Data transfers outside the Principality: scenarios to consider

Although Law no. 1.565 of December 3, 2024 no longer requires prior authorization from the APDP, except in rare cases, for data transfers to countries, territories or international organizations that do not have a legal framework offering an adequate level of protection, it nevertheless provides for a wide range of **legal tools and conditions** to **govern** such transfers.

The principle of no prior formalities for any transfer to a country, territory or international organization with an adequate level of protection remains, but **several scenarios are now to be considered successively** if the country, territory or international organization concerned is not considered adequate.

These tools apply to both the data controller and the processor, and also concern **subsequent transfers** of personal data from the recipient country, territory or international organization to another country, territory or international organization.

The aim is to ensure that the level of protection for individuals guaranteed by the Law is not compromised by such transfers.

What does data transfer mean?

A data transfer is **any flow of data** to a country, territory, or international organization outside of the Principality.
This may involve a **physical transfer** or a **remote access**, either within a group or to a third party.

Examples :

- data hosting by the parent company located in France
- access to data by the IT provider located in India for maintenance purposes

The principle: No prior formalities are required if the data are transferred to a country, territory or organization with an adequate level of protection

Article 97 of the Law establishes the principle whereby **any transfer of personal data outside the Principality** may be undertaken **without any prior formality** providing the legislation or regulation of personal data of the recipient country, territory, or international organization has an **adequate level of protection** as observed by the Principality.

The list of countries, territories, and international organizations with an adequate level of protection is **adopted by the Government** by Ministerial Order .

The APDP is consulted **beforehand for its opinion.**

This list is published in the Journal de Monaco and on the APDP website.

It is regularly updated. Thus, when it is found that a country, territory or international organisation no longer provides an adequate level of protection, the Ministerial Order is amended to take this into account.

This update has no effect on personal data transfers that have already been made.

Member States of the European Union are deemed to offer an adequate level of protection.

Member countries of the European Union:

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

If the country, territory or international organization receiving the data is not on the list of countries providing an adequate level of protection, the other scenarios provided for by the Law must be considered in succession.

Scenario 1: Appropriate safeguards have been put in place by the data controller or processor

Data may be transferred to a country, territory or international organization that is not on the list of countries, territories or international organizations whose legislation or regulations ensure an adequate level of protection, provided that appropriate safeguards have been put in place.

There are 5 safeguards:

- compliance with an **enforceable commitment in the Principality**;
- the use of **standard protection clauses previously approved** by the APDP;

- compliance with **binding corporate rules approved by the APDP** or by a data protection authority of a State that ensures an adequate level of protection;

Definition of binding corporate rules (Article 2 of Law no. 1.565 of December 3, 2024):

« *the internal rules relating to the protection of personal data that a controller or processor established on the territory of the Principality applies for transfers or for a set of transfers of personal data to a controller or processor established abroad within a group of companies, or a group of companies engaged in a joint economic activity* ».

Binding corporate rules must cover at least the following points :

- the structure and contact details of the group of companies to which these rules apply and of each of its entities;
- the measures put in place within the group of companies to ensure compliance with these rules;
- the application of the data protection principles set out in Law no. 1,565 of December 3, 2024, in particular the principles of lawfulness of processing, purpose, fairness, transparency, proportionality and accuracy referred to in Article 4;
- the categories of data transferred and data subjects;
- the type and purpose of the transfer of personal data;
- the names of the recipient countries, territories and international organisations;
- the conditions applicable to the storage and erasure of data;
- the recipients authorised to process the data;
- the measures to ensure the security of personal data;
- the conditions applicable to onward transfers to organisations not bound by binding corporate rules;
- the obligation for recipients to inform data subjects about the processing of their data;
- the obligation to notify data breaches;
- the rights of data subjects, in particular the right to access their personal data, the right to object to the processing of their data or to request its restriction, the right to request the rectification or erasure of their data, and the right to lodge a complaint with the APDP.
- the manner in which binding corporate rules are provided to data subjects;
- the acceptance by the data controller or processor established in Monaco of its liability in the event of a breach of these rules by a company located in a country that does not have an adequate level of protection, unless it proves that the event giving rise to the damage is not attributable to it.

Any amendments to binding company rules previously approved by the APDP must be submitted to it for approval.

- a **certification mechanism** implemented by the APDP or by independent bodies approved by it;

What is a certification mechanism?

Certification demonstrates that **processing operations** carried out by data controllers or processors **comply with Law no. 1.565 of December 3, 2024.**

It is a **legally binding** compliance tool for those who choose to commit to this approach.

Certification candidates undertake to:
- comply with the criteria approved by the APDP and
- maintain compliance with these criteria throughout the period of validity of their certificate.

