand the implications of the data presented.

## Oral Presentation

Another common way to deliver the report is through an oral presentation during a meeting of the executive committee or a specialized committee on risk or compliance. In this format, the DPO has the opportunity to present the key points of their report and respond to questions in real time.

### PROS

- Oral presentation allows senior management to interact directly with the DPO. This facilitates immediate resolution of doubts and clarification of specific aspects of the report.
- The DPO has the opportunity to emphasize the most important points and persuade senior management of the need to act on certain risks. Oral delivery enables communication of not just data, but also urgency and priority.
- During the presentation, the DPO can adapt to their delivery based on the reactions of senior management, focusing more on topics that generate greater interest or concern.

### CONS

- **Time constraints:** The time available for the presentation is usually limited, which can make it difficult to cover all relevant information. The DPO must be highly efficient in time management to ensure key points are addressed.
- Although a written summary may be provided afterward, senior management may not have a detailed document for future reference, which can hinder follow-up on discussed issues.

## Presentation to the Board of Directors

In certain organizations, especially those operating in highly regulated sectors, the DPO may be required to report directly to the board of directors. This type of reporting has a significant impact, as the board holds direct responsibility for managing organizational risks.

### PROS

- Direct reporting to the board ensures that data protection issues are addressed at the highest level of the organization, with decisions made at this level carrying strategic weight and potentially leading to significant organizational changes.
- Involving the board directly into data protection oversight reinforces the organization's responsibility and commitment to regulatory compliance.

### CONS

- Not all organizations allow the DPO to report directly to the board. In many cases, the time allocated for the DPO to present their report may be extremely limited.
- At the board level, discussions may be very high-level, and specific details of the DPO's report may not receive adequate follow-up.

## Combination of Methods

As explained in the previous section, the best solution may be a combination of several methods.

***“The DPO may present a detailed written report with visual charts and tables to support key points, accompanied by an oral presentation during a meeting with senior management, where the most important points are summarized and questions addressed.”***

This approach ensures that all relevant information is available in multiple formats, and that details are not lost, while also allowing direct interaction with senior management.

Although the DPO has the flexibility to propose a reporting method, they consider it effective. **The final decision on how and when the process should be carried out lies with the data controller.** According to **Article 38 of the GDPR**, the controller must ensure that the DPO can properly perform their duties, including providing direct access to the highest hierarchical level for accountability.



The reporting format will therefore depend on the needs and preferences of senior management, as well as the nature and risk associated with the personal data being processed. In any case, it is the controller's duty to provide the necessary mechanisms for the DPO to effectively fulfill their reporting responsibilities.

#### 4.1.6. Reporting Guidelines

Regardless of the reporting model chosen, the DPO must follow a series of guidelines to ensure effective communication with senior management:

- **Clear and accessible language:** The report must be understandable to all members of senior management, including those without deep technical knowledge of data protection. Technical jargon should be avoided or briefly explained to maintain engagement.
- **Highlight key risks and actions:** Senior management must be able to quickly identify critical issues requiring attention. The report should not be an exhaustive list of minor incidents, but a presentation of matters with significant compliance impact.
- **Include potential impacts:** The report should incorporate potential consequences for the organization from both legal (fines or sanctions) and reputational perspectives. The DPO should be able to present these impacts on economic or strategic terms to help senior management understand the implications.

***"However, it must be remembered that data protection compliance should not be limited to avoiding fines or sanctions, but should reflect a proactive stance that integrates data protection as an added value for the organization."***

- **Propose practical solutions:** The DPO should not merely describe problems, as this could lead to their role being perceived as obstructive. Instead, they should propose specific solutions without creating a conflict of interest. These recommendations should be practical and aligned with the organization's capabilities and resources. Ultimately, it is the controller who must make the informed decision to implement a specific action plan or measure.
- **Emphasize shared responsibility:** The DPO must stress that data protection is a shared responsibility within the organization. While the DPO plays a key role in oversight and advisory, effective implementation of data protection policies and measures requires collaboration across all departments involved in personal data processing—from IT to HR and marketing.

### 4.1.7. Relationship with Other Areas of the Organization

The DPO is a key figure in ensuring compliance with personal data protection regulations within an organization. Therefore, it is essential that they integrate properly into the organizational structure, collaborating with different departments and generating synergies that support the effective performance of their duties. This includes cooperation from all departments involved in the processing of personal data, from IT to Human Resources and Marketing.

The success of the DPO does not rely solely on their technical knowledge of the legislation, but also on their soft skills—such as communication, influence, and coordination with other key departments, especially those that have a direct impact or relationship with personal data processing activities. The relationships they build with each area of the organization can make the difference between a mechanical implementation and a true integration of a proper data protection culture into the organization's daily operations.

### 4.1.8. Human Resources (HR)

The Human Resources department is one of the most critical areas with which the DPO must collaborate, as it typically handles large volumes of personal data related to employees, candidates, and former employees. These often include highly sensitive data (e.g., disability certificates, health data, payroll information, etc.). At times, the DPO may encounter resistance and significant challenges in this area, particularly regarding the retention of personal data.

### 4.1.9. IT Department (Information Technology)

**The DPO and the IT team should be natural allies** in implementing security measures to protect personal data, although challenges may arise due to differing priorities. While the DPO may focus on regulatory compliance, the IT department may prioritize operational efficiency or the implementation of new technologies. These differences can hinder collaboration if not properly managed.

The DPO needs a solid understanding of the technologies and systems used within the organization—such as servers, databases, and networks—in order to assess the risks associated with personal data processing. However, beyond technical knowledge, the key for effective collaboration lies in the DPO's ability to build a relationship of trust with IT teams, ensuring that technical solutions are compatible with and appropriate for GDPR requirements. A common challenge will be the DPO's ability to convey the need to adopt sufficient and appropriate technical security measures from the design phase of information systems, tailored to the risks involved in the organization's personal data processing activities.

#### 4.1.10. CISO or Chief Information Security Officer

The collaboration between the DPO and the CISO (Chief Information Security Officer) is strategic and **must be based on smooth coordination, as both roles share the responsibility of protecting the organization's data, although from different perspectives.** Despite the clear synergies, the DPO focuses on ensuring that the processing of personal data is lawful and respectful of individuals' rights, while the CISO concentrates on implementing technical and organizational security measures to prevent vulnerabilities and attacks that could compromise the organization's information (including personal data).

One of the most common challenges is aligning priorities, as the CISO provides guidelines aimed at ensuring information security—whether personal data or general information—while the DPO's guidelines are aimed at safeguarding individuals' rights and freedoms, not necessarily the security of the information itself (as per Article 77 of the GDPR).

#### 4.1.11. Marketing and Sales

Marketing and sales departments are often at the core of personal data management, using tools such as CRM (Customer Relationship Management) systems or conducting email marketing campaigns. In this context, the DPO must ensure that the department's actions comply with requirements for transparency, appropriate legal bases (consent or legitimate interest), and the exercise of data subjects' rights.

A common challenge for the DPO in working with marketing is balancing regulatory compliance with commercial strategies. It is understandable that the marketing team seeks to maximize the use of personal data to personalize campaigns and improve conversion rates. The DPO must ensure that such processing is carried out within the legal framework, advising on the most appropriate legal basis, ensuring necessary consents are obtained, and responding to data subjects exercising their rights—all while minimizing the impact on the organization's commercial strategies.

#### 4.1.12. Legal Department

The collaboration between the DPO and the legal department is likely one of the smoothest, as both share the role of advisor and risk informer, acting as a second line of defense for the company. However, tensions may arise when approaches differ, since the legal department receives directives and instructions to align legal strategies with business objectives, which may sometimes conflict with the DPO's responsibilities.

Proper coordination between the DPO and the legal department is essential to address issues such as security breaches, international data transfers, or managing contracts with vendors that involve personal data processing. They must work together to implement contractual clauses that protect the organization from potential sanctions while also complying with GDPR requirements.

### 4.1.13. Senior Management

As discussed in the previous chapter, support from senior management is essential for the DPO to effectively fulfill their responsibilities. However, one of the biggest challenges the DPO faces is conveying to leadership the strategic importance of data protection, especially when there is no clear perception of the risks associated with mishandling personal data.

The DPO must be able to clearly articulate the benefits of a robust data protection policy—not only in terms of regulatory compliance but also in relation to customer trust, corporate reputation, and minimizing financial risks from potential sanctions. This process requires a special ability **to influence and persuade at the highest hierarchical level, demonstrating that investing in data protection is an investment in the long-term sustainability of the business and a generator of corporate value.**

# 5 PUBLIC SECTOR

## 5. 1. Obligation to Appoint a DPO in the Public Sector

Article 37 of the GDPR states that the controller and the processor of processing carried out by a public authority or body must appoint a Data Protection Officer (DPO), except for courts acting in their judicial capacity.

The obligation to appoint a DPO stems directly from the GDPR, as the Spanish Data Protection and Digital Rights Act (LOPDGDD) refers in Article 34 to the provisions of Article 37 of the GDPR, without adding any clarification or specification regarding public entities or institutions.

The terms “public authority or body” are very broad and require further precision. For this, we refer to national law, specifically Article 2 on the subjective scope of Law 40/2015, of October 1, on the **Legal Regime of the Public Sector (hereinafter, Law 40/2015)**, which states:

### The Public Sector includes:

1.

- 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.

### The Public Sector includes:

2.

- a) Any public bodies and entities governed by public law that are linked to or dependent on Public Administrations.
- b) Private law entities that are linked to or dependent on Public Administrations.
- c) Public universities.

## 3.

They are considered Public Administrations: 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 governed by public law referred to in letter a) of section 2.

Given this broad and heterogeneous subjective scope of application, the role of the DPO in these institutions and entities must, in any case, be adapted to the particular idiosyncrasies of each one, which is not an easy task due to their organizational diversity.

As in other areas or sectors, the first decision must be whether to carry out the task with internal resources or to outsource it.

## 5. 2. External DPO

As in other areas or sectors, the first decision must be whether to carry out the task with internal resources or to outsource it. Article 37.6 of the GDPR allows for the possibility of outsourcing the DPO role. In the case of outsourcing, the DPO—who may be a natural or legal person—will be linked to the public entity through a service contract. For the tendering, awarding, and execution of these service contracts by public entities, the provisions of **Law 9/2017, of November 8, on Public Sector Contracts must be followed.**

The subjective scope of application of this law includes the entire public sector and can even be considered broader than that mentioned above regarding the obligation or even the mere recommendation to have a DPO (see Article 3 of Law 9/2017). Furthermore, the service contract is a typical administrative contract (see Article 17 of the same law).

It must be considered that the organizational models applicable to private entities cannot be directly transferred to public entities. The service provision **requires adequate knowledge of the needs, organization, and specific characteristics of the contracting public entity, always bearing in mind that actions and powers involving the exercise of authority cannot be outsourced** (Article 17 of Law 9/2017).

Therefore, in terms of contract responsibility (Article 62 of Law 9/2017), the public entity must appoint a liaison with the contracted company to ensure the proper execution of the agreed service.

## 5. 3. Collegiate Body

**There is nothing preventing the DPO function from being assumed by a collegiate body.** These bodies are generally regulated for most public entities by Articles 15 to 24 of Law 40/2015. In such cases, a clear internal assignment of tasks and responsibilities must be made, which should be properly documented in the creation agreement and in the operating rules.

**The National Cryptologic Center, in its CCN-STIC Guide on Responsibilities and Functions within the scope of the National Security Framework**, establishes that in organizations of significant size, certain bodies or committees may exist to collaborate in the entity's security—whether physical, information, data protection, or all of them. Among the most common are the Corporate Security Committee, the Information Security Committee, and the **Data Protection Committee**.

The guide states: *"When, exceptionally, a joint Information Security–Data Protection Committee is formed, special care must be taken to analyze potential conflicts of interest, especially regarding the Data Protection Officer, who, in the exercise of their functions, must not receive instructions, must report to the highest hierarchical level, and must not participate in decisions regarding the purposes and means of processing."*

From all the above, it follows that **regardless of the creation of a committee, it must include, among others, the distinct figure of the Data Protection Officer**.

## 5. 4. Organizational Model

In this regard, the entity must organize security by involving all members through the designation of different security roles with clearly defined responsibilities within the regulatory framework that governs the activities and competencies of a public administration. This framework essentially includes its legal regime, all legal norms related to electronic administration and its interoperability, information security and the services that handle it, data governance and management, its reuse regime, transparency, and the protection of personal data.

Since security is a process that integrates all technical, human, material, and organizational elements, and considering the provisions of the **National Security Framework (Royal Decree 311/2002, of May 3)**, which contains the basic principles and minimum requirements necessary for adequate protection of the information processed and the services provided by public sector entities, and also considering the guidelines established in the **CCN-STIC-801 Guide "Responsibilities and Functions in the NSF,"** the public administration will undertake the following actions:

- **Designate security roles:** Service Managers, Information Managers, Information Security Manager, System Manager, and Data Protection Officer.
- **Establish a consultative and strategic body for decision-making** in Information Security matters. This body will be formed as a collegiate body and will be called the Security and Data Protection Committee. It will be chaired by a natural person who will formally assume responsibility for its actions.

Security and Data Protection Roles and Bodies:

- **Service Managers and ENS Information Managers:** Heads and managers of the various administrative bodies and units.
- **Data Protection Officer (DPO):** The Security and Data Protection Committee, with the designated Service

Head acting as liaison with the Spanish Data Protection Agency (AEPD) Responsable de Seguridad de la Información ENS.

- **ENS Information Security Manager.**

- **ENS System Manager.**

- **Security and Data Protection Committee:**

- o **Chairperson:** Highest representative of the entity responsible for data processing.

- o **Secretary:** Information Security Manager.

- o **Members:**

- » A manager from the entity's leadership
    - » A manager for Electronic Administration and Transparency, acting as data controller
    - » A manager for Data Governance, acting as information controller
    - » System Manager
    - » Person designated as liaison with the AEPD

- **Other Information and Service Managers** will be summoned by the Chairperson depending on the matters to be addressed.



### 5.5.1. Data Protection and Information Security in the Public Sector: Toward a New Organizational and Relational Model

If the task is to be carried out with internal resources, it is possible to appoint a single DPO for each public institution. However, this is not advisable in cases of large units or bodies with distinct identities and clearly differentiated tasks, even if they are organically dependent on a single entity. (This was the position of the now-defunct Article 29 Working Party in its analysis of the DPO role.)

#### 5.5.1.1. Shared Responsibility for Security and Data Protection in the Public Sector

Despite the existence of clearly defined roles in the areas of security (CCN-STIC-801 Guide) and privacy (GDPR – DPO), it is not feasible to manage Personal Data Protection and ENS adaptation measures independently. These are not separable fields; they form a unified system from both a functional and legal perspective. Therefore, shared responsibility between the Security Manager and the DPO in establishing and determining protection measures makes sense, especially since in Public Administrations, the object of security regulated by the ENS is public sector information, which mostly refers to personal data.

In this regard, the **Spanish Data Protection and Digital Rights Act (LOPDGDD)** of December 5, 2018, in its First Additional Provision (Security measures in the public sector), states:

1.

The ENS shall include the measures to be implemented in cases of personal data processing, adapting the criteria for determining risk in data processing, and the provisions of Article 32 of Regulation (EU) 2016/679.

2.

Public entities listed in Article 77.1 of this Organic Law (as data controllers) must apply the appropriate ENS security measures to personal data processing and promote equivalent implementation levels in associated private law entities such as companies or foundations.

Later, **Article 3 of Royal Decree 311/2022, of May 3, regulating the ENS**, establishes that when an information system processes personal data, the rules governing personal data protection (GDPR and LOPDGDD) and their protection techniques (risk analysis and impact assessment in data protection) shall apply. If these measures are stricter than those provided by the ENS, they shall prevail.

