November 2025

Formalities to be completed with the APDP

While, in line with the principle of accountability for data controllers, a large number of data processing operations are no longer subject to formalities with the APDP, exceptions remain with a system of prior requests for opinions for the most sensitive data processing operations, prior requests for authorisations for certain transfers, and declarations, in particular for video surveillance systems installed in places not open to the public.

In addition, new obligations are also imposed on data controllers, and sometimes on processors, under Law No. 1.565 of December 3, 2024, such as the appointment of a data protection officer and the notification of data breaches.

Prior requests

Requests for opinions

The following three categories of **particularly sensitive** processing are 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**;

For these first two categories of processing, this obligation of prior formalities concerns only the **competent administrative and judicial authorities** within the missions conferred on them by law.

- processing for the purpose of **research in the field of health**.

The APDP shall issue its opinion within **two months** of the submission of the complete request for an opinion.

This period may be extended once, subject to a **reasoned decision** by the President of the APDP.

If the opinion has not been issued by the end of this period, it shall be **deemed to be favourable**.

What must requests for opinion contain?

The requests for opinion submitted to the APDP must include the following information:

- the **name and professional contact details** of the data controller or his or her representative in Monaco;
- the **legal basis** for the processing and, where applicable, the draft ministerial order or the draft order of the Secretary of State for Justice, Director of Judicial Services;
- The **purposes** of the processing;
- the **name**, if any, of the processing
- the **categories of personal data** processed, their origins, and the categories of the data subjects of the processing;
- the **retention period** of the personal data processed or, if this is not possible, the criteria used to determine this period;
- the **departments in charge of the implementation** of the processing;
- **a risk analysis relating to the safeguarding** of the processing, including security measures;
- the authority or function of the person or department to whom the **right of access** is exercised and the measures taken to facilitate the exercise of this right;
- the categories of persons who, by reason of their functions or for the purposes of the service, **have access to the personal data**;
- the recipients or recipient categories entitled to **receive the personal data**;
- where applicable, **interconnections, reconciliations**, or any other form of connection with other processing;
- where applicable, the identity and address of the **processor**;
- where applicable, the **transfer of data outside the Principality** and the **appropriate guarantee**s governing such transfers.

Any change in the processing relating to:

- the **legal basis** for the processing (and, where applicable, the draft ministerial order or draft order);
- the **purpose(s)** of the processing;
- the **categories of personal data** processed, their origin and the categories of the data subjects of the processing;
- the **retention period** for the personal data processed or, if this is not possible, the criteria used to determine this period;

must be the subject of a new request for an opinion without delay.

Any other change to the processing must be communicated to the Authority in writing without delay.

Autorisation requests

Transfers of data to a State, territory or international organisation **that does not ensure an adequate level of protection** are subject to **prior authorisation** by the APDP when:

- the data are transferred to a country, territory, or international organization that **does not ensure an adequate level of protection**, and
- **appropriate safeguards** have not been put in place, and
- **none of the derogations provided for** in Article 99 of Law no. 1.565 of December 3, 2024 apply, and
- the **4 conditions provided for** in paragraph 3 of Article 99 **are not met**.

The APDP renders a decision within **2 months** after receiving the complete request for authorization.

This delay may be renewed once by **reasoned decision** of the President.

If the authorization has not been issued by the APDP by the end of this period, the authorization is deemed to have been **refused.**

[For more information, refer to the factsheet **Data transfers outside the Principality : scenarios to consider**]

Where a request for an opinion or authorisation does not contain all the information required for its examination, the APDP shall inform the data controller, within 15 days of receipt, of the documents or information to be provided. If these are not provided within one month of notification, the request shall be declared inadmissible.

Mandatory declarations

Video surveillance systems in places not open to the public

Article 85 of the Law stipulates that video surveillance systems installed in **places not open to the public must be reported to the APDP without delay**.

What do we mean by places not open to the public?
According to the explanatory memorandum, 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* ».

In the case of homes or any other place used for personal or domestic purposes, the declaration to the APDP must be carried out only if people outside the family or friends' circle intervene in the home, e.g. housekeepers, home helpers.

What about cameras installed in places open to the public?
Video surveillance systems installed in **places open to the public or filming the vicinity of public roads, spaces open to the public or to public traffic** remain subject to **prior authorisation by the Minister of State**. According to the explanatory memorandum, places open to the public include, for example, « *a restaurant, a shopping centre or an administrative office* ».

Transfers meeting the criteria of paragraph 3 of Article 99 of Law No. 1.565 of December 3, 2024

Paragraph 3 of Article 99 of Law no. 1.565 of December 3, 2024 provides that **in the absence of an adequate level of protection** and **appropriate safeguards,** and if **none of the derogations** provided for in paragraphs 1 and 2 of Article 99 is applicable, a data transfer to a country, territory or international organization that does not have an adequate level of protection is possible, if the following **4 conditions** are met:

- the transfer is **not repetitive**;
- the transfer only affects a **limited number of data subjects**;
- the transfer is necessary for the purposes of pursuing **compelling legitimate interests** of the data controller which are not overridden by the interests or rights and freedoms of the data subject;
- **appropriate safeguards** have been taken.

The data controller must inform the APDP of this transfer.

The data controller **shall also inform the data subjects concerned** by the transfer of the **compelling legitimate interests** it is pursuing **and the appropriate safeguards** that have been taken.

The Data Protection Officers (DPO)

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**; - 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;** - 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**.

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.**

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

It is the responsibility of the organisation to publish the professional contact details of the Data Protection Officer and to communicate them to the Data Protection Authority.

