Know your obligations

Law No. 1.565 of December 3, 2024 sets forth a number of obligations for data controllers, many of which also apply to data processors.

COMMON OBLIGATIONS FOR DATA CONTROLLERS AND PROCESSORS

The obligation to appoint a representative : all data controllers or processors not established in Monaco, must, apart from the exceptions provided by Law, appoint a representative in the Principality or, failing that, within a member state of the European Union, if they:

- offer products or services to individuals located in the **territory of the Principality**;
- implement processing related to the **monitoring of their behavior**.

This person will be the contact for both the data subjects concerned by the processing and the APDP, **to respond to all questions**.

[For more information, refer to the factsheet **The key players in data protection in the Principality**]

The obligation to maintain a record of processing activities : all data controllers or processors must, apart from the exceptions provided by Law, maintain a record of processing activities carried out under their responsibility if they have at least 50 employees.

WARNING this threshold of 50 employees does not apply if the processing is not occasional (example of occasional processing: sending e-mails specifically for the launch of a new product).

This record aims to **replace a large part of the preliminary formalities** established by Law No. 1.165 of December 23, 1993, as amended.

[For more information, refer to the factsheet **The record of processing activities in 10 questions and answers**]

The obligation to appoint a Data Protection Officer: mandatory in certain organizations and often recommended in others, the Data Protection Officer (DPO) facilitates compliance with the data protection legislation and acts both as the primary point of contact for all questions related to personal data, whether internal or arising from an individual affected by a processing operation, and as the correspondent for the Data Protection Authority.

[For more information, refer to the factsheet **Job description of the Data Protection Officer**]

The obligation to ensure the level of security appropriate to the risks : all data controllers or processors must take appropriate technical and organizational measures to ensure a level of security appropriate to the risks to the rights and freedoms of individuals.

The adoption of these measures requires an analysis to identify the risks and then determine their level of probability and severity.

[For more information, refer to the FAQ **What are the obligations of the data controller?** and **What are the obligations of the data processor?**]

The obligation to supervise any use of processors : whenever a data controller uses a processor, the latter must provide sufficient guarantees regarding the implementation of appropriate technical and organizational measures to ensure the protection of personal data and the respect for the rights of the data subjects.

Any use of a processor must be governed by a contract **that is in written form**, with the minimum clauses provided for in Article 26 of Law No. 1.565 of December 3, 2024.

[For more information, refer to the factsheet **The key players in data protection in the Principality**]

THE OBLIGATIONS SPECIFIC TO DATA CONTROLLERS

The obligation to ensure data protection by design : the data controller must implement **appropriate technical and organizational measures both at the time of determining the means of processing and at the time of the processing itself** to ensure a **high level of protection** of the personal data.

[For more information, refer to the FAQ **What are the obligations of the data controller?**]

The obligation to ensure data protection by default : the data controller must implement appropriate technical and organizational measures to ensure that only the personal data **necessary** for **each specific purpose of processing** are processed.

[For more information, refer to the FAQ **What are the obligations of the data controller?**]

The obligation to conduct an impact assessment when processing is likely to result in a high risk to the rights and freedoms of data subjects: a Data Protection Impact Assessment (DPIA or AIPD in French) is a study whose objective is to identify and analyze how the privacy, security, or availability of data would be affected by a given action or activity.

[For more information, refer to the factsheet **Impact assessment on personal data protection**]

The obligation to notify data breaches : the data controller must notify the APDP of any breach of personal data of which it is aware **where such a breach is likely to cause a risk to the rights and freedoms of the data subjects.**

This notification must be done **without undue delay**, and if possible within a maximum of **seventy-two hours after becoming aware of it**.

This notification may also be accompanied, in certain cases, by a communication to the impacted data subjects.

[For more information, refer to the factsheet **Notification of personal data breaches**]

The obligation to submit certain processing to the APDP : if a very large number of processing are no longer subject to formalities with the APDP, exceptions remain.

The following three categories of particularly sensitive processing are thus subject to the prior opinion of the APDP:

- the processing operations for the purposes of the **prevention, detection, investigation, and prosecution of criminal offences or the execution of criminal sanctions**, including protection against and prevention of threats to public security;
- the processing of **genetic or biometric data** necessary to **authenticate** or **verify a person's identity**, implemented by the administrative and judicial authorities acting within the missions conferred on them by law;
- processing for the purpose of **research in the field of health**.

Certain data transfers to a country, territory, or international organization that **does not ensure an adequate level of protection** are also subject to **prior authorization** of the APDP.

Lastly, Article 85 of the Law provides that video surveillance systems installed in **places not open to the public** shall be **brought to the immediate attention of the APDP**.

According to the explanatory statement, a place not open to the public is "*for example, a private place (home, garage, etc.) or premises for professional use such as offices or warehouses*".

[For more information, refer to the factsheet **Formalities to be completed with the APDP**]

STRICTER REQUIREMENTS REGARDING THE RIGHTS OF DATA SUBJECTS

The rights of data subjects have been strengthened, notably the right to information, which has been enhanced and the right of access, which states that the data controller must provide a copy of the personal data undergoing processing to any person requesting it.

Moreover, new rights have been added (the right to data restriction, the right to data portability, and the right not to be subject to a decision producing legal effects).