Therefore, and in line with efficiency principles, many public administrations opt for a joint definition of the Data Security and Privacy Policy, and the establishment of a single committee called the Security and Data Protection Committee, where both the Security Manager and the DPO work collaboratively.

This policy must define specific mechanisms for resolving disputes and conflicts, and clearly identify the responsibilities of each role, including any positions that may be incompatible with these functions.

### 5.5.1.2. Electronic Communication Between Public Sector Entities Requires Collaborative Work

Law 40/2015, in Article 156.2, defines the ENS as follows:

“The National Security Framework aims to establish the security policy for the use of electronic means within the scope of this Law and is composed of the basic principles and minimum requirements that adequately guarantee the security of the processed information.”

Similarly, **Article 3 of Law 40/2015** states that Public Administrations shall interact with each other and with their bodies through electronic means, ensuring system interoperability and security, and guaranteeing the protection of personal data.

This same principle of systematic and collaborative action is reflected in the conceptual framework of the **CCN-CERT STIC 801 Guide** for organizing DPO, ISM (Information Security Manager), and SM (System Manager) roles and responsibilities. As shown, no hierarchical relationship is proposed between the ISM and the DPO, whose activities fall within a shared framework of concurrent actions.

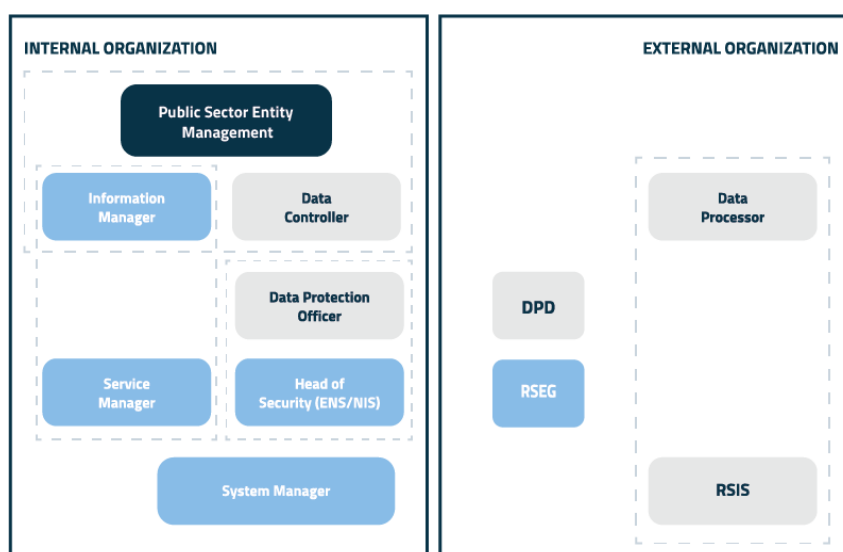


Figure 1. Conceptual Diagram of Information Security and Data Protection

An example of the logical concurrence of responsibilities is that the Spanish Data Protection Agency (AEPD) has indicated the possibility that the role of the Data Protection Officer (DPO) may coincide with that of the ENS Security Officer in organizations that, due to their size and resources, cannot maintain such separation. (See the report from the Legal Office of the Data Protection Agency<sup>7</sup>).

## DPO and Deputy Security Officer

As stated in the development of the National Security Framework (ENS), in those information systems that, due to their complexity, distribution, physical separation of elements, or number of users, require additional personnel to carry out the functions of the Security Officer, each organization may appoint Deputy Security Officers to whom functions—but not responsibility—will be delegated. Each Deputy Security Officer will maintain a direct functional dependency on the Security Officer, to whom they will report. Similarly, the possibility of appointing Deputy System Officers is also established.

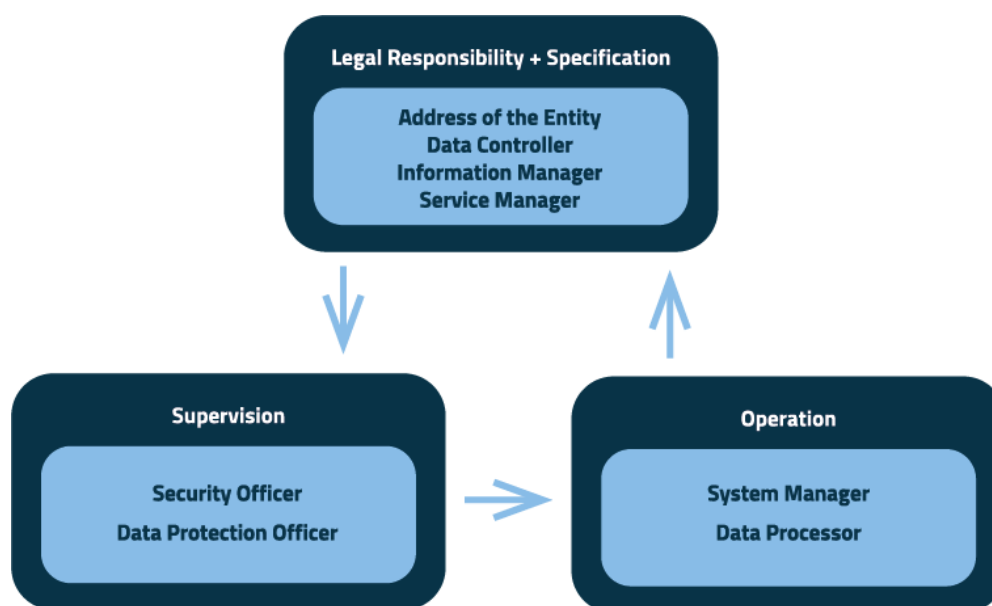
Following this reasoning, and in light of the DPO's obligations to supervise compliance with the GDPR and other applicable regulations—including the assignment of responsibilities—and considering the evident lack of resources available to public DPOs, one way to address the absence of a dedicated privacy office or support area required by a DPO is the assignment of data protection responsibilities to Information and Services Officers, or alternatively, the appointment of Deputy DPOs who assume the functions entrusted to them within their area of competence, acting as specialized collaborators. It is emphasized that what is delegated are functions, not responsibility.

### 5.5.1.3. Relationship of the DPO with Other Areas of Responsibility in the Public Sector

The CCN-CERT STIC Guide 801 presents a framework that distinguishes three major blocks of responsibility:

1. **Legal responsibility and specification of needs or requirements**, which correspond to the entity's management and the controllers of the information or service.
2. **Supervision**, which corresponds to the Security Officer and the DPO.
3. **Operation of the information system**, which corresponds to the System Officer.

<sup>7</sup><https://www.ismsforum.es/ficheros/descargas/independencia-dpd-responsable-de.pdf>



*Image 2. Responsibility Blocks*

Given the current national and European technological and regulatory ecosystem, where all regulations regarding ICT, security, and data protection are harmonized and interdependent, we proceed to detail the close relationship of the DPO with the following figures of the Public Administration, whether traditional roles or newly created ones, part of whose responsibilities could initially be assumed by the DPO.

### The DPO as a “transparency tool”:

#### DPO and Head of Electronic Administration/IT:

- Establishment of visible, accessible, and simple mechanisms, including electronic means, to maintain control over personal data and the exercise of rights, as well as procedures that allow responding to rights requests within the deadlines set by the GDPR.
- Design of security, privacy, accessibility, and data reuse by default.
- Coordination of obtaining data from other Public Administrations for purposes other than the processing of administrative procedures.
- Obtaining legally valid consent with due safeguards in the case of minors.

#### **DPO and Head of Archiving/Document Management:**

- Definition of metadata that determines the existence of personal data.
- Management of metadata in publications if it could identify or make a natural person identifiable.

All in accordance with the National Interoperability Framework, specifically the metadata schema for electronic document management (e-EMGDE).

#### **DPO and Contracting Officers:**

- Determination of standard conditions and clauses to be included in data processing agreements.
- The need for processors contracted to provide certain services to collaborate in responding to data subject requests. In these cases, such collaboration must be included in the data processing agreements.
- Criteria to assess whether processors with whom processing operations have been or will be contracted offer guarantees of GDPR compliance. To strengthen this assessment and provide greater legal certainty to organizations, it would be advisable to have a specific certification that accredits compliance with the requirements for data processing services in terms of data protection. This type of certification would standardize best practices, facilitate the selection of service providers, and promote greater transparency and trust in personal data processing.
- Regarding Data Governance, include standard clauses to determine obligations related to access and reuse of datasets that may be generated during service provision or within the framework of a research project.

#### **DPO and Head of Information and Services:**

- Establishment of the Record of Processing Activities.
- Risk analysis for the rights and freedoms of citizens regarding the data processing activities carried out.
- Assessment of whether the processing operations require a Data Protection Impact Assessment because they pose a high risk to the rights and freedoms of data subjects and carrying out such an assessment.
- Assumption by the Head of Information and Services of ownership of the risks related to the information and services under their responsibility, as well as any error or negligence that results in a confidentiality or integrity incident in terms of data protection and availability in terms of security.

**DPO and Security Officer:**

- Need to review the security measures applied to processing activities in light of the results of their risk analysis. The GDPR requires that security measures be appropriate to the characteristics of the process, its risks, the context in which it is carried out, the state of the art, and the costs.
- Need to establish mechanisms to quickly identify the existence of data security breaches and respond to them.

**DPO and System Owner:**

- Collaborate in conducting Security and GDPR compliance audits.
- Propose, for security reasons, the suspension of processing certain information.
- According to the ENS, the security officer must be different from the system owner, and there should be no hierarchical dependency between them. This is because the security officer needs the necessary independence to assess and ensure the implementation of security measures without conflicts of interest.

In line with EU Regulation 2022/868 of May 30, 2022, on European Data Governance, and Regulation 2023/138 of December 21, 2022, on high-value data and modalities for publication and reuse, as well as Law 37/2007 of November 16 on the reuse of Public Sector Information.

- Collaborate in personal data anonymization processes.
- Establish data quality requirements.
- Provide security and trust measures for public sector data spaces, along with access and reuse conditions.
- Collaborate in data governance: define organizational and technical mechanisms to obtain and process data in accordance with individuals' rights, lawfulness, quality, and ethical standards.
- Obtain consent from data subjects to share the data provided.
- Conditions for the preservation or destruction of historical data.
- Coordinate the content of the inventory of datasets and information sources with the public Record of Processing Activities (RPA).
- Collaborate in assessing the lawfulness of reuse and access requests for datasets based on their purpose.
- Determine processing limitations for reusable datasets when required by the GDPR.
- Ensure the quality and integrity of data for subsequent use in AI systems, guaranteeing regulatory compliance and the rights of data subjects.

**DPO and Head of the AI Competence Center:**

- Inform and define the legal basis or obtain consent for profiling and personalization of services and other purposes of public interest.
- Indicate in the inventory of datasets and information sources the automated generation of administrative acts or other decisions, specifying the nature of such acts, the rights of individuals that could be affected—especially if the data is inaccurate or the algorithm is inconsistent or biased.
- Inform data subjects adaptively at each stage of the AI lifecycle where processing occurs.
- In the case of automated individual decisions (Article 22 GDPR), prepare a report on their adequacy, identifying potential risks and proposing mitigation measures in accordance with the AEPD's Adequacy Guide for processing involving AI. [Guía Adecuación AEPD](#).
- Conduct continuous reassessments and audits of processing activities involving AI, following AEPD recommendations on AI audit requirements. [Requisitos auditorias IA. AEPD](#).

## 5.6. Profile of the DPO in the Public Sector

The GDPR, in Article 37.5, states that the DPO “shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39.”

Article 35 of the LOPD establishes that the DPO may be a natural or legal person, and that, to demonstrate compliance with the qualification requirements set out in Article 37.5 of the GDPR, certification mechanisms may be used.

These certification mechanisms should particularly consider, on the one hand, obtaining a university degree that certifies specialized knowledge in law, and on the other hand, practical experience in data protection. Recital 97 of the GDPR states that, in the case of a public entity, the controller or processor “should be assisted by a person with expert knowledge of data protection law and practices if the processing is carried out by a public authority or body, except for courts acting in their judicial capacity.” Conversely, this requirement for legal and data protection expertise is adjusted in the case of private entities, based on the nature (types of data) and scale (large-scale) of the processing.

Consequently, in the public sector, it seems logical that, in addition to the general professional and competency requirements for a DPO, certain mandatory requirements apply due to the specific type of entity involved. This means, in any case and regardless of the processing or the amount of data processed, the requirement for a specialized legal profile. Furthermore, as the WP29 states, it is important to consider that, in the case of a public authority or body, the DPO must also have knowledge of the specific regulations applicable to the organization, which implies a solid understanding of public law and administrative procedures, both in conventional and digital environments.

Therefore, we are designing an academic and professional profile that should include high-level knowledge and a university degree, typically at MECES level 3 (Master's). Additionally, given the nature of the functions, it seems appropriate to consider a career civil servant profile (Article 9.2 of the Basic Statute of Public Employees, Royal Legislative Decree 5/2015, of October 30), which would guarantee independence and stability, as opposed to other figures such as interim officials.

In principle, it might seem acceptable to allow a permanent employee profile (with an indefinite contract) for the DPO; if we have accepted the possibility of outsourcing the DPO through a service contract, it seems we understand that the DPO's functions do not involve exercising authority. However, upon analyzing the DPO's functions, a potential issue arises regarding the function set out in Article 37.1 of the LOPDGDD (not included in the GDPR).

Beyond the collaboration with supervisory authorities expressed in GDPR Article 39(1)(d) and reflected in Article 37.2 of the LOPDGDD, Article 37.1 introduces the possibility for the data subject to submit a "prior complaint" before filing a complaint with the AEPD. This complaint will be addressed to the DPO, who must "communicate the decision adopted within two months."

The application of this procedure in the public sector, especially in the administrative field, necessarily leads us to the matter of complaint resolution, an eminently administrative procedure linked to the concept of exercising authority.

It could therefore be inferred from the existence of this procedure that public entities may be prohibited not only from outsourcing the DPO role but also from appointing an employee whose employment relationship with the entity is contractual rather than statutory (civil servant).

However, if we analyze the literal wording of the regulation, we can also reach a more flexible solution in the areas of public contracting and categorization of public employees. The regulation never states that the DPO must instruct or decide on the complaint. The DPO is not granted competence to resolve the matter: the regulation merely designates the DPO as a "communication channel" for the complaint, both in terms of receiving it and communicating the resolution to the data subject. In other words, the LOPDGDD does not address the nature or competence for resolving this prior complaint and leaves room for the public entity to decide whether to include or exclude the DPO from procedures and administrative acts involving the exercise of authority.

Applied to public law frameworks, each case must analyze the decision-making competence of the public organization and act accordingly.

***"Therefore, unless it is understood that the competence to instruct or resolve the complaint lies with the DPO, we can speak of the DPO's involvement in this prior complaint procedure at an advisory level, but not as an exercise of authority, thus allowing both external contracting and employment relationships."***

In any case, it is logical that the position falls within professional classification group A1 for civil servants or equivalent for employees (Articles 76 and 77 of the Basic Statute of Public Employees, Royal Legislative Decree 5/2015, of



October 30), requiring knowledge in certain general and specific competencies. In the public sector, the DPO's specific competencies are the same as those already mentioned for the private sector. The difference lies in the general competencies required.

The public sector DPO must have general competencies at a specialized level in public law, meaning a deep understanding of regulations applicable to the public sector in general and specifically to the type of public entity. Additionally, they must have knowledge of digital technologies as applied to public entities and administrations. This requires an understanding of digital technologies, not at a deep technical level, but from the perspective of their interaction with the personal data protection system and as a strategic element to achieve a reliable and integral data security system. It is understood that technical staff responsible for the security system must interact effectively with the DPO in this area.

