Glossary

Anonymization: a technique that consists in « *removing any identifying characteristics from a set of data* ».

It corresponds to the « *process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII subject can no longer be identified directly or indirectly, either by the data controller of the PII alone or in collaboration with any other party* ». (ISO 29100: 2011).

As such, anonymization is recognizable by the **irreversibility** of the **loss of any identifiable individual characteristics**.

[For more information, refer to the factsheet **Anonymization or pseudonymisation**]

Biometric data: defined in article 2 of Law no. 1,565 of December 3, 2024 as « *personal data resulting from a specific technical processing, relating to the physical, physiological, or behavioral characteristics of an individual, which allow or c*onfirm their unique identification, such as facial images or fingerprint data ».

Biometrics refers to the **physical characteristics** but also to the **behavioral characteristics** of an individual.

Examples:

- body language
- way of walking

However, within the meaning of the law, these characteristics are only considered to be biometric data when they are processed for the purpose of uniquely identifying or authenticating a natural person.

Examples:

- the voice recording for the purpose of uniquely identifying an individual is a biometric data
- the voice recording for the purpose of improving a company's quality service without identifying the person is not a biometric data

Certification: as provided for in article 34 of Law no. 1.565 of December 3, 2024, the certification makes it possible to demonstrate that the **processing operations** carried out by data controllers or processors comply with the law. responsables du traitement ou les sous-traitants respectent la Loi.

It is a **legally binding** compliance tool for those who choose to engage in this process.

Thus, the candidate for certification agrees to comply with the criteria approved by the APDP and to maintain this compliance with the criteria for the **duration of the certificate's validity**.

This is, however, a **voluntary approach**.

The certification procedure may be implemented by the APDP or by independent bodies accredited by the APDP.

Codes of conduct: developed by associations and professional bodies representing categories of data controllers or processors, codes of conduct are part of the new compliance tools established by article 33 of Law no. 1.565 of December 3, 2024.

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.

This **voluntary approach** encourages professionals in a given sector to adopt good practices (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**.

Consent: defined in article 2 of Law no. 1.565 of December 3, 2024 as « *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* ».

To be valid, the consent given by the data subject must therefore **meet four conditions**:

- **freely-given**: the data subjects must be able to **make a real choice** regarding the processing of their data. Therefore, they **must not be coerced or influenced** in their choice. They should not suffer from any negative consequences if they do not consent.
- **specific**: the consent **must be specific to the purpose** of the processing. Therefore, when the processing has **several purposes**, the consent should be **obtained independently for each purpose**. This is referred to as **separate consent** for each purpose.
- **informed**: before the data subject makes a choice, the data controller must **inform** the data subject of **certain information** as listed in article 11 of Law no. 1.565 of December 3, 2024.
- **unambiguous**: the consent must be given by an **oral or written** statement from the data subject or result from a **clear affirmative** act. There must be no reasonable doubt as to the data subject's wish to give consent to the processing of his or her data.

Silence or inaction of the data subject **does not constitute valid consent** within the meaning of the legislation relating to the protection of personal data as consent cannot be unambiguous.

[For more information, refer to the factsheet **The consent of data subjects**]

Data breach notifications: pursuant to article 32 of Law no. 1.565 of December 3, 2024, a data controller must notify the APDP of **any data breach of which it has become aware and which is likely to pose a risk to the rights and freedoms of the affected individuals**.

Example: an unauthorized third party accesses a company's HR file and modifies its content

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

It **must** be done through the **APDP** to ensure the preservation of the rights and freedoms of the individuals affected by the violation by any necessary intervention.

The notification may also be accompanied, in certain cases, by a **communication** to the **data subjects** impacted by this breach, when the said breach is **likely to result in a high risk to the rights and freedoms of an individual**.

The assessment of high risk is made in the light of a particular incident and is based on the consequences that could arise from it.

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

Data controller: defined in article 2 of Law no. 1.565 of December 3, 2024 as the « *natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data* ».

The data controller is therefore the person or body with **decision-making power** over the purposes and means of data processing.

In general, this is the **legal entity** (e.g. a company) represented by **its legal representative** (e.g. its Chairman).

Example: a holding company which decides on the purposes of data processing for its entities is the data controller

If two or more data controllers **jointly determine** the purposes and means of the processing, they are considered to be **joint data controllers** under article 24 of Law no. 1.565 of December 3, 2024.

Example: creation and use of a common platform by two data controllers who offer different services

To this end, they must determine **their respective responsibilities for compliance in a transparent arrangement**, particularly with regard to the exercise of the data subject's rights.

Irrespective of the terms of the arrangement, the data subject will be able to exercise his or her rights conferred by the law in respect of and against each of the controllers.

