How we work

- ***The plenary formation:***

The plenary session is responsible for developing tools to comply with Law no. 1.565 of December 3, 2024 and ensure compliance with the law.

Pursuant to Article 46 of the Law, the plenary formation, **outside the restricted formation, shall carry out, on its own initiative or on the basis of a report, the necessary verifications and investigations** to monitor the implementation of the processing operations.

In addition to **on-site inspections and those carried out in response to a summons**, members of the Authority, its agents or investigators may carry out **any useful observations**, such as, for example, consulting data freely accessible or made accessible via an online communication service.

Where a non-compliance is found to be likely to be remedied, the President of the Authority may issue a formal notice to the controller or processor to comply, which may be made public. This procedure will be closed if compliance is achieved.

- ***The restricted formation:***

The restricted formation is responsible for **taking measures** and **imposing penalties** on data controllers or processors who **fail to comply with** the provisions of Law no. 1.565 of December 3, 2024.

This formation is made up of **three members of the plenary formation**, namely the **judge of the court** who is the President and two other members elected by the Authority from among its members.

These members may not exercise **any powers of investigation or prosecution**.

The restricted formation deliberates outside the presence of the Authority staff, with the exception of a meeting secretary.

Cases may be referred to the restricted formation:

- when the **formal notice** given to the data controller or its processor to comply has **remained unsuccessful**;
- without prior formal notice, **when the non-conformity is not likely to be brought into compliance** as it cannot give rise to a corrective measure:

Example : data have been destroyed or a disputed transfer has taken place.

- When a data controller or processor **fail to comply with the obligations of the Law**.

At the end of an **adversarial procedure**, the restricted formation of the APDP may impose one of the following sanctions:

- a **warning**;
- an obligation to **bring the processing into compliance** or to **satisfy the requests of the data subject**, which may be accompanied by a penalty payment of up to to 10,000 Euros / calendar day of delay;
- a **temporary or permanent restriction of processing**;
- a **withdrawal of the issued accreditation** to a certifying body or an injunction to the latter to refuse or withdraw the granted certification;
- a **withdrawal of the delivered certification**;
- a total or partial suspension of the **decision approving the binding corporate rules**;
- the **suspension of data flows** addressed to a recipient located in a foreign country;
- 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 amount is the higest**.

The restricted formation may decide to **publish its decisions**.

The decisions of the restricted formation are also **subject to full litigation appeals** before the **Court of First Instance**.

Breaches constituting **criminal offences** are reported **without delay to the Public Prosecutor**.

The administrative fines 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 amount is the higest.
Article 53 of Law no. 1.565 of December 3, 2024, stipulates that failure to comply with the following obligations is punishable by this fine: • verification that **consent has been obtained** where processing is based on such consent; • **cooperation** of the data controller or processor **with the Authority**; • **protection by default** and **protection by design**; • requirements for joint **responsibility**, appointment of a **representative, processing, record of processing activities** or appointment of a **data protection officer**; • the **security measures** for processing; • **communication of personal data breaches** to the Authority and, where applicable, to data subjects; • **codes of conduct**; • **impact assessment requirements**; • **informing the Authority** of the existence of a video surveillance system installed in **a place not open to the public**.
The administrative fines 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 amount is the higest.

Article 54 of Law no. 1.565 of December 3, 2024, stipulates that this fine applies to breaches of the following obligations:

- principles relating to **data quality** and the conditions for lawful **processing**;
- **information of the data subjects**;
- the collection, recording, storage or use of **sensitive data**;
- the rights of the **data subjects**;
- the **communication of inaccurate information or documents** to the data subjects or to the persons in charge of verifications or investigations;
- with the exception of administrative and judicial authorities, the collection, recording, storage or use of personal data relating to **offences, convictions or security measures or whose purpose is the prevention, investigation, recording or prosecution of criminal offences or the execution of criminal convictions or security measures**;
- **data transfers** outside the Principality that do not comply with the provisions of the Law;
- failure to comply with **injunctions and prescriptions** issued by the Authority's **restricted formation**.

What criteria must be taken into account to ensure that the fine is effective, proportionate and dissuasive?

Article 52 of Law no. 1.565 of December 3, 2024, stipulates that when imposing a penalty payment or administrative fine, the restricted panel must take the following criteria into account:

- the **nature, seriousness and duration** of the breach;
- whether the breach was **deliberate, negligent** or **repeated**;
- **the measures taken** by the data controller or processor to **mitigate the damage** suffered by the data subjects;
- the degree of **cooperation with the Authority** in order to remedy the breach or mitigating any adverse effects;
- the **categories of personal data** affected by the breach;
- any applicable **aggravating or attenuating circumstances.**