Finally, it should be noted that, depending on the activity, a DPO may be appointed on a part-time or full-time basis. In the former case, the appointment must necessarily address the distribution of shared tasks, avoiding in any case both conflicts of interest and the predominance of one task over the other to such an extent that it compromises the proper performance of DPO functions. y deja margen de maniobra para incluir o excluir, según se estime conveniente por la propia entidad pública, al DPO de los procedimientos y actos administrativos que impliquen ejercicio de autoridad.



# PRIVACY GOVERNANCE

## 6. 1. Duties and Responsibilities of Data Protection Governance

In accordance with the GDPR, public and private entities must establish appropriate policies and procedures to ensure that the company, its executives, employees, and third parties comply with the applicable regulatory framework.

*“Responsibility for breaches and infringements under the GDPR ultimately lies with the highest hierarchical level in the organization: the Board of Directors and any other body to which management and governance functions have been officially delegated, such as Board Committees, the CEO, or the Executive Chairman.”*

However, in large organizations, it may be unmanageable for these roles to continuously monitor that data protection processes are properly implemented and functioning effectively, and it is also unlikely that these high-level figures possess the specialized knowledge required to know how or what decisions to make regarding certain processing activities.

Therefore, to comply with the accountability obligation, the GDPR proposes defining a clear and documented privacy governance model within the organization. This model should demonstrate that, while maintaining their role as the highest decision-making authority and receiving regular reports, other specialized teams and intermediate bodies provide closer oversight and effectively implement privacy management as required. **Beyond regulating cases where there is an explicit obligation to appoint a Data Protection Officer, the GDPR allows organizations to establish the governance model they consider most appropriate,** provided it enables them to meet their obligations as Controllers and/or Processors.

Data Protection Governance must demonstrate leadership and commitment to GDPR compliance through its actions, creating an environment where different stakeholders fully participate and where the management system can operate effectively in synergy with organizational objectives, including:

**a.**

Establishing organizational guidelines and objectives, ensuring that appropriate data protection policies are in place, and determining the organization's strategic direction.

**b.**

Promoting policies and objectives at all levels of the organization to increase awareness and engagement.

**c.**

Ensuring the integration of data protection management system requirements into organizational processes.

**d.**

Determining the necessary competence of the Data Protection Officer and committing to support their functions to contribute to the effectiveness of the data protection management system.

**e.**

Ensuring that the necessary resources for the data protection management system are available, with adequate budgets.

**f.**

Communicating the importance of proper data protection management and GDPR compliance to achieve the intended results.

**g.**

Ensuring that stakeholder requirements (customers, employees, shareholders, supervisory authorities, etc.) are prioritized at all organizational levels.

**h.**

Guaranteeing that processes and controls are implemented to help meet the requirements of affected individuals.

**i.**

Ensuring that responsibilities and authorities for relevant functions are assigned and communicated within the organization.

**j.**

Assessing the risks of personal data processing activities.

## 6.2. Data Protection Governance Model

The starting point for a robust model is to establish an organizational structure that clearly defines roles and responsibilities, ensuring that data protection is an integral component of decision-making. This model should cover all levels of the organization, from top management to operational areas, ensuring alignment with the data protection objectives set by the organization.

***“An effective governance model should not only ensure regulatory compliance but also integrate data protection into the organization’s strategic and operational processes.”***

The proposed governance model is organized into three main layers: **governance, supervision and control, and operations.**

### 6.2.1. Governance Layer

This level is responsible for defining general policies, approving the control framework, and setting strategic guidelines for data protection, typically corresponding to the organization’s top management. Key elements of this layer include:

- Setting the organization’s data protection strategy.
- Approving data protection policies and procedures that regulate data protection management within the organization (DPMS).
- Defining the governance model: establishing roles, responsibilities, and reporting lines within the organization.

### 6.2.2. Supervision and Control Layer

This layer monitors and evaluates compliance with the policies and processes established by the governance layer. It works closely with the operational layer to ensure that business processes correctly implement data protection policies and procedures. Additionally, this layer must regularly report to top management on compliance levels, identified risks, and corrective measures taken.

Within this layer, the DPO or a specialized privacy team acts as the second line of defense, responsible for overseeing regulatory compliance, promoting a culture of privacy within the organization, and ensuring that business units manage risks appropriately.

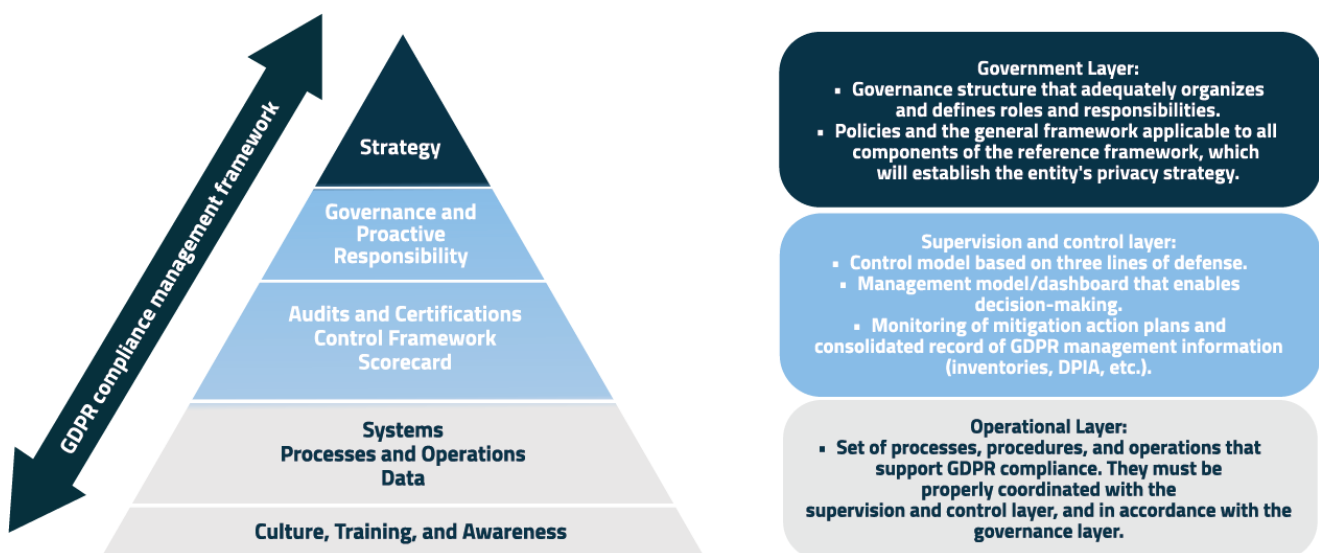
Furthermore, internal and external audit functions operate within this layer, independently assessing the effectiveness of the data protection governance model. This line of defense ensures that established controls are properly applied and that necessary corrective measures are taken, meeting the data protection objectives set by top management.

This layer also maintains and updates the dashboard with KPIs defined by the governance layer. Reports generated from these indicators allow top management to assess compliance levels and make corrective decisions if necessary.

### 6.2.3. Operational Layer

The operational layer (systems, processes, operations, etc.) is responsible for the day-to-day execution of privacy-related processes within the organization, implementing the policies and procedures established for the processing of personal data. This is where business processes are directly aligned with the requirements of the GDPR, and where the necessary technical and organizational measures are implemented to safeguard personal data.

Within the operational layer, business and support units (legal advisory, procurement, operations/IT, security, etc.) are encompassed, acting as the first line of defense and bearing responsibility for identifying, assessing, and managing privacy-related risks. The operational layer is directly supervised by the oversight and control layer, receiving directives and reporting on their implementation.



## 6.2.4. Personal Data Information Management System (PDIMS)

Although the term PDIMS is not a standardized or universally recognized concept in the field of privacy and data protection—at least not with the widespread use of other frameworks such as ISMS (Information Security Management System), which is linked to international standards like ISO/IEC 27001—it can be defined as follows:

*“The Personal Data Information Management System (PDIMS) can be defined as the documentary framework that governs comprehensive privacy governance within the organization, establishing the principles, policies, procedures, and controls necessary to ensure compliance with the GDPR and other applicable data protection regulations.”*

*“The PDIMS is based on the principles of proactive accountability, risk management, and continuous improvement, ensuring the integration of privacy into all organizational processes..”*

This documentation ranges from the **global data protection policy**, which sets out general principles and guidelines, to specific procedures such as **security breach management**, **internal data protection audits**, and the **exercise of data subjects’ rights**. Each of these components is essential to ensure the adequate protection of personal information and compliance with current regulations.

Below is a detailed proposal for the structure of the PDIMS. It is important to note that each organization must tailor this structure to its specific needs and characteristics, thereby ensuring an effective and customized implementation of the system.

### 1. Global Personal Data Protection Policy

This document should establish the fundamental principles underpinning personal data protection within the organization. It defines the obligations and responsibilities of all stakeholders involved in data processing and ensures the organization’s commitment to regulatory compliance.

There are both internal and public versions of this policy, allowing the organization to inform its staff, clients, and business partners about its data protection practices.

## **2. Data Protection Audit**

The audit is an essential process to ensure the effectiveness of the data protection system. Through periodic audits, the organization can identify potential failures or areas for improvement in its data processing practices.

This procedure should establish guidelines for conducting internal audits, defining roles and responsibilities, as well as the methodologies to be followed during the audit process.

## **3. Security Breach Management**

This procedure describes the process to be followed in the event of detecting a security breach affecting personal data, from its identification and analysis to the notification of the breach to the supervisory authority and, where applicable, to the data subjects, or to the data controller in the event of a breach occurring while acting as a processor.

It is also advisable to define response plans, as well as the methodologies and criteria that will be used to assess the risk caused by a security breach.

## **4. Handling Data Subject Rights Requests**

This procedure details the process for managing data subject rights requests, establishing responsibilities, and the appropriate response process for each request, as well as the recording of evidence, etc.

## **5. Política de Formación**

This policy should establish the need for periodic data protection training for all employees, the classification of training activities, planning, delivery methodology, roles and responsibilities, indicators, etc.

## **6. Data Retention Policy**

This policy will define the retention periods for personal data based on the purpose of processing, the criteria and legal grounds for blocking or deleting personal data, as well as the deletion and blocking mechanisms implemented by the organization.

## **7. Privacy by Design and by Default Policy**

This policy reinforces the adoption of the “privacy by design” principle, ensuring that personal data protection is integrated into every process and technology from the planning stage, establishing the procedure to be followed for new projects or initiatives involving the processing of personal data.

## 8. Risk Analysis and DPIA Procedure

This procedure should establish the guidelines for identifying and managing risks in the processing of personal data, including the methodology defined for both risk analysis and the comprehensive management of Data Protection Impact Assessments (DPIAs), the identification of roles and responsibilities, and how to document

## 9. Supply Chain Control Policy

This document will address the relationship with third parties, such as suppliers and business partners who may handle or access personal data on behalf of the organization, establishing the process to be followed for the assessment and approval of processors and sub-processors, as well as the framework for periodic audits of key third parties.

## 10. Organizational Structure for Data Protection

This document will describe the organizational structure for data protection within the company, clearly identifying roles, responsibilities, and functions, as well as establishing reporting flows and interaction between different departments to ensure an integrated and coordinated management of personal data throughout the organization.

The PDIMS is not only a set of policies and procedures but becomes a vital tool within the data protection governance model, providing a clear and detailed operational framework that regulates the processing of personal information.

**The effectiveness of the PDIMS will largely depend on its approval by senior management.** Firstly, this ensures the necessary commitment and support from the highest levels of the organization, which is essential for the effective and sustained implementation of the system. Furthermore, senior management approval reinforces the organizational culture of compliance and accountability by sending a clear message to all employees about the importance of data protection.

On the other hand, senior management support is essential to address and mitigate risks associated with personal data management, including potential legal sanctions and reputational damage to the organization. An PDIMS approved and endorsed by senior management demonstrates to stakeholders—including employees, customers, business partners, and regulators—that the organization takes data protection seriously and is committed to complying with applicable legislation.



## 6.2.5. Integration with Other Compliance Functions

An effective governance model cannot operate in isolation. It is essential that it aligns with other key compliance functions within the organization, such as risk management, information security, and internal audit.

1.

### Information Security

Collaboration between the data protection team and the information security department is critical. While both disciplines have different objectives, they must work hand in hand to ensure comprehensive protection of personal data.

It is crucial to establish regular communication channels between both teams to manage security incidents and ensure that information security policies are aligned with data protection regulations. For example, measures such as data encryption, access management, and physical and logical security controls should be jointly assessed.

2.

### Internal Audit and Risk Management

The internal audit function, as the third line of defense, plays a critical role in monitoring and controlling the mechanisms implemented. By integrating data protection into internal audit programs, organizations ensure that controls over personal data processing are periodically reviewed, and that potential failures or areas for improvement are identified.

To achieve this, it is highly useful to integrate data protection risk assessments into the organization's overall risk matrix. This will allow prioritization of processes that pose the greatest privacy risks and allocation of resources to effectively mitigate them.

3.

### Compliance

The compliance function (also part of the second line of defense, like the DPO) is another area with which the data protection model must be aligned. Many regulations—such as those related to anti-money laundering, healthcare, financial services, or the management of internal whistleblowing channels—have intersections with data protection requirements.

### 6.2.6. Continuous Training and Awareness

Another key pillar for the success of a governance model is ensuring that all employees understand their obligations regarding data protection and apply them in their daily activities.

Training should be tailored to the needs of each role within the organization, ensuring that each department receives training aligned with its responsibilities in relation to personal data processing. For example, IT staff need to understand technological risks and how to protect data within their systems, while marketing personnel must be aware of the rules on consent and the use of personal data for advertising campaigns.

Likewise, training should not be a one-time event but an ongoing process that ensures employees remain informed about regulatory and technological changes affecting data protection. This includes not only legislative changes but also new risks or technological trends such as AI or big data analytics. Therefore, it is essential to establish a continuous training program with mandatory annual courses and periodic assessments to measure staff knowledge levels.

As previously stated, data protection must become part of the organizational culture. This involves not only technical training but also raising awareness about the importance of privacy and the protection of individuals' rights, for example, through awareness campaigns using concrete examples of risks and promoting an "open-door" policy where employees can raise questions or concerns about data protection.

### 6.2.7. Promoting a Privacy Culture

The data protection governance model should not be limited to formal structures and processes. Its success largely depends on a strong privacy culture embedded throughout the organization, fostering awareness and commitment from all members to protect personal data beyond mere regulatory compliance. From senior management to frontline employees, everyone must understand the importance of safeguarding personal data and how this contributes to the company's success and reputation.

It is therefore relevant to include references to data protection and privacy in the organization's mission, vision, and values. Doing so reinforces the idea that data protection is an integral part of the business, not just a legal obligation.

## 6.3. Strategic Level – Data Protection Policy

As a result of the previous point, corporate objectives and those of the management system itself must be formalized in a data protection policy, as established in Article 24 of the GDPR and highlighted in Recital 78, demonstrating the organization's commitment and leadership in fostering a proactive and effective data management culture, as

well as compliance with applicable regulations. This is achieved through the establishment and dissemination of the organization's principles, values, and commitments in this area. Data protection policies are typically high-level, key documents that must later be translated into procedures, standards, and guidelines to support compliance with these objectives.



***“The implementation of a Data Protection Policy is a fundamental part of privacy governance and establishes the organization’s commitment to processing personal information with full respect for the fundamental rights and freedoms of data subjects.”***

The policy should cover clients, employees, contractors, partners, and other entities requiring occasional access to data, and its content may be adapted based on the level and type of risk associated with the processing activities carried out by the organization.

For example, the level of detail, robustness, and comprehensiveness of the policy for an entity handling millions of data subjects’ records in complex processing involving sensitive personal information or large volumes of data will be greater than for a small company performing limited processing of non-sensitive data. Likewise, the policy should be easy for staff to understand and follow; its implementation should not be complex or burdensome, and it should be reviewed and updated periodically.