This is a **voluntary process**.

- the adherence to a **code of conduct** approved and published by the APDP.

What is a code of conduct?

Developed by an association or professional body representing **categories of data controllers or processors**, a code of conduct meets the **operational needs** of professionals in a **specific sector,** in their data protection compliance efforts, by providing a **detailed description** of the most appropriate and ethical **behavior**.

It is a **voluntary approach** that encourages professionals in a given sector to adopt **good practices and customs** (for example, specific security measures) and to demonstrate, to data subjects and other stakeholders, **compliance with the provisions applicable to the processing of personal data**.

Where data transfers are covered by a **certification mechanism** or **code of conduct**, they must be accompanied by a **binding and enforceable commitment** by the data controller or processor in the recipient country, territory or international organisation **to apply the appropriate safeguards contained in those instruments**, including with regard to the rights of data subjects.

The data controller or processor **shall forward this commitment to the APDP.**

Scenario 2: The transfer meets the conditions for the application of one of the derogations provided for in the Law

In the absence of an adequate level of protection and **appropriate safeguards**, article 99 of Law no. 1.565 of December 3, 2024 provides for **derogations** to allow data to be transferred to a country, territory or international organization that does not have an adequate level of protection.

There are 7 such derogations:

- the person to whom the data relate has **explicitly consented** to their transfer **after having been informed** of the absence of an appropriate level of protection or safeguards and of the **nature of the risks** introduced by this absence;

Example: an Internet user has consented by means of a checkbox to the transfer of his or her data to the United States for statistical purposes after having been duly informed of this transfer beforehand by an information banner

- the transfer is necessary to **protect the vital interests of the data subject or of other persons**, where the data subject is **physically or legally incapable of giving consent**;

Example: sharing of personal data by the relatives of a victim of an earthquake in Peru with the authorities in charge of local rescue operations

- for **important reasons of public interest**;

In the context of this derogation, the APDP may request **any relevant information** from the data controller or processor.

- if the transfer is **necessary for the establishment, exercise, or defense of a legal claim**;

Example: the disclosure of documents as part of an anti-trust investigation

- for the **consultation of a public register** provided for by law, intended for the information of the public and open to consultation by the public or any person **demonstrating a legitimate interest**;

Example: register of companies

- If the transfer is **necessary for the performance of a contract** between the data controller or its representative and the data subject **or for the implementation of pre-contractual measures taken at the data subject's request**;

Example: the transfer by a travel agency of its customers' personal data to hotels located in Asia as part of the organization of holidays abroad

- when the transfer is **necessary for the conclusion or performance of a contract** concluded or to be concluded, **in the interest of the data subject**, between the data controller or its representative and a third party.

Only 4 of these 7 derogations apply to the activities of public authorities in the exercise of their **prerogatives as public authorities**, namely:

- ❑ the protection of vital interests;
- ❑ the important reasons of pubic interests;
- ❑ the establishment, exercise or defense of a legal claim;
- ❑ the consultation of a public register.

Scenario 3: The special case provided for in paragraph 3 of article 99

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 must not be carried out as part of the normal course of operations within an entity.

  Example: one-off access to a file as part of legal proceedings

- the transfer only affects a **limited number of data subjects**;

  This condition will be assessed on a case-by-case basis, but the number must be sufficiently small given the type of transfer.

  Example: only the data of employees working in a bank's IT department are transferred

- 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;

  Example: the transfer is necessary to protect an organization from serious and immediate harm

- **appropriate safeguards** have been taken.

  Example: deletion of data as soon as possible after transfer

The APDP must be informed 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.

This exception provided for in paragraph 3 of article 99 of Law no. 1.565 of December 3, 2024 does not apply to the activities of public authorities in the exercise of their prerogatives as public authorities.

Scenario 4 : Prior authorization of the APDP

If:

- 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 data controller or processor must request **prior authorization** from the APDP.

This transfer will be authorized if:

- **appropriate safeguards other than those referred to above** have been taken,

  Example : provisions to be incorporated into administrative arrangements between public authorities or public bodies which provide enforceable and effective rights for the data subjects

  or

- **specific contractual clauses** between the data controller and the processor or between one of them and the data controller, the processor and the recipient of the data have been provided for.

The APDP renders a decision within **2 months** after receiving the 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.**

What is the penalty for failure to comply with data transfer obligations?

Pursuant to article 54 of Law no. 1.565 of December 3. 2024, failure to comply with the obligations relating to data transfers outside the Principality is punishable by an administrative fine of up to **10,000,000 Euros or, in the case of a company, up to 4% of the previous year's total worldwide annual revenue, whichever is the highest.**

In a nutshell :