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

Data Protection Impact Assessment (DPIA or AIPD in French): a new instrument introduced by Law no. 1.565 of December 3, 2024, the data protection impact assessment is a study whose objective is to **determine and analyze** how the rights and freedoms of the individuals concerned by the processing **will be impacted before launching a new personal data processing**.

Any operation that could cause risks to the rights and freedoms of individuals does not automatically require an impact assessment.

Indeed, the Law only requires such an analysis when processing is likely to result in a **high risk to rights and freedoms**, particularly in the case of the use of a **new processing technology**.

The list of criteria for determining whether processing is likely to result in a high risk is established by Ministerial Oder No. 2025-361 of July 14, 2025 implementing Article 35 of Law no. 1.565 of December 3, 2024 on the protection of personal data.

Data Protection Officer or DPO: as provided for in articles 28, 29 and 30 of Law no. 1.565 of December 3, 2024, the DPO is the person within an entity who facilitates compliance with the data protection legislation and acts both as the **privileged contact** for all issues related to personal data, whether internal or arising from a data subject affected by processing, and as the **interlocutor of the APDP**.

Article 29 of the Law provides that with the exception of courts within the exercise of their judicial duties, the appointment of a DPO is mandatory in the following cases:

- the data processing is carried out by a **legal person governed by public law or a legal person governed by private law entrusted with a mission of general interest or a public service concession**;
- the core activities of the head of the data controller consist of processing operations, which by reason of their nature, scope or purposes, require **regular and systematic monitoring of the data subjects on a large scale**;

Example: profiling and rating for risk assessment purposes

- the basic activities of the organization consist of **large-scale processing of sensitive data or personal data relating to criminal convictions or offences**.

Example: processing of customer data by an insurance company or bank in the normal course of its business.

The Data Protection Officer has 5 missions:

- **inform and advise** the organization and the employees who carry out the processing of their obligations pursuant to the legislation currently in place in the Principality;
- monitor compliance with the personal data protection legislation and the organization's internal rules on the protection of personal data, including the allocation of responsibilities, **awareness-raising, and training of staff involved in the processing operations, and related audits**;
- **provide on-demand advice**, on data protection impact assessment;
- **cooperate** with the Data Protection Authority and be its contact point on matters relating to the processing;
- **submit requests for opinion to the Data Protection Authority** when they relate to 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 for the purposes of preventing, detecting, investigating, prosecuting or punishing criminal offences, including protection against and prevention of threats to public security.

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

Data subject: the **natural person** whose **data** are being processed. **Example**: when a store sets up a video surveillance system, the data subjects are all people who can enter the cameras' field of vision, i.e. employees, visitors, and any service provider working on site.

Although Law no. 1.165 of December 23, 1993 granted rights to **legal persons whose data were processed**, namely a right of opposition and a right of access, the new Law has **chosen not to maintain these rights**; practice has shown that the **exercise** of these rights is **extremely limited, if not non-existent and a source of difficulty**.

Data transfers: a data transfer is **any flow of data** to a country, territory, or an international organization outside the Principality.

This may involve a **physical transfer** or a **remote access**, either within a group or to a third party.

Example: the outsourcing of processing

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.

When the recipient country, territory, or international organization of the data does not appear on the list of countries with an adequate level of protection, the other scenarios provided for in articles 98, 99, and 100 are then to be considered successively:

- appropriate safeguards have been put in place by the data controller or the processor;
- the transfer meets the conditions of one of the derogations provided for by the Law;
- the 4 conditions provided for in paragraph 3 of article 96 are met;
- the transfer has been previously authorized by the APDP based on special protection measures or specific contractual clauses.

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

Encryption: defined in article 2 of Law no. 1.565 of December 3, 2024, as a « *cryptographic transformation process of data that makes them incomprehensible to anyone who does not have the decryption key* ».

It is a **reversible** process that makes the information in a document **unreadable** to preserve its **confidentiality.**

After encryption, it is therefore still possible to retrieve the initially encrypted data using a key, that is to say, a decryption algorithm.

Genetic data: defined in article 2 of Law no. 1.565 of December 3, 2024 as « *personal data relating to the hereditary or acquired genetic characteristics of a natural person that provide unique information about the physiology or health status of that natural person and that result, in particular, from an analysis of a biological sample from the person in question* ».

These data relate to **hereditary characteristics** and are used in particular in the **health sector**.

Examples:

- saliva
- blood
- hair bulb

They can also be used for **the purpose of identifying a person** through their genetic fingerprints.

Information society service: defined in article 2 of Law no. 1.565 of December 3, 2024, as « *any service, whether or not for consideration, provided at a distance and without the parties being simultaneously present, by electronic means and at the individual request of a recipient of services* ».