The policy must recognize the data protection principles and rights established under the GDPR and explain how they will be implemented in relation to the processing activities carried out by the organization. Without intending to provide an exhaustive list, **the following points may form part of such a policy:**

**1.****Transparency**

Commitment to providing clear and simple information to data subjects regarding the conditions of processing activities that affect them, as well as in responses to rights requests, regardless of their level of knowledge. When collecting personal data from minors or other special groups, the information provided must be adapted to ensure comprehension.

**2.****Data Minimization**

Commitment to applying technical and organizational measures to ensure that only data strictly necessary for each specific processing purpose is processed, reducing the scope of processing, limiting retention periods, and restricting accessibility.

**3.****Lawfulness, Fairness, and Transparency**

Commitment to processing personal data lawfully, fairly, and transparently for the data subject.

**4.****Legal Basis**

All data processing must rely on a valid legal basis (e.g., consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest or in the exercise of official authority, or legitimate interests).

**5.****Accuracy**

Commitment to implementing reasonable measures to ensure that data is kept up to date and promptly deleted or corrected when inaccurate in relation to the purposes for which it is processed.

6.

#### **Record of Processing Activities**

Commitment to creating and maintaining an up-to-date record of personal data processing operations, both as Data Controller and as Data Processor.

7.

#### **Storage Limitation**

Commitment to retaining personal information in a form that permits identification of data subjects for no longer than necessary for the purposes of processing—except when retained for archiving in the public interest, scientific or historical research, or statistical purposes.

8.

#### **Data Subject Rights**

Commitment to enabling data subjects to exercise their rights of access, rectification, erasure (“right to be forgotten”), objection, portability, restriction of processing, and the right to object to automated decision-making (including profiling).

9.

#### **Security of Processing**

Commitment to determining and implementing appropriate technical and organizational security measures to ensure a level of security appropriate to the risk, considering the state of the art, implementation costs, and the nature, scope, context, and purposes of processing, as well as the varying likelihood and severity of risks to individuals’ rights and freedoms.

10.

#### **International Data Transfers**

Commitment to only carry out international data transfers outside the European Economic Area when an adequate level of data protection is guaranteed in accordance with EU law, as established in Chapter V of the GDPR.

**11.****Internal Roles and Responsibilities**

Identification of key roles with internal responsibilities within the data protection management system.

**12.****Reviews and Audits**

Commitment to conducting internal audits of the management system and reviewing its effectiveness and efficiency by senior management.

**13.****Processor Relationships**

Obligation to adopt appropriate measures for selecting service providers with access to personal data, ensuring and demonstrating that processing is carried out in compliance with the GDPR (accountability principle). Likewise, relationships between the controller and the processor must be formalized in a contract or legal act binding the processor to the organization.

**14.****Risk Analysis**

Obligation to adopt accountability measures based on the risks that processing may pose to the rights and freedoms of data subjects, performing risk assessments of processing activities to determine which measures should be applied and how.

**15.****Privacy by Design and by Default**

The organization has the responsibility to consider data protection from the very moment a processing activity, product, or service involving personal data is designed.

16.

#### **Personal Data Breaches**

Commitment to notify the competent data protection authority in the event of a personal data breach, unless it is unlikely that the breach poses a risk to the rights and freedoms of the affected individuals. In cases where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the notification to the supervisory authority must be complemented by a notification to the affected individuals.

17.

#### **Data Protection Impact Assessment (DPIA)**

Obligation to conduct a DPIA prior to implementing processing activities that are likely to result in a high risk to the rights and freedoms of data subjects.

18.

#### **Data Protection Officer (DPO)**

Responsibility to assess whether the organization is required to appoint a DPO and to justify cases where such mandatory appointment is not made, in accordance with Article 37 of the GDPR.

19.

#### **Processing of Minors' Data**

Obligation to make reasonable efforts to adapt the information duty and the process of obtaining consent, as well as the processing activities carried out by the organization, when handling data of minors under the age of fourteen.

20.

#### **Training and Awareness**

Commitment to providing employees with periodic data protection awareness training. This training is essential to ensure that staff are familiar with the organization's policies, applicable regulations, and legal requirements relevant to their daily functions.

Finally, as with any management system, the policy must be approved by senior management, securely communicated within the organization, and made available to stakeholders within its scope, typically the organization's staff. Likewise, it is necessary to ensure and demonstrate that the policy has been properly implemented and applied. The development of the various components of the management system must be linked to this policy, ultimately forming a comprehensive set of organizational standards.

## 6.4. Organizational Level – Roles and Relationships

In terms of organizational level, the most common key roles found among entities in privacy management decision-making include:

1.

**Senior Management:** The GDPR establishes that it is the controller or processor, and not the Data Protection Officer, who is obliged to implement “appropriate technical and organizational measures to ensure and be able to demonstrate that the processing complies with this Regulation” (Article 24.1). Compliance with data protection regulations is the corporate responsibility of the controller.

Senior management (at board level) plays a key role in enabling the DPO to perform their duties effectively, has an obligation to actively support their work, and must be directly informed of the DPO's advice and recommendations.

In addition, they will be responsible for promoting a culture of compliance with data protection regulations by establishing and disseminating the organization's principles, values, and commitments in this area.

2.

**Data Protection Officer (DPO):** The DPO is the cornerstone of data protection compliance in organizations and, therefore, is the key participant in privacy governance. Specifically, the DPO is the link between senior management and the data protection management system. At the governance level, the DPO must report directly to senior management, but must also communicate and coordinate with all stakeholders in the different business areas.



3.

**Data Protection Officer's team:** depending on the size and structure of the organization and the assignment of the role of Data Protection Officer, it may be necessary for the Data Protection Officer to have a support team to carry out their duties. In such cases, the internal structure of the team and the tasks and responsibilities of each of its members must be clearly defined.

4.

**Data Protection Officers by Business Area:** they are responsible for ensuring that the data protection policy is properly incorporated and managed within the scope of their duties and business activities. When organizations have different key departments that process personal data, it is common to find that global/local representatives of these departments are assigned specific data protection duties.

5.

**Data Controller:** The entity that, by defining the purposes and means of processing, is ultimately responsible for the appropriate use and security of personal data throughout the entire processing lifecycle.

6.

**Processor:** the entity that processes personal data on behalf of and for the account of the controller. The processing activities it carries out must comply with the policies, procedures, standards, and general privacy principles established by the controller.

Among the most common mechanisms for interaction between these roles and entities within an organization, the following are worth noting:

1.

**Board of Directors:** The Data Protection Officer must report key issues related to compliance with data protection regulations to the organization's senior management. Reporting directly to the Board of Directors or another management body or committee is standard practice when particularly significant situations arise, and at least one annual report on the DPO's activities must be submitted.

2.

**Other Committees:** depending on the structure, it is common to find examples of interaction between the Data Protection Officer and other committees in different areas:

- Global Committees: Risk Control and Compliance Committee, Information Security, Legal, Cybersecurity, etc.
- Country
- Business Functions

3.

**Data Protection Officer Forums:** Data Protection Officers often establish forums to coordinate the privacy management system with different liaison points in business units or data protection officers in each country.

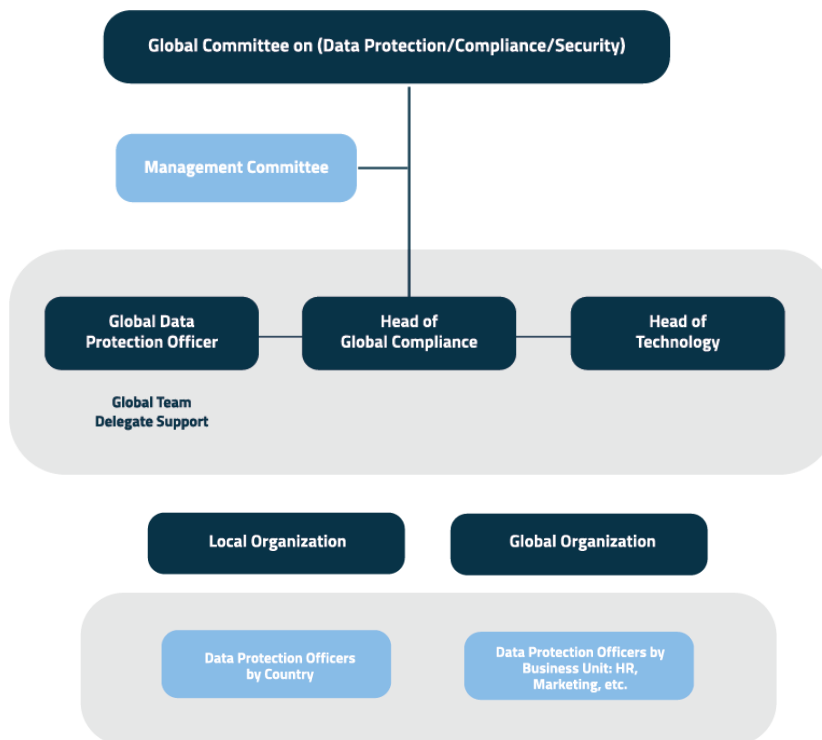


Figure 5. Privacy Governance Model – Multinational

## 6.5. Practical Challenges in Data Protection Governance

From what has been discussed so far, it is evident that implementing Data Protection Governance within organizations, both public and private, continues to face challenges common to other compliance areas. These include the positioning of the Data Protection Officer (DPO) and their relationship with roles such as the Compliance Officer or the CISO, within the company's organizational structure, often with unclear reporting lines and potentially dysfunctional governance bodies. Added to this is the uncertainty regarding the new responsibilities the DPO must assume with the entry into force and application of the Artificial Intelligence Regulation.

It is important to summarize the challenges related to the effective implementation and management of the data protection governance model:

### a) Data Protection Culture

One of the biggest challenges in recent years has been to implement a culture of data protection in all organizations. The challenge facing public and private entities subject to GDPR compliance, through their main

actors in this area, both the Data Protection Authority and the Data Protection Officer, can be broken down into two lines of action. The first is to **extend the culture of data protection to the entire organization**, being aware that its success will depend on choosing the governance model that best suits the characteristics of each entity, public and private, and the support that senior management offers to it; and second, to **educate all members of the organization in the culture of data protection compliance**, through awareness programs and good management of its policies in this area.

## **b) Support and Involvement of Senior Management**

Much is said about reporting to senior management, but little about the leadership it must exercise by providing the necessary resources (financial, human, and technological) and leading by example so that data protection is seen not only as a regulatory obligation but as a strategic and added value for the organization. This includes ensuring that effective policies are established, roles and responsibilities are clearly defined, and the interrelationships between individuals or teams involved in personal data processing are well understood, and that this model is explicitly communicated throughout the organization. This avoids ambiguity regarding who assumes responsibility for privacy governance, who makes decisions on data protection policies, and who bears the risks of non-compliance.

*“Active commitment from senior management is essential for the success of data protection governance, as its leadership and support in resource allocation, role definition, and promotion of a compliance culture ensure that data protection is perceived as a strategic value rather than merely a regulatory obligation. Without this backing, the DPO’s efforts may be limited or even ineffective.”*

In practice, the lack of senior management involvement often results in data protection being perceived as a purely bureaucratic task, undermining the adoption of best practices across the organization.

It is common for smaller organizations to exhibit less leadership and commitment, which places a greater burden on the DPO to establish the foundations for effective privacy governance within the organization.

## **c) Establishing Clear Guidelines, Responsibilities, and Objectives**

The lack of clarity in assigning roles and responsibilities related to data protection objectives can lead to ineffective management and compliance risks. It is essential that responsibilities are clearly defined and communicated throughout the organization. However, even when roles and responsibilities are well defined, many organizations often struggle to translate data protection principles and complex requirements into strategic guidelines that effectively integrate with their business objectives.

This challenge can also create tensions between regulatory compliance, the protection of individuals' rights, and other strategic priorities, resulting in data protection policies that are not uniformly implemented or understood across the organization. It is common, for example, for areas such as marketing to overlook fundamental principles or basic data protection requirements, perceiving regulatory demands as an obstacle to their core activities and business agility.

***“It is essential to clearly define and communicate roles and responsibilities throughout the organization, integrating data protection principles with business objectives.”***

Effective communication plays a critical role in ensuring that the entire organization understands the importance of data protection. However, messages often fail to reach all levels adequately. It is therefore necessary to tailor communication to different audiences and roles within the organization to achieve real impact.

Similarly, regarding role allocation, in smaller companies, it is common for the DPO to assume multiple responsibilities to maximize resources, which can lead to conflicts between their privacy oversight role and other operational roles. In such cases, the organization may struggle to ensure that the DPO acts with

#### **d) Integration into Operational Processes and Resource Allocation**

The effective implementation of data protection requirements and obligations must be embedded within internal processes. This can conflict with the rigidity of certain existing or new processes. It is therefore common for the DPO to be informed of changes or modifications to business processes to assess whether specific controls should be integrated to comply with current and applicable data protection regulations.

In practice, some companies still do not perform data mapping based on business processes, as they continue to rely on a file-based structure, which is simpler and easier to maintain.

***“The effective integration of data protection into operational processes requires adapting controls to current regulations, which can be hindered by the rigidity of certain processes and the lack of communication with the DPO.”***

On the other hand, the lack of resources affects not only the implementation of technical and organizational measures but also the ability to carry out training programs, audits, and impact assessments. As noted in previous sections, having an external DPO, an internal DPO, or an entire privacy department significantly impacts the budget and can define the scope of the governance model or privacy architecture to be developed.

A common reality in small and medium-sized enterprises, for example, is that they have all the required documentation prepared but not integrated into their processes, due to a lack of a compliance culture in data protection and limited resource allocation.

### **e) Risk Management, Assessment, and Documentation**

In such a dynamic environment, data protection risks have become increasingly significant due to the rise in cyberattacks. Conducting periodic assessments—ranging from basic risk analyses to more comprehensive evaluations such as Data Protection Impact Assessments (DPIAs)—and updating and implementing security measures can become an ongoing challenge, particularly for organizations with more complex structures.

In recent years, the implementation of preventive measures through incident and data breach response protocols has become standard practice and a fundamental tool. However, in some organizations, there is still a lack of awareness of these predefined processes due to insufficient staff training or education.

Finally, inadequate documentation management—not only regarding security breaches but in general—can lead to deficiencies in effective data protection governance. The goal is not to produce excessive documentation but to ensure that the documentation created serves to promote efficiency and continuous improvement in data governance.

***“Effective data protection management requires periodic risk assessments, preventive measures for incidents, and proper documentation that promotes continuous improvement.”***

### **f) DPO Functions in Artificial Intelligence**

With the recent entry into force of the Artificial Intelligence Regulation, the DPO’s functions must adapt to address the specific challenges associated with the use of AI technologies, as discussed in this document.

***“The DPO must adapt their functions to address AI-related risks, ensuring data protection, transparency in automated decision-making, and regulatory compliance throughout the entire lifecycle of AI systems.”***

For now, the DPO will continue to play a role in assessing data protection risks associated with algorithms and AI systems involving data processing, ensuring that appropriate measures are implemented to protect individuals' rights, such as transparency in automated decision-making and data minimization. Additionally, the DPO must coordinate and communicate with other teams to ensure compliance during the design phase (Privacy by Design, PbD) and throughout the lifecycle of AI systems. This also implies staying up to date with regulatory developments related to data protection.

# 7 MECHANISMS TO ENSURE INDEPENDENCE

Since the introduction of the General Data Protection Regulation (GDPR), the role of the Data Protection Officer (DPO) has evolved within organizations, becoming a key element in ensuring compliance with personal data protection regulations. However, one of the most debated and least understood principles of this role is its independence. This chapter delves into the need for such independence and the mechanisms that can guarantee it—not only as a formal requirement under the GDPR and the Spanish Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD), but as an essential foundation for the DPO to perform their duties effectively.

*“Independence is not merely a legal formality or another checkbox in compliance; it is a structural and functional requirement that ensures the DPO can carry out their responsibilities without interference.”*

This principle is enshrined in Articles 37, 38, and 39 of the GDPR, which outlines the DPO's framework of action, protecting them from conflicts of interest and undue influence.

