July 2025

Job description of the Data Protection Officer

Described by the Article 29 Working Party (Art. 29 WP)[1] as a « *cornerstone of accountability* », the Data Protection Officer (DPO) or Délégué à la protection des données in French (DPD)? is now a key player in the Principality's new data governance system.

Mandatory in certain organizations and often recommended in others, the DPO facilitates compliance with data protection legislation and acts as the preferred point of contact for all questions relating to personal data, whether internal or emanating from a data subject, and as the correspondent for the Data Protection Authority.

When must a Data Protection Officer be appointed?

Article 29 of Law no. 1.565 of December 3, 2024 stipulates that, with the exception of courts in the exercise of their jurisdictional functions, the appointment of a Data Protection Officer is mandatory in the following cases:

- the processing is carried out by a **legal entity under public law or a legal entity under private law entrusted with a mission of general interest or a public service concession**;

- where the core activities of the data controller or the processor consist of processing operations, which, due to their nature, scope or purpose, require **regular and systematic monitoring** of data subjects **on a large scale;**

[1] The Article 29 Working Party was and independent European Union advisory body on data protection and privacy until May 25, 2018 before being replaced by the European Data Protection Board.

What about the notion of regular and systematic monitoring?

According to the « *Guidelines on Data Protection Officers* » adopted by the Article 29 Data Protection Working Party on December 13, 2016, the term « ***regular*** » must be understood as:

- ongoing or occurring at particular intervals for a particular period; or
- recurring or repeated at fixed times; or
- constantly or periodically taking place.

The term « ***systematic*** » is understood to mean:

- occurring according to a system; or
- pre-arranged, organized or methodical; or
- taking place as part of a general plan for data collection; or
- carried out as part of a strategy.

Examples: data-driven marketing activities, profiling and scoring for purposes of risk assessment or location tracking by mobile apps

- the core activities of the data controller or the processor consist of processing **on a large scale of sensitive data or personal data relating to criminal convictions and offenses**.

What about the notion of large-scale processing?

Under article 2 of Law no. 1.565 of December 3, 2024 a large-scale processing is defined as « *any operation which is intended to process a considerable volume of personal data, which may affect a significant number of data subjects, assessed either as a specific number or as a proportion of the relevant population, and which is likely to give rise to a high risk, taking into account in particular the duration or permanence of the data processing activity and its geographical extent* ».

Examples: processing of patient data in the regular course of business by a hospital, processing of travel data of individuals using a city's public transport system or processing of customer data in the regular course of business by an insurance company or a bank

In all other cases, even if it is not mandatory, it is **recommended to appoint a Data Protection Officer** whenever an organization is **faced with issues relating to the protection of personal data.**

Who can be appointed Data Protection Officer?

Qualifications

The Data Protection Officer must be designated on the basis of his/her professional qualities and, in particular, **expert knowledge of data protection law and practices** and the ability to fulfil his/her tasks.

This level of expertise must be **commensurate** with the sensitivity, complexity and amount of data the organization processes.

It is also important that the Data Protection Officer has a **good understanding** of the processing operations carried out by the organization, the information systems used by the organization and the organization's data protection needs.

The organization must also enable the Data Protection Officer to **maintain and supplement his or her skills and knowledge** (ongoing training, participation in workshops, etc.) throughout the duration of his or her assignment.

Risks of conflicts of interest

The position of Data Protection Officer is not necessarily a full-time job. In some cases, the Data Protection Officer may be appointed on a part-time basis, and perform other functions within the organization. To prevent the Data Protection Officer from being "*judge and jury*" the organization must ensure that he or she has **no decision-making power in determining the purposes and means of data processing**.

To achieve this, data controllers and data processors must adopt **internal rules** to define and prevent conflicts of interest.

The risk of conflicts of interest is indeed assessed *on a case-by-case basis*, depending on the organization's activities, size and structure. It is therefore recommended to identify incompatible functions before appointing a Data Protection Officer.

By way of example, the following functions are more likely than others to give rise to a conflict of interest: CEO, Chief Financial Officer, Operations manager, HR Director, CISO (Chief Information Security Officer).

Special cases

A single Data Protection Officer may be appointed for several legal entities governed by public law, or for several legal entities governed by private law entrusted with a mission of general interest or holding a public service concession, given their organizational structure and size.

An agreement will then have to determine the conditions under which this pooling is carried out. **Each of the parties to the pooling agreement remains responsible for the processing operations it carries out and for its data processors.**

A group of companies can also appoint a single Data Protection Officer, provided that he or she is easily **accessible from each establishment**.

Finally, the Data Protection Officer may be a member of the controller's or processor's staff, or fulfil his or her taks on the basis of a service contract (consultant, law firm, consultancy firm, etc.).

