GDPR CARPA

CNPD

# GDPR CERTIFICATION

*Build trust, demonstrate compliance*

*Compliance* *Transparency* *Trust*

https://cnpd.public.lu/en.html
certification@cnpd.lu

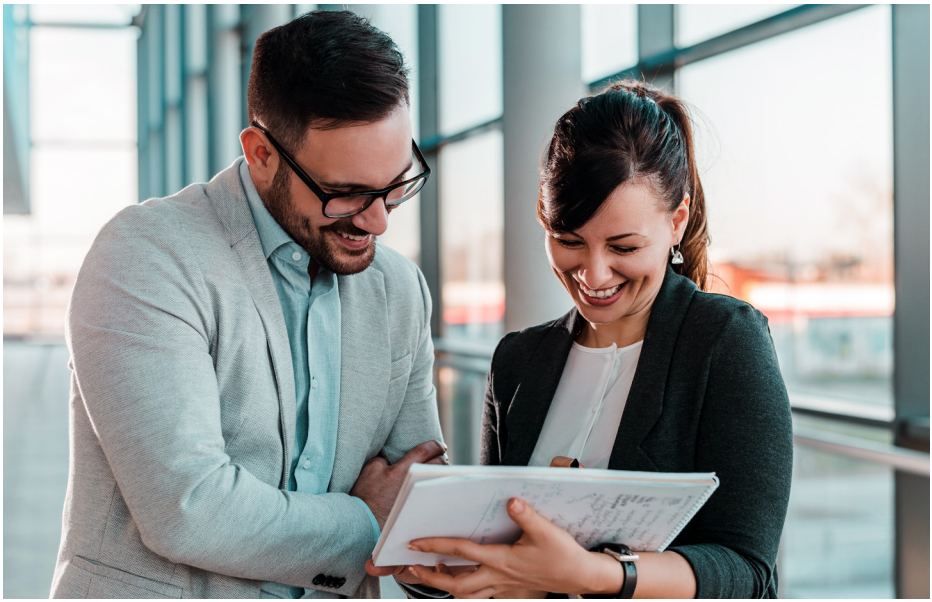
GDPR
CARPA
CNPD

# What is the GDPR certification?

A certification is a compliance tool under the General Data Protection Regulation (GDPR), aimed at professionals who wish to demonstrate the level of data protection of their processing operations.

It certifies that the processing of personal data complies with the criteria of a certification scheme, approved either by the CNPD at the national level or by the European Data Protection Board (EDPB) at the European level. This compliance is verified by an approved certification body.

Certification is valued by the regulation as a guarantee of compliance and trust.



## How may a certification benefit you?

By integrating data protection from the design phase of services and processes onward, in line with Article 25.3 of the GDPR, the organisation enhances its consistency and improves its overall efficiency. Certification accompanies this process by structuring practices, clarifying responsibilities and making data protection sustainable.

It represents both a lever for operational efficiency and a guarantee of good governance of personal data. It also reduces risk, facilitates internal and external audits, and builds trust among clients and partners.

Finally, certification values stakeholders, including the organisation and the data protection officer. It recognises their commitment to data protection, in an environment where compliance is becoming a growing factor of differentiation.

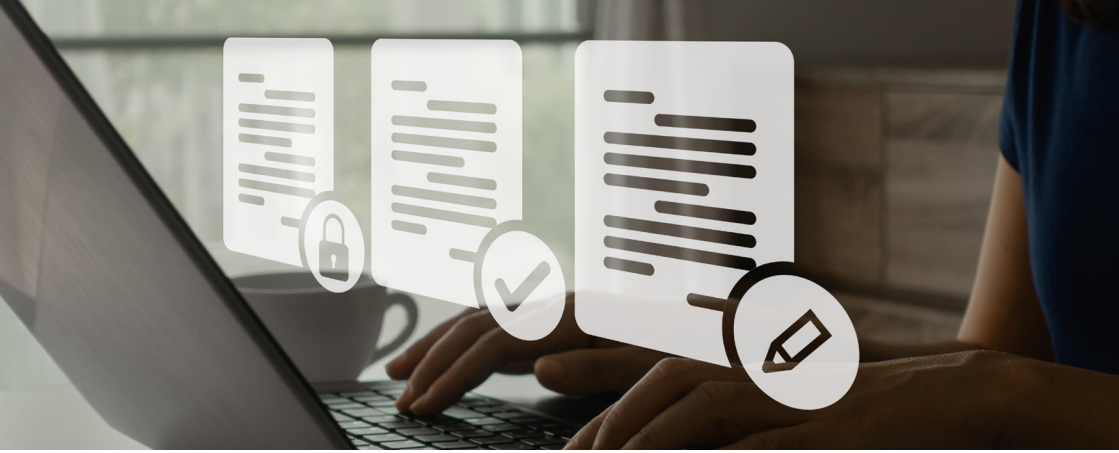
## Good to know:

### Consideration of certification in the decision to impose an administrative fine (Art. 83 of the GDPR):

- It can be considered as proof of good faith, by demonstrating the will to comply with the regulation, and of diligence, by attesting to the effective implementation of technical and organisational measures.
- It can also reduce the severity of a sanction, as long as the organisation is able to demonstrate concretely the technical and organisational measures it has put in place.

## Please note:

This does not guarantee that no sanction will be imposed.



## What do the criteria for a GDPR certification entail?

In accordance with Article 42 and recital 100 of the GDPR, the criteria aim to assess compliance with the principles and obligations of the regulation. In this context, they may cover different aspects of data protection, such as: data governance (privacy by design, the role of the DPO, etc.), compliance with the fundamental principles of processing (lawfulness, minimisation, purpose limitation, etc.), considering the rights of data subjects (access, rectification, erasure, etc.) or keeping a register of processing operations.