However, while the concept of independence may seem straightforward in definition, in practice it presents a series of challenges that go beyond mere regulatory interpretation.

## The Legal Context: Regulation and Recent Case Law

The GDPR clearly defines the role of the DPO within the organization, assigning them a key position to ensure regulatory compliance:

- Article 38.3 stipulates that the DPO *must not receive instructions regarding the performance of their tasks and must report directly to the highest management level.*
- Article 38.6 allows the DPO *to perform other functions within the organization, provided these do not result in a conflict of interest.*

In this regard, two recent rulings by *the Court of Justice of the European Union (CJEU)* have been decisive: June 22, 2022, in the case *Leistriz AG vs LH (C-534/20)*<sup>9</sup> and February 9, 2023, in the case *X-FAB Dresden GmbH & Co. KG vs FC (C-453/21)*<sup>10</sup>.

<sup>9</sup>[TJUE de 22 de junio de 2022 en el caso Leistriz AG vs LH \(C-534/20\)](#)

<sup>10</sup>[TJUE de 9 de febrero de 2023 en el caso X-FAB Dresden GmbH & Co. KG vs FC \(C-453/21\)](#)



In both cases, the CJEU ruled on the interpretation of Article 38.3 of the GDPR, which applies “both to the DPO who is part of the controller’s or processor’s staff and to one who performs their duties under a service contract.” It confirmed that Member States may adopt stricter rules to protect the DPO’s position, provided these do not interfere with the objectives of the GDPR. The Court also emphasized that the independence of the DPO is not a mere formality: dismissal without just cause, even if not directly related to the performance of their duties, may contravene the GDPR if it jeopardizes their functional independence.

In Spain, Article 36.2 of the LOPDGDD reinforces this independence by stating that the DPO, when a natural person within the organization of the controller or processor, “may not be removed or penalized” for the performance of their duties, unless they have acted with intent or gross negligence in the exercise of their functions: “The independence of the Data Protection Officer within the organization shall be guaranteed, and any conflict of interest shall be avoided.” This protection is designed to enable the DPO to act impartially and with full autonomy.

## Why is DPO Independence Required?

The independence of the DPO is often considered a secondary attribute, subordinate to the organization’s operational functions. However, this perception is profoundly mistaken.

***“Independence is not an end in itself, but an indispensable means to ensure that the DPO can effectively perform the functions assigned by the GDPR without interference.”***

This independence must necessarily allow DPOs to exercise their functions in accordance with the GDPR’s objective, which is to guarantee a high level of protection for natural persons within the Union (CJEU, C-534/20). To this end, the DPO must audit, advise, and ensure that personal data processing is carried out in compliance with the principles of transparency, proportionality, and security. This implies that the DPO assumes a control role that, in many cases, may act as a “brake” on business practices that, without proper oversight, could infringe data subjects’ rights.

This supervisory role can create tensions with the organization’s commercial or strategic objectives, especially in first-line functions such as IT, Marketing, Finance, or even the Legal Department. If the DPO lacks sufficient independence, these tensions could translate into direct or indirect pressures that compromise their ability to act objectively and to advise and monitor compliance with data protection regulations as required by the GDPR.

## 7.1. Interference in the Performance of Duties

Another significant obstacle to DPO independence is direct interference from management. Although Article 38.3 GDPR prohibits DPOs from receiving instructions on how to perform their tasks, the 2023 survey conducted by the European Data Protection Supervisor (EDPS), **Results of the Survey on the designation and position of the data protection officer in the EU institutions, bodies, offices and agencies**<sup>11</sup>, revealed that, in many cases, DPOs reported having received guidance on how to interpret or apply the GDPR, thereby compromising their ability to act independently.

Such interference, whether subtle or explicit, undermines the DPO's role as a guarantor of legality and protector of data subjects' fundamental rights. For the DPO to effectively fulfill their obligations, they must be able to act without undue pressure and with the assurance that their recommendations will be valued and respected.

## 7.2. Practical Challenges to DPO Independence

Despite the clarity of the GDPR and LOPDGDD provisions, in practice, ensuring DPO independence can be a significant challenge, particularly in private companies where commercial pressures are intense. Some key issues affecting DPO independence include:

### 7.2.1. The DPO's Role in Safeguarding Corporate Sustainability

One of the greatest challenges to ensure DPO independence is cultural resistance within organizations. Many companies—especially in sectors where personal data is an essential raw material (such as marketing, technology, or finance)—tend to view the DPO role and personal data protection as a “technical” or “legal” function, a secondary regulation disconnected from business objectives or, in any case, subordinate to operational needs. This perception, besides being incorrect, compromises both the organization's regulatory compliance and its trust and legitimacy in today's market.

*“Far from being an obstacle to business interests, the DPO is a strategic asset that helps the company mitigate regulatory, financial, and reputational risks.”*

In an increasingly regulated environment with consumers aware of their rights, the DPO's role is not to block business but to guide and advise it so that the company's operations are carried out within legal boundaries, protecting data subjects' rights and avoiding sanctions and reputational damage that could be devastating. This, in turn, strengthens the trust of customer and business partner.

To change this perception, senior management must send a clear signal that compliance with data protection regulations is not a burden but an opportunity to differentiate and gain consumer trust. Business leaders

---

<sup>11</sup> [Results of the Survey on the designation and position of the data protection officer in the EU institutions, bodies, offices and agencies](#)

should be the first to understand and support the independence of the DPO, integrating this role into the company's overall strategy and ensuring that their recommendations are considered in key decisions.

Building a compliance culture requires continuous training, the dissemination of best practices, and transparent communication between the DPO and the various areas of the company. This culture should reinforce the concept that privacy is a business value and that the DPO is a key player in safeguarding this value.

An independent DPO can provide an objective view of the risks the organization faces, which is essential for strategic decision-making. For example, the DPO can anticipate issues that might otherwise lead to data breaches or sanctions, ensuring that the company maintains its integrity and reputation. In this way, the DPO becomes a protector not only of individual rights but also of the company's long-term sustainability.

For this function to be exercised effectively, the organization must recognize that the DPO cannot be treated like any other team member, subordinated to the interests of a specific department or management area. Their independence is crucial for acting as an effective counterbalance within the corporate governance structure, ensuring compliance with data protection regulations in a context where commercial incentives or operational efficiency might otherwise prevail.

### 7.2.2. DPO Reporting and Hierarchical Independence

To guarantee independence, the GDPR establishes that the DPO must report directly to the highest management level of the organization. In practice, many organizations still make the mistake of assigning the DPO to operational or business areas—the “first line of defense”—such as IT, Marketing, or Finance, which may be tempted to treat personal data as just another “commercial asset.” For these areas, data is essential for optimizing processes, segmenting customers, or creating new business opportunities. It is precisely in this context that the DPO must exercise their advisory and oversight role to ensure that the organization uses data in accordance with the principles of transparency, minimization, and proportionality established by the GDPR.

However, when the DPO reports hierarchically to these areas, their ability to act independently can be severely limited. The objectives of some first-line functions—such as maximizing efficiency and profits—may directly conflict with data protection principles. Areas like IT or Marketing may have incentives to exploit data to the fullest, even if this involves questionable privacy practices, such as mass data collection without a proper legal basis or processing personal data without informed consent.

The hierarchical dependence of the DPO on the first line of defense is not just a theoretical risk but a daily reality in many organizations. A common example is the management of security incidents involving personal data. Imagine a scenario where an organization suffers from an incident exposing customer data. The CIO and IT team might be tempted to downplay the incident to avoid regulatory or media repercussions. In such situations, the GDPR requires notification to both the supervisory authority and the affected individuals, but if the DPO reports to the CIO, their ability to fulfill this obligation objectively may be compromised. The CIO, concerned about sanctions or reputational damage, may pressure the DPO to avoid reporting the incident, which not only constitutes a GDPR violation but also jeopardizes the organization's long-term sustainability.

These situations are not uncommon and highlight the need for the DPO to be aligned with a different line of defense, one not directly involved in operational decision-making regarding data processing. The independence of the DPO goes beyond the formal question of “who signs their contract”; it is about ensuring they are not subordinated to areas whose interests may conflict with data protection principles.

A good practice in this regard, to enable the DPO to perform their role effectively, is aligning them with the “second line of defense,” where other control functions such as Compliance and Risk are located. These functions share the goal of monitoring and ensuring regulatory compliance without directly intervening in operational decisions that could compromise their objectivity and independence.

It is also advisable to establish Privacy Committees in which the DPO plays a prominent role and where potential conflicts of interest can be discussed and resolved. These committees, composed of members from different areas, ensure that decisions regarding data processing are made collectively and transparently, preventing the DPO from being isolated or pressured by specific commercial interests.

However, experience over the years shows that in certain complex organizations, placing the DPO within the first line of defense has also proven effective. This has been possible thanks to organizational synergies that have maintained the DPO’s functional independence in accordance with the GDPR. Therefore, determining the existence of conflicts of interest in such cases must be done individually, considering all relevant circumstances, the organizational structure of the controller or processor, and the applicable regulations, including the organization’s internal policies (CJEU, C-453/21, paragraph 45).

Although challenges remain in defining the ideal placement of the DPO, each organization must evaluate its governance model to ensure that the DPO can perform their duties with full autonomy and independence. As noted in the introduction to this second edition of the DPO White Paper, over the years we have learned much about different organizational models for the DPO: from internal structures to outsourcing or the creation of collegiate teams, with each organization finding its own way to ensure the effectiveness and independence of this role.

What is crucial is that, at the end of the day, the DPO can confirm that they maintain the essential characteristics of independence, as detailed in this chapter.

### 7.2.3. Conflict of Interest: A Constant Challenge

Conflict of interest is one of the most serious risks to the DPO’s independence. As stated in Article 38(6) of the GDPR, the DPO may perform other functions within the organization, provided these do not result in conflicts of interest. However, in practice, identifying and managing these conflicts can be complex, as roles and responsibilities within organizations often overlap.

A clear case of incompatibility arises when the DPO assumes responsibilities in the Legal department, where their role as an independent data protection supervisor may conflict with defense or legal advisory functions.

This conflict of interest was highlighted in a recent decision by the Spanish Data Protection Authority (AEPD, EXPEXP202211394, 2024), which emphasized that the DPO should not represent the organization in sanctioning proceedings or submit arguments in its defense, as this “implies active defense and a declaration of position.” The AEPD considers that there is a “conflict of interest, as the DPO cannot simultaneously inform and advise the controller and, at the same time, act in its defense. This duality of roles in the same person seriously compromises their independence and objectivity, which are fundamental pillars for the proper performance of their duties under current regulations.”

Similarly, conflicts of interest may arise when the DPO assumes additional functions in IT or Operations, areas where they may feel pressured to prioritize operational efficiency over the protection of data subjects’ rights, compromising their independence.

With the recent publication of the EU Artificial Intelligence Act, a new debate emerges regarding potential conflicts for the DPO in AI governance. It will be crucial to distinguish between regulatory governance of AI and its operational use within organizations. While some experts anticipate possible conflicts of interest, the AI Act—focused on risk management and regulatory compliance—should not create direct tension with the DPO’s current role. In contrast, other roles, such as the Chief Data Officer (CDO), focus on maximizing AI’s business value.

***“The DPO could play a key role in regulatory oversight without compromising their independence.”***

Therefore, supervisory authorities recommend structural separation between the DPO and these functions. In organizations where such separation is difficult, measures such as clearly defining responsibilities, establishing independent reporting channels to senior management, and conducting periodic internal audits are recommended to manage potential conflicts of interest.

In practice, while some organizations may achieve a degree of role compatibility, this often depends more on the DPO’s personal position and influence within the organization than on structural independence. Therefore, whenever structure and size allow, it is essential that the DPO’s functions and position within the organization are clearly differentiated.

***“Determining the existence of a conflict of interest under Article 38(6) of the GDPR must be carried out on a case-by-case basis, based on an assessment of all relevant circumstances, particularly the organizational structure of the controller or processor and in light of all applicable regulations, including their internal policies” (CJEU, C-453/21, paragraph 45).***

### 7.2.4. Resources and Training

Access to sufficient resources is another key aspect to ensure the DPO's independence. The GDPR requires that DPOs be provided with the resources necessary to perform their tasks, including staff, infrastructure, and access to continuous training. However, in many organizations, DPOs report lacking their own budget or the technical and human support needed to carry out their work effectively.

This lack of resources not only compromises the DPO's independence but also reduces their ability to implement the measures necessary to ensure compliance. This is especially critical in large organizations or those with complex data processing activities, where the volume of data and process complexity require rigorous oversight.

However, this responsibility does not rest solely on organizations. DPOs must also actively leverage the resources provided to them, particularly regarding training. It is important for DPOs to maintain a proactive approach to their professional development, seeking certifications that validate their knowledge, such as the AEPD's Certified Data Protection Officer credential, to strengthen their qualifications and credibility.

### 7.2.5. Lack of Integration into Critical Processes

DPOs are often excluded from key decisions involving personal data processing, limiting their ability to prevent risks. The lack of DPO involvement in processes such as Data Protection Impact Assessments (DPIAs) or security incident management is a recurring issue. According to the GDPR, the DPO must be consulted in a timely and proper manner on all matters relating to personal data processing, but in practice, this consultation is often insufficient or nonexistent.

## 7.3. Mechanisms to Ensure DPO Independence

The independence of the DPO cannot be guaranteed solely through hierarchical structure; it requires a proactive approach by organizations. They must implement mechanisms that reinforce this independence and protect the DPO from potential pressure or undue influence.

Below are some key mechanisms that should be considered:

### 1. Reporting to the Highest Level of the Organization

**The DPO must report directly to the highest level of management, such as senior leadership or the board of directors, without intermediaries. This ensures that their work is visible and has the necessary support to act independently.**

**This mechanism guarantees that the DPO's recommendations are heard and that they have the influence needed to impact the company's strategic decisions. Furthermore, direct reporting to the board or senior management prevents the DPO from being subordinated to the interests of specific operational areas that could conflict with data protection.**

### 2. Separation of Functions

The DPO should not have responsibilities involving decision-making on personal data processing. To avoid conflicts of interest, it is essential that the DPO's functions do not overlap with other operational responsibilities within the company. Internal policies should clearly identify roles incompatible with the DPO's responsibilities, ensuring they are not involved in decisions regarding personal data processing.

The GDPR allows the DPO to perform other functions, but these must not compromise their independence. This means organizations must ensure that the DPO does not hold roles in departments where pressure to maximize the use of personal data could conflict with the principles of minimization and lawful processing.

### 3. Adequate Resources and Budgetary Autonomy

Access to appropriate resources is a sine qua non condition for DPO independence. A lack of staff, infrastructure, or access to continuous training limits the DPO's ability to fulfill their responsibilities independently. Companies should ensure that the DPO has their own budget to access essential tools such as audit software, specialized training, and external services for audits or expert advice in key areas of data

protection. This budgetary autonomy is crucial to prevent the DPO from depending exclusively on other departments that may have different interests regarding personal data use.

Additionally, DPO incentives should be clearly aligned with data protection and compliance objectives, avoiding prioritization of economic or commercial interests—even indirectly—through performance targets or internal “clients.” Recommended objectives include effectiveness in managing data breach incidents, implementing preventive measures, and delivering high-quality privacy training to employees. To ensure incentives do not compromise independence, it is advisable for an audit or privacy committee to oversee their allocation, ensuring alignment exclusively with the data protection mission.

#### 4. Active Participation in Decision-Making Processes

The DPO must be proactively consulted on all relevant decisions affecting personal data processing. This includes conducting Data Protection Impact Assessments (DPIAs), managing security incidents and personal data breaches, and planning new technological projects involving large-scale data processing or technologies already impacting personal data—such as Artificial Intelligence. With the EU AI Act entering into force in 2024, the debate on the DPO’s role in this area is now active. Integrating the DPO into these processes from the outset not only ensures GDPR compliance but also enables the company to identify and mitigate risks in time, avoiding sanctions or reputational damage.