Examples:

- ordering clothes from a retail website
- online subscription to an electronic magazine

Personal data: defined in article 2 of Law no. 1.565 of December 3, 2024, as « *any information relating to a natural person identified or identifiable (referred to hereinafter as "data subject"). An "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifiersuch as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* ».

These data, which were qualified as " personal information" by Law no. 1.165 of December 23, 1993, as amended, have been detailed in relation to this old definition in order to specify that the following are **personal data**:

- **the genetic data** and
- **the location data**

Therefore, any information **relating to an individual** constitutes personal data.

It is important to distinguish between two types of personal data:

- **directly identifiable** data.

These data clearly identify the identity of a person. For example, a person’s first and last name.

- **indirectly identifying** data.

These data allow for the identification of a person in 2 ways:

- **by reference** to an identification number, for example, such as:
  - a phone number
  - a postal address or e-mail address
  - a social security number
  - a file number
  - a vehicle registration plate
  - an IP address
- **by elements specific to its physical identity**, such as:
  - a photo or video
  - a voice recording
  - a fingerprint

On the other hand, company contact details as well as generic e-mail addresses **are not**, in principle, considered to be personal data.

When it is possible to identify a person by **cross-referencing several pieces of information** such as gender, age, profession, and place of residence, the data are **always** considered personal.

Personal data processing: defined in article 2 of Law no. 1.565 of December 3, 2024 as « *any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, retrieval, consultation, use, adaptation or alteration, disclosure by transmission, dissemination or otherwise making available, the reconciliation or interconnection, limitation, the application of logical or arithmetic operations to such data* ».

Any operation involving personal data in this way constitutes processing within the meaning of the applicable legislation.

Examples:

- the collection of a person's name and e-mail address via the contact section of a website
- the recording of telephone conversations
- the implementation of a geolocation device on company vehicles

The processing **may or not be computerized**.

Example: a paper file.

However, processing relating to **personal and domestic activities** are excluded from the scope of Law no. 1.565 of December 3, 2024.

Example: the creation of a file containing friends' contact details.

Processing at a large scale (large-scale processing): defined in article 2 of Law no. 1.565 of December 3, 2024, a large-scale processing is « *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* ».

Example: processing of customer data in the regular course of business by an insurance company or a bank

Processor: defined in article 2 of the Law no. 1.565 of December 3, 2024, as « *the natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller* ».

In this respect, article 26 of Law no. 1.565 of December 3, 2024 stipulates that when the 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 **respect for the rights of data subjects**.

Furthermore, a processor can only act **on documented instructions** from the data controller.

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

Profiling: article 2 of Law no. 1.565 of December 3, 2024 defines profiling as « *any form of automated processing of personal data consisting in using such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict elements concerning that person's job performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements* ».

Example: the approval of a loan is conditioned on the result of an algorithm based on fully automated criteria.

Pseudonymization: pseudonymisation is defined in point 16 of article 2 of Law no. 1.565 of December 3, 2024 as « *the processing of personal data in such a way that these data can no longer be attributed to a specific data subject without recourse to additional information, provided that this additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person* ».

Also know as "reversible anonymisation", it consists of **replacing one attribute by another** in a record.

Hence, the physical (natural) persons may still be likely to be identified indirectly.

Example: for medical research, participants are identified solely by a patient number assigned by the investigating physician. However, the latter keeps a non-automated document in which this patient number is associated with the name and surname of the patient to whom it has been assigned, so that they can be identified if necessary.

[For more information, refer to the factsheet **Anonymyzation or pseudonymization**]

Recipient: defined in article 2 of Law no. 1.565 of December 3, 2024 as the « *natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not* ».

This same article further specifies that « *public authorities which may receive personal data in the framework of a particular inquiry shall not be regarded as recipients* ».

The following are therefore considered as recipients: persons, departments, divisions, etc. other than the public authorities in the context of a specific investigation, who receive the data.

Example: commercial partners

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

Representative: pursuant to article 2 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. The data subjects 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

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

Sensitive data: defined by Article 2 of Law No. 1.565 of December 3, 2024 as « *personal data that reveal either directly or indirectly, opinions or political affiliations, racial or ethnic origins, religious, philosophical or trade union beliefs, or genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning a natural person's health, sex life or sexual orientation* ».

Sensitive data are particular personal data due to their **highly private nature**.

Article 7 of the Law establishes the **prohibition of processing sensitive data principle**.

However, the Law provides for **13 exceptions** to this principle, notably:

- for processing based on the **explicit consent of the data subject**;
- for the processing **necessary to safeguard the vital interests of the data subject or of another natural person**, in the event that the person cannot validly give consent due to an impairment of his or her faculties, **physical or legal incapacity** or a complete material impossibility;
- for processing relating to data data manifestly **made public by the data subject**.