The representatives

Referred to in article 25 of Law no. 1.565 of December 3, 2024, the representative is the natural person or legal entity **established on the territory of the Principality** or, failing that, within a Member State of the European Union who has been **appointed** by a data controller or processor to be the **contact** both for the data subjects and for the APDP. These will then be able to contact the representative with any questions they may have.

The representative **must** be appointed whenever a data controller or processor, **not established in Monaco, offers products or services** to individuals located in the Principality or implements processing operations relating to the **monitoring of their behaviour**.

Examples :

- an e-commerce company based in Italy offering products or services to people in the Principality
- an American press company offering an online newspaper subscription service without having an office in Monaco

A representative may be appointed by **any written means**.

This obligation is not general and has **3 exceptions**:

- the processing is **occasional** and does not **involve large-scale processing of sensitive data**;
- the processing relates to **criminal convictions** or **offences**;
- the data controller is a **legal person governed by public law** or a **public organization**.

Notifications of data breaches

Law no. 1.565 of December 3, 2024 introduces a new obligation for data controllers: they must notify **any personal data breach of which they have become aware** that is **likely** to result in a **risk to the rights and freedoms of the affected individuals**.

What is a data breach?
A data breach is a security incident involving personal data held by a data controller. In accordance with the three classic security principles, these breaches can be classified into three categories: - « ***Confidentiality breaches*** »: occur in the event of disclosure or unauthorized or accidental access to personal data; - « ***Integrity breaches*** »: occur in the event of unauthorized or accidental alteration of personal data; - « ***Availability breaches*** » : are the accidental or malicious loss or destruction of personal data, or their encryption by an unauthorised third party.

This notification **must** be made to the **APDP** whenever a breach presents a **low, medium or high** risk to the rights and freedoms of the individuals concerned.

It must be made **as soon as possible**, and if possible within a maximum of **72 hours after becoming aware of it.**

The data controller may not have all the information concerning a breach within 72 hours of becoming aware of it, particularly in the case of a complex breach. In such cases, a **notification in phases** is possible, with prior notification of the APDP within 72 hours with a brief summary of the incident, followed by the provision of additional, more detailed information.

If the notification is not made within 72 hours, the reasons for the delay are given.

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

Mandatory consultations/approvals

Impact assessments

What is an impact assessment?
A new instrument introduced by Law no. 1;565 of December 3, 2024, the data protection impact assessment (DPIA) is a study whose purpose is to identify and analyze the risks that data processing may pose to individuals' privacy. Not every operation that could pose a risk to the rights and freedoms of individuals automatically requires an impact assessment. The law only requires an impact assessment when processing is likely to result in a **high risk to rights and freedoms**, particularly when **new processing technology** is used.

If, when carrying out the impact assessment, the data controller realises that the **identified risks cannot be sufficiently reduced** and that there are **high residual risks that cannot be controlled**, Article 36 of Law no. 1.565 of December 3, 2024 stipulates that they **must** first consult the APDP.

The data controller shall provide the Authority with the following information:

- the **respective responsibilities** of the data controller, joint controllers and data processors involved in the processing, and the contact details of the data protection officer, where one has been appointed;
- **the purposes and means** of the proposed processing;
- **the measures and safeguards** envisaged to protect the rights and freedoms of data subjects;
- the **impact assessment** carried out;
- any other information requested by the Authority.

The APDP will then have a maximum of eight weeks to issue a **written opinion** to the data controller; this period may be extended by six weeks in the case of complex processing operations.

If the Authority considers that the processing constitutes a violation, it will impose **appropriate measures** on the data controller and may carry out the **verifications and investigations** provided for in Article 46 of Law no. 1.565 of December 3, 2024.

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

Codes of conduct

What is a code of conduct?
Codes of conduct are part of the new compliance tools introduced by the new legislation (Article 33). They are developed by associations and professional bodies representing **categories of data controllers and processors**. They thus enable professionals, **in a specific sector**, to meet their **operational needs** in terms of data protection compliance by providing a **detailed description** of the most appropriate and ethical **behaviors**.

Once developed, the codes of conduct applicable in Monaco are forwarded to the APDP for **validation and publication**.

Any subsequent changes to a code or, where applicable, **its extension** must be sent to the APDP who then verifies that the said code still **offers appropriate guarantees of protection**.

The APDP approves draft codes, amendments and extensions within **4 months** of receipt of the request. This period may be extended by a **further 2 months** by decision of its President.

If the APDP has not reached a decision within this timeframe, the request is **deemed to have been rejected**.

The codes of conduct, their amendments and, where appropriate, their extensions are listed by the APDP in a **register open to the public**.

When a code of conduct has been approved already by a **foreign protection authority**, the data controller or the processor must forward it to the APDP so that the latter can verify that the provisions of the said code contain the **appropriate guarantees pursuant to the Law**.

In a nutshell:

Prior requests	Declarations	Consultations/approvals
Requests for opinions: (research in the field of health and certain treatments implemented by the competent administrative and judicial authorities within the exclusive framework of the tasks legally assigned to them) **Requests for authorisation** (transfers that do not meet any of the conditions set out in Articles 97 to 99 of the Law)	**Video surveillance** in places not open to the public **Transfer** meeting the criteria of paragraph 3 of Article 99 **Data protection officers** **Representatives** **Data breach notifications**	**Impact assessments** that present high uncontrolled residual risks **Codes of conduct**

The forms required to complete these preliminary formalities are available free of charge on the APDP website under the **Forms and Tools** tab on the **Professionals** page.