#### 5. Policies and Transparency

Organizations must clearly document the DPO’s roles and responsibilities, as well as procedures to prevent conflicts of interest. This documentation should be reviewed periodically to ensure the DPO can act with the autonomy required by the GDPR.

Organizations should establish clear procedures for the DPO to submit periodic reports on compliance status and risk areas, promoting transparency. This reinforces the DPO’s visibility within the organization and ensures their work aligns with corporate objectives without compromising independence.



## 6. Privacy Committees

Creating dedicated privacy committees or multidisciplinary working groups (such as AI governance technical offices) can be an effective tool to strengthen the DPO's independence. These committees can serve as a forum to discuss and resolve potential conflicts of interest, as well as support the DPO in making strategic decisions related to data protection.

These committees also ensure that senior management is informed of the DPO's concerns and facilitate collective decision-making, preventing the commercial interests of specific departments from prevailing over legal obligations.

## 7. Independent Audits

Conducting external audits on the DPO's functioning and level of independence can help identify potential weaknesses in the organizational structure and propose solutions to improve the DPO's autonomy.

## 8. Protection Against Unjustified Dismissal

Finally, the DPO's independence cannot be effective without protection against sanctions or unjustified dismissal for performing their duties. Article 38(3) of the GDPR states that the DPO cannot be dismissed or penalized for fulfilling their obligations. However, in practice, some DPOs have reported pressure to relax oversight or downplay risks, especially when these conflicts directly affect the company's commercial interests.

To ensure real independence, organizations must create an environment where the DPO can act without fear of retaliation and where their oversight role is valued and supported by senior management. This protection should also be formalized in internal policies that clearly define the DPO's responsibilities and rights and establish an internal review mechanism in case of disputes regarding their performance.

In its judgment of June 22, 2022 (Leistriz, C-534/20, EU:C:2022:495, paragraphs 20 and 21), the CJEU, after noting that the GDPR does not define the concepts of "dismissed," "penalized," and "for performing their tasks" in Article 38(3), emphasized that "according to its ordinary meaning, the prohibition imposed on the controller or processor from dismissing or penalizing a data protection officer means that the officer must be protected against any decision that terminates their functions, is unfavorable to them, or constitutes a sanction." Such a decision may include the removal of a DPO by their employer, resulting in the termination of their functions within the controller or processor. (CJEU judgment of February 9, 2023, X-FAB Dresden GmbH & Co. KG vs FC (C-453/21), paragraphs 21 and 22).

Article 38.3, second sentence, of the GDPR, “by protecting the data protection officer against any decision that terminates their functions, is unfavorable to them, or constitutes a sanction when such decision is related to the performance of their tasks, must be regarded as primarily intended to preserve the functional independence of the data protection officer and, therefore, to ensure the effectiveness of the GDPR provisions” (judgment of June 22, 2022, Leistritz, C-534/20, EU:C:2022:495, paragraph 28).

## 7.4. Independence of the DPO and Decisions by Data Protection Authorities

The independence of the DPO is a crucial element to ensure compliance with data protection regulations. However, guaranteeing this independence is not an easy task, as it requires a cultural shift within organizations, where operational areas understand that the DPO’s role is not a hindrance but a guarantee of the company’s long-term sustainability and legitimacy. And, as previously referenced from the CJEU, each case must be assessed “on a case-by-case basis, based on an evaluation of all relevant circumstances, in particular, the organizational structure of the controller or processor and in light of all applicable regulations, including their internal policies.”

Challenges to the DPO’s independence—such as conflicts of interest, lack of resources, or interference from senior management—must be addressed through clear mechanisms that reinforce autonomy.

Organizations that fail to take the DPO’s independence seriously risk compromising both regulatory compliance and their reputation. In an environment where privacy rights are increasingly valued, having an independent DPO is not only a legal obligation but also a competitive advantage that can make the difference between a company that thrives in the long term and one that faces sanctions and loss of customer trust.

This independence does not mean that the DPO cannot be subject to oversight or even dismissed. As clarified by the CJEU in the rulings repeatedly referenced throughout this chapter, “the enhanced protection of the DPO must not jeopardize the achievement of the GDPR’s objectives.” This would be the case “if it prevented any dismissal by a controller or processor of a DPO who no longer possesses the professional qualities required to perform their duties,” in accordance with Article 37(5) of the GDPR, or “who fails to comply with the provisions of that Regulation” (see, in this regard, the judgment of 22 June 2022, Leistritz, C534/20, EU:C:2022:495, paragraph 35).

It is essential for companies to implement the necessary mechanisms to ensure that the DPO can perform their role without interference, with full access to senior management and the necessary support to act objectively.

***“The independence of the DPO is ultimately a safeguard for the organization itself, protecting it from the risks associated with the misuse of personal data and ensuring that its practices align with the ethical and legal principles governing data processing today.”***

### 7.4.1. Regulation of the DPO under the GDPR and LOPDGDD

The **General Data Protection Regulation (GDPR)** establishes in **Articles 37, 38, and 39** the obligations relating to the Data Protection Officer (DPO), regulating their designation, position within the organization, functions, and resources. Failure to comply with may constitute an infringement subject to penalties under **Articles 83.4 and 83.2 of the GDPR**.

In Spain, **Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)** complements the GDPR and regulates specific aspects of the DPO, also establishing a national sanctioning regime.

### 7.4.2. Infringements Related to the DPO under the GDPR and LOPDGDD

#### GDPR:

- **Article 37. Designation of the DPO:** Failure to appoint a DPO when mandatory constitutes a serious infringement. The GDPR sets specific criteria to determine when such designation is required, both in the public and private sectors.
- **Article 38. Position of the DPO:** Situations that compromise the **DPO's independence**, such as lack of support in performing their duties, absence of adequate resources, or the imposition of instructions that may influence their decisions, are considered infringements.
- **Article 39. Functions of the DPO:** Failure to fulfill the functions assigned to the DPO, including monitoring compliance, staff training, and cooperation with the supervisory authority, also constitutes an infringement.

#### LOPDGDD:

- **Article 34. Designation of a DPO:** Reinforces the obligation to appoint a DPO in specific cases in Spain, expanding the GDPR criteria, for example, for professional associations, online gambling operators, or entities processing large volumes of sensitive data.
- **Article 65. Infringements:** Infringements related to the DPO are classified as **minor, serious, or very serious**. Failure to appoint a mandatory DPO, lack of cooperation with the supervisory authority, or failure to communicate the appointment are considered **serious** or even **very serious** infringements, depending on the circumstances.

### 7.4.3. Sanctioning Regime under the GDPR and LOPDGDD

#### GDPR:

- **Article 83.4 (a):** Infringements of Articles 37, 38, and 39 may result in administrative fines of **up to €10 million** or, in the case of an undertaking, **up to 2% of the total worldwide annual turnover** of the preceding financial year, whichever is higher.
- **Article 38.2:** Establishes the **criteria for determining the amount of the fine**, including the nature, gravity, and duration of the infringement, whether it was intentional or negligent, measures taken to mitigate damage, and the degree of cooperation with the supervisory authority.
- **Article 58.2:** In addition to financial penalties, supervisory authorities may impose corrective measures such as **warnings, reprimands, or orders to remedy non-compliance**.

#### LOPDGDD:

- **Article 71 – Classification of Infringements.** Infringements are classified into three levels:
  - o **Very serious:** Fines of **up to €20 million or 4% of the total worldwide annual turnover** (as applicable under the GDPR).
  - o **Serious:** Fines of **up to €10 million or 2% of the total worldwide annual turnover**.
  - o **Minor:** Lower financial penalties or warnings, especially in the case of public administrations.
- **Article 77 – Regime applicable to Public Administrations:** For public administrations, the LOPDGDD provides for non-financial sanctions, such as warnings or corrective measures, since **financial penalties** are generally not imposed on public entities.

### 7.4.4. Decisions by Supervisory Authorities

Including these decisions in the analysis helps to better understand the **limits and obligations** established by the GDPR and the LOPDGDD, as well as the **legal consequences** of non-compliance.

*“Decisions issued by supervisory authorities, although still limited in number, show a growing trend to protect the role of the DPO and sanction practices that compromise independence, resources, and the absence of conflicts of interest in the performance of their duties.”*

### 7.4.4.1 AEPD Decisions

Although the AEPD has not been particularly active in imposing sanctions for breaches of **Articles 37, 38, and 39 of the GDPR**, there are some significant decisions addressing key aspects related to the independence and functions of the DPO:

- **Failure to appoint a mandatory DPO:** The AEPD has frequently issued warnings to a large number of public administrations. Regarding sanctions on private entities for this reason, case **PS/00140/2022**<sup>12</sup> stands out, where a fast-food restaurant chain was fined €20,000 for failing to appoint a DPO when, in the agency's view, the chain processed personal data that, due to its nature, scope, and/or purposes, required regular and systematic monitoring of data subjects on a large scale. Although the company argued that its activity did not require mandatory appointment of a DPO, the AEPD considered that the large-scale marketing activities carried out by the chain were inseparable from its core business, making the appointment mandatory.
- **Conflicts of interest:** Regarding incompatibility of functions and conflicts of interest, the AEPD has not issued many sanctioning decisions on this matter. One notable case is the decision on the appeal filed by the State Secretariat for Security against **PS/382/2023**<sup>13</sup>, where the AEPD stated that submitting arguments in the context of a sanctioning procedure by the DPO represents a conflict of interest and compromises their independence, as it implies active defense in sanctioning proceedings, which is incompatible with their internal advisory role. In this case, the AEPD argued that the controller also has the capacity to manage communications with the AEPD and cannot delegate administrative functions that jeopardize the DPO's impartiality. The Agency concluded that the DPO's actions constituted a substantive infringement due to the lack of independence and objectivity, as the DPO cannot simultaneously advise and defend the controller, as this compromises independence and objectivity.

---

<sup>12</sup>[\*Procedimiento N.º PS/00140/2022.\*](#)

<sup>13</sup>[\*Resolución de Recurso de Reposición\*](#)

### 7.4.4.2 Decisions by Other European Supervisory Authorities

- **BELGIUM.** In 2020, the Belgian Data Protection Authority [Autorité de protection des données – APD / Gegevensbeschermingsautoriteit – GBA<sup>14</sup>], imposed a fine of **€50,000** on a company for violating Article 38(6) of the GDPR. The main reason was that the DPO simultaneously held roles as a hierarchical superior or head of other departments within the organization (compliance, risk management, and internal audit). These roles granted decision-making power over the purposes and means of processing within the respective departments.

In this context, the fact that the DPO had decision-making authority over certain processing activities prevented them from performing their data protection oversight duties independently, resulting in a conflict of interest as prohibited by the regulation, despite the company's arguments that these positions were merely advisory.

The Belgian authority concluded that independence cannot be guaranteed when the same person not only belongs to a specific department but is also responsible for advising it while acting as DPO—especially when there is no evidence of measures implemented to prevent the conflict of interest.

The same authority also determined in 2021<sup>15</sup> that a conflict of interest existed when a person simultaneously held the roles of DPO and Head of Operational Risk Management.

- **CROATIA.** In September 2023, the Croatian Personal Data Protection Agency [Agencija za zaštitu osobnih podataka – AZOP] imposed a fine of **€15,000**<sup>16</sup> on a hotel group for appointing the **hotel director as DPO**. This situation created an inherent conflict of interest due to the **incompatibility between operational management** and the DPO's supervisory functions. In this case, the hotel director and the DPO were responsible both for making management decisions regarding data processing and for ensuring compliance with those processing activities, which is clearly incompatible (Article 38.6 GDPR).

- **ITALY.** In April 2024<sup>17</sup>, the **Italian Data Protection Authority (Garante per la Protezione dei Dati Personali)** issued a decision regarding DPO incompatibilities, imposing a sanction on a public entity for appointing a DPO who simultaneously held other professional roles, such as Head of several services within the organization (Director's Secretariat for Sector I, Assistance to Bodies, Information Systems, Tourism, and ultimately the Legal Service).

In this case, the Garante concluded that the appointed DPO, by holding multiple positions, lacked the necessary resources—particularly time—and was potentially in a situation of conflict of interest, which violated Article 38.2 and Article 38.6 of the GDPR.

---

<sup>14</sup> [APD/GBA \(Belgium\) - 18/2020](#)

<sup>15</sup> [APD/GBA \(Belgium\) - 141/2021; Dossiernummer: DOS-2020-03763](#)

<sup>16</sup> [AZOP \(Croatia\) - Decision 26-09-2023](#)

<sup>17</sup> [Garante per la protezione dei dati personali \(Italy\) - 10013391](#)

- **LUXEMBOURG:** It is worth highlighting, the ruling of the **High Court of Luxembourg**<sup>18</sup> (equivalent to the Spanish Supreme Court), which addresses the role of the DPO within a corporate group. In this case, the court upheld a fine of €18,000 imposed by the Luxembourg Data Protection Authority (CNPD) on a company for failing to directly involve its DPO in data protection matters and for not providing sufficient resources.

The company was part of a group that had appointed a single DPO for all its entities (in accordance with Article 37.2 of the GDPR) and a local lawyer as the point of contact in Luxembourg. A Data Protection Committee was created in Luxembourg, but the DPO was not a member and only received information through meeting minutes and questions from the local contact point. In fact, the DPO only intervened when a data subject was dissatisfied with the response provided by the local contact point.

The company also failed to demonstrate that the DPO had been consulted in advance regarding the establishment of the specific Data Protection Committee in Luxembourg. The only person with data protection responsibilities in Luxembourg was the company's lawyer, which limited their ability to properly support the DPO. Given the size of the company (70 locations, between 1,600 and 2,100 employees, and 25,000 daily customers), it was necessary to have at least one full-time professional dedicated to data protection.

Also in Luxembourg, the DPA<sup>19</sup> considered that the DPO was involved in tasks that could result in a conflict of interest by overlapping their role with that of Head of Compliance. In this case, the DPO participated in determining and implementing personal data processing as part of their duties as Head of Compliance and was therefore required to assess data processing practices they had themselves implemented. None of the measures adopted by the controller to mitigate the risk of conflict of interest (such as requiring that any processing involving a potential conflict be approved by the DPO's superior) were deemed sufficient.

---

<sup>18</sup> [TADM - 46401](#)

<sup>19</sup> [CNPD \(Luxemburgo\) - Délibération n° 37FR/2021 - GDPRhub](#)



# THE DPO PROFILE

## 8.1. Legal Framework

Once appointed, Article 38.1 of the GDPR and Article 44.1 of the GDPR require controllers and processors to keep the DPO “involved, properly and in a timely manner, in all issues relating to the protection of personal data.” Article 38.2 of the GDPR and Article 44.2 of the GDPR oblige controllers and processors to “support” the DPO by “providing resources” for their tasks, and Article 38.3 of the GDPR and Article 44.3 of the GDPR require that the DPO act independently of the influence of controllers and processors.

Article 39 of the GDPR and Article 45 of the GDPR set out a series of tasks for the DPO, including monitoring and advising on GDPR compliance and cooperating with supervisory authorities. DPOs are also intended to be visible figures who can interact with data subjects; Articles 13.1(b), 14.1(b), and 37.7 of the GDPR, as well as Articles 15.1(b), 16.1(b), and 43.3 of the GDPR, require controllers to make the DPO’s contact details available so they can be reached when necessary.

EU data protection law also provides flexibility to adapt the appointment and functioning of the DPO to the specific needs of the controller or processor, considering the complexity of their personal data processing. Under Article 38.6 of the GDPR and Article 44.6 of the GDPR, the role may be combined with other duties (provided these do not result in a conflict of interest), and under paragraph 3 of both provisions, the DPO “shall report directly to the highest management level of the controller or processor.”