## Should your organisation consider certification?

Any public or private entity that processes personal data can apply for GDPR certification.

Certification may cover different aspects of personal data processing operations, such as the processing of personal data by a website or online service, storage services, customer data management, human resources or medical data processing.

In this context, the certification body may need to assess both the technical systems used for the processing operations (infrastructure, hardware, software) and the processes or procedures related to the processing operations.

# How to obtain a GDPR certification in Luxembourg

**1**

## Choose a recognised certification scheme

Examples:

- GDPR-CARPA (Luxembourg)
- Europrivacy (European Data Protection Label)

**2**

## Contact an accredited certification body

Certification bodies approved and established in Luxembourg

**3**

## Prepare your compliance case

Evidence, internal policies, measures put in place

**4**

## Undergo an independent evaluation

Certification body verifies compliance and issues certification

**5**

## Maintain compliance

- Certification valid for 3 years (in practice)
- Periodic monitoring
- Conformity to be maintained continuously

## What is the cost of a certification?

The rates are set directly by the certification body on the basis of several elements, such as the complexity of the treatments to be assessed, the size of the organisation and the scope of the certification scheme chosen. The cost usually covers the analysis of the assignment, the issuance of the certificate and the surveillance audits.

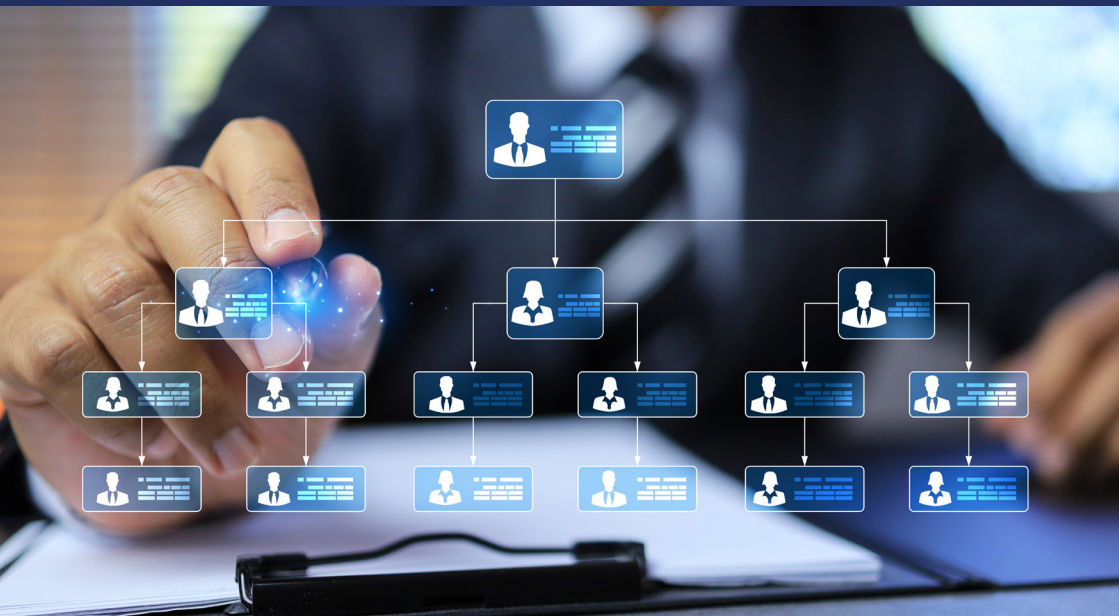
## Please note:

The CNPD does not issue certification or intervene in pricing.

## Who can issue a GDPR certification in Luxembourg?

The list of certification bodies accredited by the CNPD is available on the authority's website.

European certification, also known as the European Data Protection Seal, may be issued by certification bodies duly accredited in one of the Member States and will be recognised throughout the European Economic Area, including Luxembourg.



# What are the certification schemes established in Luxembourg?

- **GDPR-CARPA**, a national scheme designed to reflect the specificities of the Luxembourg context

The GDPR-CARPA certification is a national scheme for controllers and processors established in Luxembourg, for processing operations carried out on the Luxembourg territory. Developed by the supervisory authority itself (CNPD), it is based on the ISAE 3000 standard, thus ensuring high standards and strengthening the trust of the data subjects.

- **Europrivacy**, a European scheme aligned with GDPR expectations and recognised across borders

The Europrivacy certification is a European data protection label recognised by the EDPB and suitable for both controllers and processors. It is applicable to processing operations carried out throughout the European Economic Area.

**Explore the EDPB-approved certification schemes**

## DISCOVER ANOTHER COMPLIANCE TOOL

In addition to certification, a group of organisations in a specific sector may develop their own GDPR code of conduct or choose to adhere to an already existing code. Once approved by the CNPD, this tool makes it possible to demonstrate compliance with the GDPR, while considering the operational needs of the sector concerned. The benefits are comparable to those of certification, particularly in terms of governance and monitoring.

Example of a code of conduct in Luxembourg:

The Code of Conduct for the Temporary Work Sector, approved by the CNPD in 2024, is the first to be recognised at the national level.

At the European level, you can also consult the list of codes of conduct approved by the EDPB by scanning the QR code on the left.

To discover all the compliance tools proposed by the CNPD, scan the following QR code:

## GET TO KNOW THE GDPR CERTIFICATION

- **Explore the framework for certification criteria**
- **Identify accredited certification bodies in Luxembourg**
- **Discover the GDPR-CARPA certification scheme**