What are the tasks of the Data Protection Officer?

The Data Protection Officer's role is to support, inform and advise the organization so that it complies with Monegasque data protection legislation.

He is also responsible for cooperating with the Data Protection Authority.

The Data Protection Officer has 5 missions:

- **Inform and advise** the organization and the employees who carry out the processing on their obligations under the legislation in force in the Principality;
- **Monitor** compliance with personal data protection legislation and with the organization's internal rules on personal data protection, including the **allocation of responsibilities**, **awareness-raising** and **training of staff** involved in processing operations, and the related **audits**;
- **Provide advice**, on request, on data protection impact assessment;
- **Cooperate** with the Data Protection Authority and act as its contact point on matters relating to processing;
- **Submit requests for opinion** to the Data Protection Authority when they concern the following processing operations:

- processing for the purposes of preventing, detecting, investigating, prosecuting or punishing criminal offences, including protection against and prevention of threats to public security;
- processing carried out by administrative and judicial authorities, acting within the scope of their prerogatives as public authorities, involving genetic data or biometric data necessary for authenticating or controling a person's identity.

Data subjects may also contact the Data Protection Officer if they have any questions about the processing of their data, or if they wish to exercise their rights.

In performing his or her tasks, the Data Protection Officer **must take into account the risk associated with the processing operations** in view of the nature, scope, context and purposes.

How does the Data Protection Officer perform his/her tasks?

The guarantees

A number of safeguards have been put in place to enable Data Protection Officers to carry out the tasks for which they have been appointed.

First and foremost, the Data Protection Officer must be able to **act completely independently**. To this end, he/she must not receive instructions from any authority regarding the performance of his/her duties as DPO. A manager cannot, for example, tell the Data Protection Officer what result should be obtained or what interpretation of a legislative provision on data protection should be adopted.

However, this independence does not mean that the Data Protection Officer has decision-making powers that go beyond the tasks entrusted to him or her.

The Data Protection Officer must also have **sufficient resources**.

In addition to the necessary financial resources and adequate infrastructure (premises, equipment, etc.), this guarantee also includes the active support of the Data Protection Officer by senior management, the necessary time (particularly when the Data Protection Officer works part-time) to fulfil his or her duties, and easy access to other departments (human resources, legal, IT, etc.) to obtain the information he or she needs.

The Data Protection Officer must also be **involved**, in an appropriate manner and in due course, in **all matters relating to data protection**. The organization must therefore ensure that it invites the Data Protection Officer to all relevant meetings and that it obtains his opinion before any decision is taken that has an impact on personal data protection. It must also consult the Data Protection Officer immediately in the event of a data breach or any other incident.

He/she **reports directly** to the **highest level of management** of the data controller or processor.

The organization must also give the Data Protection Officer access to the data and processing operations, with the exception of processing that affects national security.

Data subjects may contact the Data Protection Officer regarding **any issues relating to the processing of their personal data** and the exercise of their rights under the Law.

The Data Protection Officer **may not be dismissed or penalized** by the organization for performing his/her tasks. In practical terms, this means that the Data Protection Officer may not, for example, be dismissed for having advised the organization to carry out an impact assessment for a data processing operation that he or she considers is likely to result in a high risk for the protection of personal data.

Finally, the Data Protection Officer cannot be **held responsible for the organization's failure to comply with data protection legislation**. It remains the responsibility of the organization to ensure and be able to demonstrate that processing complies with data protection legislation. Consequently, if the organization takes decisions contrary to the opinion of the Data Protection Officer, the latter must be able to clearly communicate his or her divergent opinion to senior management.

The obligations

In return for all these guarantees, the Data Protection Officer is also bound by certain obligations.

The very first of these is an **obligation of confidentiality** with regard to the performance of his/her duties. They are also bound by **professional secrecy.**

The Data Protection Officer must also demonstrate integrity and a high level of ethics in order to promote and ensure respect for the protection of personal data within the organization in which he or she performs his or her duties.

Finally, the Data Protection Officer **must be reachable**, either by being physically in the same place as employees, or through a telephone helpline or any other secure means of communication, so that data subjects can contact him or her.

In this respect, it is up to the organization to publish the professional contact details of the Data Protection Officer and to communicate them to the Data Protection Authority.

What is the penalty for failing to appoint a Data Protection Officer?

Article 53 of Law no.1.565 of December 3, 2024 provides that failure to fulfil the obligation to appoint a Data Protection Officer is punishable by an administrative fine of up to **5,000,000 Euros or, in the case of a company, up to 2% of the previous year's total worldwide annual revenue, whichever is the highest**.