Additionally, Articles 37.2 and 37.3 of the GDPR, and Article 43.2 of the GDPR, allow multiple controllers or processors (whether companies or public bodies under the GDPR or EU institutions under the GDPR) to designate a single DPO, provided all can easily access them. Meanwhile, Article 37.6 of the GDPR and Article 43.4 of the GDPR state that a DPO does not necessarily have to be a full-time staff member and may instead perform their duties under a service contract.

It is important to note that the GDPR does not treat these two options equally, as Article 43.4 specifies that the DPO should be a staff member of the EU institution; only when



considering its size, and if the option of sharing a DPO with another EU institution is not exercised, may an EU institution appoint a DPO under a service contract. These provisions are particularly useful for smaller controllers and processors that wish to employ a DPO but lack the resources to hire a dedicated, permanent staff member. However, even when the DPO has other functions or works part-time, their tasks remain the same, and controllers and processors must ensure they provide sufficient time, training, and resources for the DPO to perform their role effectively.

The GDPR sets out the conditions under which a DPO must be appointed, but controllers or processors may also choose to appoint one voluntarily. As a compliance method, this can be extremely useful; having a data protection expert involved in planning and decision-making processes helps not only with the accountability principle under Article 5.2 of the GDPR but also with the obligation under Article 24.1 to implement appropriate technical and organizational measures to ensure GDPR compliance, as well as the obligations under Article 25 on data protection by design and by default, among many others.

## 8.2. Qualifications

The DPO must be appointed based on their professional qualities and their expert knowledge of data protection law and practices and their ability to fulfill the tasks assigned by the GDPR, which we will review in the next section.

The Article 29 Working Party (WP29) notes that the level of expertise should be determined according to the data processing operations carried out (sensitivity, complexity, and volume of data processed) and the level of protection required for the personal data processed. The DPO should have a deep understanding of the Regulation, the sector, and the organization's business (especially when it relies on personal data processing) to facilitate innovation and competitiveness while ensuring the fundamental right to data protection.

The Confederation of European Data Protection Organizations (CEDPO) emphasizes that specialized legal knowledge should not be exclusive to law graduates; such knowledge can be held by both legal and technical profiles.

## 8.3. Professional Experience

The DPO should have proven and recognized knowledge and experience in the following areas:

### a) Legal Knowledge of Data Protection Regulations

Familiarity with regulations and provisions affecting their professional field or business sector related to data protection:

- Fundamental rights and the EU Charter of Fundamental Rights, with reference to the fundamental right to personal data protection.

- Basic principles of the GDPR and local data protection laws.
- Legal bases for processing personal data.
- Data protection requirements when using ICT.

## b) Knowledge in Information Security and ICT

The DPO should have basic technical knowledge and understand issues related to information technologies and security measures affecting systems:

- Organization of the ICT environment.
- System structures, applications, and IT processes.
- Understanding data flows, including systems where personal data processing occurs.
- Information security management based on confidentiality, integrity, availability, and resilience objectives.
- Identification of risks to data subjects arising from ICT systems, applications, and processes.
- Development of security controls and measures applicable to information systems to protect personal data.

## 8.4. Personal Skills

In addition to specialized knowledge of data protection, the DPO's soft skills are crucial. These types of social skills, key skills, or meta-skills have the common denominator of being "cross-cutting" and essential skills for any DPO, especially considering their position in the organization and the functions assigned to them.

These types of skills, some innate and others learned, are related to the personal skills that each individual possesses and manages in their own way, differentiating them from others in their character and behavior. Thus, we can talk about the following types of skills:

1.

**Introspective skills:** managing emotions, overcoming limiting beliefs, identifying strengths and areas for improvement, increasing self-awareness, and self-efficacy.

2.

**Diagnostic and action skills:** problem-solving, resource assessment, creativity, adaptability to new situations and major changes, flexibility, initiative, planning, time management.

## 3.

**Relational skills:** empathy, active listening, assertiveness, effective communication, conflict management, negotiation and consensus-building, teamwork, and leadership.

Without a doubt, these types of skills help in the daily work of a DPO and should gradually be included in the training required at school, university, and professional levels. There is no doubt that if we refer to the “three lines of defense” model and the position statement on this subject by the Institute of Internal Auditors, we can see very clearly the relationship that a DPO has to establish both with the more operational side of the business and with the internal audit side.

In this sense, the ability of a DPO to coordinate and interact with areas such as compliance or information security, as well as with other departments such as IT, HR, marketing, development, innovation, etc., is largely determined by the aforementioned soft skills.

Similarly, in addition to being independent and having sufficient “authority” within their organization, a DPO must be a person with a high degree of professional and personal ethics, integrity (without having been subject to sanctions for breaches of confidentiality, data protection regulations, or convicted of crimes, especially computer crimes or disclosure of secrets), assertive, able to delegate, and with communication skills (opinions, positions, understanding of the business and the different interests at stake) and problem-solving skills.

Once again, we see that having a legal or technical profile does not in itself mean that one has or possesses the aforementioned skills, so a DPO can have either a legal or technical profile.

## 8.5. Training

Continuous training and ongoing knowledge updates (legal and case law changes, new technologies, technical developments) are essential for the DPO.

The WP29 considers it crucial for data protection authorities to promote adequate and regular training for DPOs, as the Spanish Data Protection Authority (AEPD) has done by approving the DPO Certification Scheme, which outlines the competencies required for this role.

## 8.6. Duty of Confidentiality

According to Article 38.5 of the GDPR, the DPO—whether with a legal or technical profile—is obliged to maintain secrecy or confidentiality regarding the performance of their duties, in accordance with EU or Member State law.

## Challenges and Obstacles

In their interaction with other areas of the organization, the DPO may face a wide range of challenges depending on the organization's level of maturity regarding its data protection culture. In organizations where privacy and data protection are not among the top priorities, the DPO may perceive an initial lack of commitment that creates significant barriers to performing their duties.

Often, these organizations view privacy regulations as an additional burden rather than an opportunity to build customer trust or improve competitiveness in the market. In this context, the DPO may experience a lack of explicit support from senior management or passive resistance from other key areas that do not see the added value of investing time and resources in regulatory compliance.

Resistance to changes in organizational practices is one of the most common obstacles any DPO faces. This resistance can arise from various fronts: from lack of resources to the perception that proposed measures will interfere with operational efficiency or innovation. Frequently, the existing organizational culture does not sufficiently value privacy, and in some cases, there may be a lack of awareness about potential sanctions or the legal implications of non-compliance with data protection regulations.

It is in this scenario that the DPO must deploy not only technical knowledge but also negotiation and mediation skills. The key is to present compliance not as an imposition but as a process that can be harmoniously integrated with the organization's strategic objectives. This approach involves identifying risk areas and proposing measures that not only mitigate these risks but also add value, such as improving process efficiency or increasing customer trust.

In more advanced organizations, where data protection is already part of the organizational culture, the challenges are different but no less significant. Here, the DPO may find a more collaborative work environment where areas are more familiar with privacy and security principles. However, the DPO must be prepared to manage new complexities, such as the need to stay up to date in a constantly evolving regulatory landscape and with emerging, rapidly developing technologies like artificial intelligence.

## Best Practices:

The success of the DPO in their relationship with the different areas of the organization is intrinsically linked to their ability to build and maintain strong alliances. These alliances are based not only on the DPO's technical credibility but also on their ability to foster consensus and promote a proactive compliance culture. Below are three key aspects that the DPO can implement to improve their effectiveness and relationships within the organization:

### 1.

#### Clear and Tailored Communication

One of the most critical skills for the DPO is the ability to communicate clearly and accessibly. The technical and legal nature of data protection can be complex for many within the organization, from employees handling data in their daily tasks to senior executives. Therefore, it is essential that the DPO is not only an expert with deep knowledge of the regulations but also capable of conveying them in an understandable and contextualized way, adapting the message to each audience. The DPO's success largely depends on their ability to make technical and legal aspects accessible to everyone, thereby fostering a culture of data protection throughout the organization.

The legal and technical language associated with data protection can be dense and difficult to grasp for those unfamiliar with these concepts. However, data protection is not just a matter for legal or IT experts; it is a shared responsibility across the organization. From customer service staff handling user contact information to HR teams managing sensitive data, everyone must understand how to apply data protection principles in their daily work.

This is where the DPO must act as a translator. Their role is not simply to recite legal provisions but to ensure that each area of the organization understands what those requirements mean in practical terms for their activities. This requires not only a deep understanding of the law but also the ability to simplify and tailor the message so that it is relevant to each team or individual.

The first step toward effective communication is understanding the audience. Different levels and areas within an organization require different communication approaches. For example, an IT team managing security and data storage systems will need detailed information on specific security requirements, such as encryption, authentication, and access management. On the other hand, the marketing team may need guidance on how to obtain and manage user consent for the use of personal data.

For senior management, the DPO should not focus on technical details but on the strategic and financial risks of non-compliance. This includes potential fines, reputational implications, and the long-term benefits of adopting a strong data protection culture. Conversely, when dealing with operational teams, communication should be more practical, explaining the procedures to follow in specific situations, such as handling access or rectification requests.

It is also essential to foster two-way communication within the organization. This is not just about delivering instructions or recommendations but about creating an environment where different areas can ask questions, raise concerns, and share experiences related to data protection. By promoting this type of open dialogue, the DPO can identify potential areas of confusion or practices that need improvement. To achieve this, the DPO can establish accessible communication channels, such as a dedicated mailbox or FAQs.

Another critical aspect of clear communication is simplifying data protection policies and procedures. Policy documents are often lengthy, full of technical terms, and written in a way that employees cannot easily understand what is expected of them. The DPO should review and simplify these documents, removing unnecessary jargon and clearly explaining the steps to follow. Additionally, they can create executive summaries or quick-reference guides highlighting the most important points, so employees have an easy resource to consult when needed. This is especially useful in operational situations where employees may have little time to read lengthy documents.

For example, a quick guide on “What to Do in Case of a Data Breach” with clear, direct steps can be far more effective than a 30-page policy. By simplifying procedures, the DPO ensures compliance is more accessible, and employees are better prepared to act correctly when necessary.

## 2.

### Influence and Negotiation Skills

One of the most relevant skills a DPO must develop is the ability to influence and negotiate. Often, the DPO does not have direct hierarchical authority over the different departments within the organization, which means their effectiveness depends on their ability to persuade and negotiate effectively. This skill is essential to ensure that business areas adopt and implement the necessary measures to comply with data protection regulations without creating unnecessary friction or being perceived as an obstacle to operations and business objectives.

By definition, the DPO is an independent role within the organization. This means that, although they are responsible for advising, monitoring, and ensuring regulatory compliance, they do not always have the power to make operational decisions or enforce changes.

In organizations where the data protection culture is not fully developed or where compliance is perceived as an administrative burden, the DPO may face resistance or, at best, indifference from other key stakeholders. Therefore, their ability to negotiate agreements, build trust, and promote cross-functional collaboration is essential for success.

The DPO's influence should not rely solely on regulatory pressure but on their ability to raise awareness among other areas about the benefits of data protection. Their authority comes from their specialized knowledge and their ability to translate that knowledge into tangible benefits for the organization.

To exert effective influence, the DPO must clearly and accessibly communicate how compliance not only protects the organization from sanctions and legal risks but also enhances customer trust, improves operational efficiency, and strengthens the company's reputation. This approach requires the DPO to have a deep understanding of both the regulations and the organization's processes and priorities, so they can align their recommendations with the company's strategic objectives.

For example, in an organization that prioritizes customer experience, the DPO could argue that implementing robust data protection measures not only ensures compliance but also improves consumer trust and, ultimately, brand loyalty. This type of value-driven argument is often more effective than simply insisting on the need to comply with the law.

In this process, the DPO must also be prepared to manage potential conflicts between business objectives and regulatory requirements. For instance, if a business unit pushes to use personal data for commercial purposes that do not meet data protection requirements, the DPO must stand firm, defending individuals' rights and data protection principles while proposing alternative solutions that allow business goals to be achieved without compromising compliance. The message should not be "this cannot be done," but rather "this must be done differently."

The DPO's influence is strengthened when they foster a culture of collaboration within the organization. Instead of being seen as an external enforcer for imposing rules, the DPO should position themselves as an ally who facilitates departmental work by providing solutions that simplify compliance.

This collaboration can be encouraged by creating regular communication channels between the DPO and different teams to discuss issues, clarify doubts, and work together on implementing solutions. Setting up periodic meetings with department heads to review compliance status can be a very useful tool. The DPO must ensure their approach is proactive, not merely reactive to problems.

It is also important for the DPO to promote the idea that compliance with data protection regulations is a shared responsibility across the organization, not just the responsibility of their department. Encouraging ownership of compliance at the departmental level, by appointing privacy champions in each area, can facilitate communication and the implementation of corrective measures when necessary.

### 3.

#### **Business and Industry Knowledge**

The DPO should position themselves as a facilitator who actively collaborates with different areas of the organization to ensure that compliance with data protection regulations is not perceived as an imposition but as an element that strengthens efficiency, innovation, and business competitiveness.

A deep understanding of the business and the industry in which the organization operates will enable the DPO to adapt their recommendations and compliance measures to the company's operational reality. This minimizes process disruptions and integrates data protection measures into the organization's structure and culture.

One of the DPO's first tasks should be to become familiar with the organization's strategic objectives. In other words, they must understand the company's mission, business priorities, products or services offered, markets and customers, as well as the challenges and opportunities it faces. With this understanding, the DPO can tailor their compliance approach to align with the context in which the organization operates and in which its various areas function.





# THE DPO IN THE REGULATORY FRAMEWORK OF ARTIFICIAL INTELLIGENCE

## 9. 1. Introduction

The recently published Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (**hereinafter, the “Artificial Intelligence Regulation” or “AI Act”**) has sparked debate in professional and academic circles regarding its application in many areas. For data protection professionals, one of the most discussed topics is undoubtedly the role of the Data Protection Officer (DPO) and what their responsibilities should be under this new regulation.

Data protection authorities, for their part, have so far published guidelines addressing how this technology should comply with the General Data Protection Regulation (GDPR) when personal data processing involves AI or when the development of the technology itself entails data processing.

Artificial intelligence—like other technologies—is considered, in the context of data protection, as another tool available to controllers and processors, who must decide whether and under what conditions to incorporate it into their processes.

With the AI Act now published and during its grace period for implementation, the compliance roadmap for these systems is clear, whether or not they use personal data, as well as the cross-cutting measures organizations must adopt to analyze, detect, and mitigate associated risks.

As for the DPO, it is important to note that the AI Act does not establish or define an equivalent role—unlike the GDPR, which does so in detail in Articles 37 (designation), 38 (position), and 39 (tasks).

In this context, in Section 7 of this Guide, we will outline the key considerations that organizations should evaluate to determine whether to assign new responsibilities related to Artificial Intelligence to the DPO—and, if so, which ones. To this end, the following

sections address the main obligations under the GDPR as well as the AI Act and, for each, analyze the feasibility of complementing the processes established for GDPR compliance to ensure compliance with the AI Act.

Before addressing these obligations, we will review the **definition of the DPO's role under the GDPR** and two cross-cutting issues that we believe impact this entire analysis: the alignment of **objectives and the complementarity of the regulatory texts (GDPR and AI Act)**.

## 9. 2. Defining the DPO's Role in Data Protection Law

Before determining which roles and responsibilities can be assigned to the DPO in the context of AI, we must first consider the functions that data protection law attributes to this role. This is essential to assess whether assigning additional responsibilities under a third regulation (the AI Act) is compatible and desirable or, on the contrary, could create a conflict of interest.

In this regard, let us recall that Article 39 of the GDPR assigns the **DPO the following tasks**:

- **Informing and advising** the controller on their obligations under data protection law, including the methodology to follow when conducting a Data Protection Impact Assessment (DPIA).
- **Monitoring** compliance with this regulation.
- **Providing advice** on DPIAs and overseeing their implementation, including whether the DPIA has been properly carried out.
- **Cooperating** with the supervisory authority and acting as a point of contact.

Additionally, Article 38 of the GDPR establishes that:

- Data subjects may contact the DPO regarding all issues related to the processing of their personal data and the exercise of their rights.

## 9.3. Common Objectives of the Data Protection and Artificial Intelligence Regulatory Frameworks

According to Article 1(2) of the GDPR:

- *"[...] This Regulation **protects the fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data.**"*

Article 1 of the AI Act states:

- *"[The objective of this Regulation is to improve the functioning of the internal market and promote the adoption of human-centric and trustworthy artificial intelligence (AI), while ensuring a **high level of protection of health, safety, and fundamental rights enshrined in the Charter, including democracy, the rule of law, and environmental protection**, against the harmful effects of AI systems (hereinafter, 'AI systems') within the Union, as well as supporting innovation.]"*

From the wording of the cited articles and the practical experience accumulated under the GDPR—along with decisions by data protection authorities and the Court of Justice of the European Union—it is clear that both the GDPR and, prospectively, the AI Act establish obligations and mechanisms to safeguard the rights enshrined in the EU Charter of Fundamental Rights.

This has been demonstrated by the practice of data protection authorities at both national and European levels and is clearly explained by Alessandro Mantelero and Maria Samantha Esposito in their article *An Evidence-based Methodology for Human Rights Impact Assessment in the Development of AI Data-Intensive Systems*, where they use these decisions as a basis for understanding how artificial intelligence can affect fundamental rights<sup>20</sup>.

## 9. 4. GDPR and AI Act: Complementarity of the Legal Texts

A joint reading of both regulations—particularly the recitals of the AI Act—leads to the conclusion that there is regulatory complementarity.

According to Recitals 9 and 10 of the AI Act, its provisions:

- *“[...] should be understood without prejudice to existing Union law, in particular in the areas of data protection, consumer protection, fundamental rights, employment, worker protection, and product safety, which this Regulation complements.”*
- *“[...] should facilitate effective enforcement and enable the exercise of rights and other remedies guaranteed by Union law on the protection of personal data, as well as other fundamental rights.”*

This complementarity and the instrumental role of the AI Act in supporting GDPR compliance are detailed throughout the AI Act, for example, in relation to definitions or concepts such as profiling (Article 4(4) GDPR), which is a determining factor for classifying a system as high-risk under Article 6(3) of the AI Act.

Having reviewed the DPO’s role under the GDPR and the alignment of objectives and complementarity between the GDPR and the AI Act, the following sections address the main obligations under the GDPR and, for each, identify those under the AI Act that could reasonably be integrated into existing GDPR compliance structures.

### a) Record of Processing Activities and AI Systems Inventory

The governance of AI systems undoubtedly requires their inventory and classification based on risk. Without this, organizations will not be able to determine the scope of the regulation or the obligations to be fulfilled.

In this regard, while the AI Act does not establish an explicit obligation to maintain an inventory of AI systems, it does impose obligations to register high-risk systems in the EU database<sup>21</sup> and specifies the information that must be provided for this purpose<sup>22</sup>.

<sup>20</sup> <https://www.sciencedirect.com/science/article/pii/S0267364921000340>  
<https://www.sciencedirect.com/science/article/pii/S0267364924000864>

<sup>21</sup> *Artículo 49. Registro y Artículo 71. Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el ANEXO I*

<sup>22</sup> *Anexo VIII del RIA*

On the other hand, data protection regulations explicitly require maintaining a record of processing activities with specific content (Article 30 GDPR). The Spanish Data Protection Authority (AEPD) has already established in its guidelines that this record must identify the assets supporting the processing, particularly any AI systems used.

Therefore, it is worth considering whether the Record of Processing Activities (RPA) under Article 30 GDPR can serve as the basis for building the AI inventory or whether it is better to create two separate registers, taking into account certain variables:

- i. **AI as a processing asset:** Data protection authorities consider AI as a means (asset) of data processing that can pose specific risks and whose introduction must be assessed in terms of necessity, suitability, and strict proportionality. Including these assets and their supply chain can be a tool for compliance governance and effective risk management.
- ii. **Personal data processing by the organization:** For organizations with large-scale data processing and that develop or use AI, it seems more reasonable to use this record than for those that do not process such data.
- iii. **Personal data processing and high-risk AI systems:** Organizations must consider that AI systems categorized as high-risk under Article 6 of the AI Act are detailed in Annexes I and III. It is difficult to imagine AI systems falling under Annex III that do not involve personal data processing (e.g., access to essential private and public services or employment, workforce management, and access to self-employment).

## b) Risk-Based Approach

According to the AEPD, the GDPR “requires the identification, assessment, and mitigation—carried objectively—of risks to the rights and freedoms of individuals in personal data processing. Mitigation must be achieved through the adoption of technical and organizational measures that ensure and demonstrate the protection of these rights. These measures must be determined with reference to the nature, scope, context, and purposes of the processing and must be reviewed and updated when necessary. In short, the GDPR requires a risk management process for the rights and freedoms of data subjects”<sup>23</sup>.

Similarly, data protection regulations explicitly require maintaining a record of processing activities with specific content (Article 30 GDPR), for which the AEPD has already established in its guidelines that the record must identify the assets supporting the processing, particularly any AI systems used.

The GDPR specifies these risks to the rights and freedoms of natural persons, among others, in Recital 75, which states that they “may result from data processing that could cause physical, material, or non-material damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data processed reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life, or criminal convictions and offenses or related security measures;

<sup>23</sup> [Guía de la AEPD, Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, de Junio 2021](#)

where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable individuals, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.”

The AI Act, for its part, requires in Article 9 the establishment of a risk management system for AI systems that pose high risks to health, safety, or fundamental rights. This article also specifies the stages that such an iterative process must include, which align with the risk management approach applied in the field of data protection.

In fact, the AI Act itself includes a provision in paragraph 10 of that article stating that this risk management may form part of the risk management procedures established under other provisions of Union law.

It will therefore be important for organizations to assess whether they fall into this category and whether they already have risk management systems in place that can incorporate the AI Act’s requirements.

In this regard, the processes, roles, and responsibilities already established for data protection can undoubtedly provide significant synergies, considering that:

- i. The risk management processes contemplated by both regulations are equivalent.
- ii. The risks they aim to identify share a common objective: safeguarding fundamental rights.
- iii. DPOs and the teams currently performing these tasks in the field of data protection have accumulated knowledge and experience over the years.

## c) Data Protection Impact Assessments (DPIAs) and Fundamental Rights Impact Assessments (FRIAs)

**Article 35 of the GDPR establishes the obligation to carry out a DPIA** in cases where processing operations are likely to result in a high risk to the rights and freedoms of natural persons. This assessment consists of **evaluating “in particular, the origin, nature, particularity, and severity of that risk. The outcome of the assessment must be considered when determining the appropriate measures to demonstrate that the processing of personal data complies with this Regulation.”**

Article 27 of the AI Act requires the performance of a Fundamental Rights Impact Assessment (FRIA) for high-risk AI systems by deployers, which must include:

- iv. A description of the deployer’s processes in which the high-risk AI system will be used, in line with its intended purpose.
- v. A description of the period during which each high-risk AI system is expected to be used and the frequency of its use.
- vi. las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico;

- vi. The categories of natural persons and groups that may be affected by its use in the specific context.
- vii. The specific risks of harm that may affect the categories of natural persons and groups identified under point (c) of this paragraph, considering the information provided by the provider pursuant to Article 13.
- viii. A description of the implementation of human oversight measures, in accordance with the instructions for use.
- ix. The measures to be taken if such risks materialize, including internal governance arrangements and complaint mechanisms.

In this case, the complementarity of both obligations is explicitly stated in Article 27(4) of the AI Act, which provides that: *“Where any of the obligations set out in this Article are already fulfilled by the data protection impact assessment carried out pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.”*

Regarding the publication of these assessments (DPIAs and FRIAs), it should be noted that while in the data protection context publication is not mandatory, supervisory authorities have recognized it as a good practice. In contrast, under the AI Act, deployers are required to include in the EU database, pursuant to Article 49(3) and Annex VIII:

*“[...] 4. A summary of the conclusions of the fundamental rights impact assessment carried out in accordance with Article 27.*

*5. A summary of the data protection impact assessment carried out in accordance with Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, as specified in Article 26(8) of this Regulation, where applicable.”*

Given these provisions, it seems logical for organizations to “reuse,” where available, the processes, roles, and responsibilities already established in the data protection domain for conducting the required FRIAs, while considering the necessary adjustments to meet the requirements of Article 27 of the AI Act in line with the guidance to be issued by the AI Office.

## d) Notification of Personal Data Breaches and Serious Incidents

The **AI Act establishes the obligation to notify serious incidents to providers or deployers**—whichever becomes aware of the incident—when a causal link between the AI system and the serious incident has been established or there is a reasonable likelihood of such a link, and in any case no later than fifteen days after the provider or, where applicable, the deployer becomes aware of the serious incident.

A serious incident is defined as an incident or malfunction of an AI system that, **directly or indirectly, has any of the following consequences:**

- The death of a person or serious harm to their health.

- A severe and irreversible disruption of the management or functioning of critical infrastructure.
- Non-compliance with obligations under Union law intended to protect fundamental rights.
- Serious damage to property or the environment.

The AI Act introduces a specific provision for **high-risk AI systems referred to in Annex III**, placed on the market or put into service **by providers subject to Union legislative instruments that establish reporting obligations equivalent to those set out in this Regulation**. In such cases, the notification of these incidents will be limited to those resulting from **non-compliance with obligations under Union law intended to protect fundamental rights**.

It is clear at this point that organizations must ensure that this new procedure for reporting serious incidents is integrated into existing processes, considering:

- i. Organizations already subject to other regulations requiring the reporting of such events may have established procedures, whether or not in addition to those derived from data protection law (e.g., DORA or other regulations).
- ii. The processes established to comply with Article 33 GDPR already ensure the assessment of personal data breaches for notification to supervisory authorities when there is a likely risk to fundamental rights.
- iii. Of the four factors that define a serious incident under the AI Act, the most challenging to assess will likely be the one concerning non-compliance with obligations under Union law intended to protect fundamental rights.
- iv. Notifications made under the AI Act to the market surveillance authority for breaches of obligations under Union law intended to protect fundamental rights will be communicated by these authorities to those responsible for protecting fundamental rights (including data protection authorities).
- v. The management and reporting process established by the AI Act is equivalent to that established by the GDPR.

In this context, it also seems clear that it will be desirable to leverage existing processes, roles, responsibilities, and the experience accumulated over the years in assessing impacts on fundamental rights for risk and reporting purposes.

## e) Transparency and Information Obligations

Article 50 of the AI Act establishes transparency and information obligations for AI systems that interact with humans, perform deepfakes, conduct emotion recognition, or biometric categorization.

- i. Require users to be informed that they are interacting with an AI system or that its content has been generated by such a system. The procedures established in compliance with Article 33 of the GDPR already ensure that personal data breaches are assessed for the purposes of reporting to supervisory authorities when there is a likely risk to fundamental rights.

- ii. his disclosure must be made “clearly and in a distinguishable manner no later than at the time of the first interaction or exposure.”

Additionally, Article 13 of the AI Act establishes transparency and information obligations, requiring AI system providers to include instructions for use containing minimum information (such as the intended purpose of the system, its level of accuracy, associated risks, etc.).

These transparency obligations and their configuration run parallel to, and enable compliance with, the transparency and information requirements set out in Articles 12 (transparency of information, communication, and modalities for exercising data subject rights), and 13 and 14 (information to be provided to data subjects when data is collected from them or obtained from other sources) of the GDPR. These include, among others, the purpose, logic, and consequences of profiling and processing, as well as the right to obtain human intervention in automated decision-making.

## f) Data Subject / Affected Individuals’ Rights

In addition to the right to information, the GDPR provides other rights for data subjects that overlap with those recognized by the AI Act. In this regard:

### ***a. Right not to be subject to automated decision-making (Article 22 GDPR) and Right to obtain an explanation of individually taken decisions (Article 86 AI Act)***

Article 22 of the GDPR establishes the right not to be subject to an automated decision based solely on automated processing and producing legal effects or similarly significantly affecting the individual, such as the automatic rejection of an online credit application or online recruitment services where there is no human intervention.

Article 86 of the IAR establishes the right to obtain an explanation when the decision is based on the output of high-risk AI and when that decision produces legal effects or similarly significantly affects those individuals in a way that has a negative impact on their health, safety, or fundamental rights.

We therefore understand that organizations must take into account (i) the circuits they have established under the GDPR to detect such decisions and (ii) facilitate the appropriate rights, including the necessary information and processes. These circuits may be those that ensure compliance with the provisions of the IAAR (enabling synergies and avoiding inconsistencies).

### ***b. Right to lodge a complaint with the supervisory authority (Article 77 GDPR) and right to lodge a complaint with the market surveillance authority (Article 85 AI Act)***

Similarly, both articles recognize these rights for affected individuals. The conclusions from the previous point apply here as well.



## g) Obligations for High-Risk AI Systems and Data Protection Principles

The AI Act establishes a series of specific obligations for each high-risk AI system, which include:

- \* Data and governance
- \* Technical documentation
- \* Record-keeping
- \* Transparency and communication of information to deployers
- \* Human oversight
- \* Accuracy, robustness, and cybersecurity

These requirements, which must be incorporated from a technical perspective into the design of high-risk AI systems, were already implicitly present in the application of data protection regulations, particularly in Article 5 of the GDPR, which establishes that personal data shall be (with the corresponding AI Act obligations indicated in *italics*):

**a.**

**Processed lawfully, fairly, and transparently in relation to the data subject** ("lawfulness, fairness, and transparency") -> data and governance regarding bias control

**b.**

**Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes** ("purpose limitation")

**c.**

**Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed** ("data minimization") -> accuracy, robustness, and cybersecurity

**d.**

**Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay** ("accuracy") -> **data and governance, accuracy, robustness, and cybersecurity.**

e.

**Maintained in a form that permits identification of data subjects no longer than is necessary for the purposes for which the personal data are processed** ("storage limitation").

f.

**Processed in a manner that ensures appropriate security of personal data**, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ("integrity and confidentiality") -> **accuracy, robustness, and cybersecurity.**

g.

**The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")** -> transparency and communication of information to deployers (instructions for use, log recording, etc.).

Additionally, regarding technical documentation and log recording, the principle of data protection by design and by default—and its enforcement—is one of the key aspects referenced by data protection supervisory authorities when system functionality is inadequate. As for human oversight, we refer to the comments included in the previous section.

## 9.5. Conclusions

The GDPR and the AI Act pursue aligned objectives and are largely configured as complementary regulations.

Both the DPO and the various professionals dedicated to data protection can undoubtedly contribute their specialized knowledge in the context of the new Artificial Intelligence Regulation, leveraging the experience accumulated over the years.

The processes, structures, procedures, and rules, as well as the roles and responsibilities established for GDPR implementation, can serve as the ideal starting point for implementing the AI Act.

Creating parallel structures to those established for data protection in organizations where personal data plays a central role could not only be redundant but also lead to inconsistencies within and outside the organization.

Continuous training, which has always been essential in the field of data protection, becomes an even greater challenge in the context of AI.

The role of the DPO is defined in great detail under the GDPR. Assigning responsibilities in the AI domain—should the organization choose to do so—must follow a careful and parallel approach. Assigning functions different from those established by the GDPR will require a thorough analysis to avoid conflicts of interest. The position granted to the DPO under the GDPR allows, from the outset, the implementation of the AI Act to be placed at the highest management level, ensuring the necessary commitment.

— —  
DECEMBER 2025

# **2ND EDITION THE WHITE PAPER OF THE DPO**



@ISMSForum