March 2026

Europrivacy Certification – GDPR Compliance and Process Optimization

Privacy, Compliance and Cybersecurity Area

ECIJA
Av. Diagonal, 458, planta 7ª
08006 Barcelona Tel: +34 933 808 255
www.ecija.com

ECIJA | Av. Diagonal, 458, planta 7ª
08006 Barcelona · Tel: +34 933 808 255
www.ecija.com

Briefing Document

Barcelona, March 2026

Europrivacy Certification – GDPR Compliance and Process Optimization

Introduction

Europrivacy is a certification scheme designed to assess the compliance of personal data processing activities and to issue compliance certifications in accordance with Article 42 of the General Data Protection Regulation (GDPR).

Europrivacy has been officially approved by the European Data Protection Board ("EDPB") as the first European Data Protection Seal, which confirms its validity and applicability across all EU jurisdictions, as well as the robustness of its methodology, based on international ISO standards.

The scheme is closely aligned with international certification standards, in particular ISO/IEC 17065 and ISO/IEC 17021-1, and its integration with standards such as ISO 27001 and ISO 27701 facilitates synergies with information security management systems, enabling the optimization of processes and the strengthening of privacy policies in a comprehensive manner within organizations. Furthermore, Europrivacy may be extended to other complementary regulations and emerging technologies.

It is a voluntary mechanism that enables data controllers and data processors to demonstrate, independently and impartially, that their processing activities comply with applicable data protection requirements.

Regulatory Framework and Key Features

The GDPR establishes, in Articles 42 and 43, the possibility of developing certification mechanisms, which constitute an appropriate tool for demonstrating compliance with data protection regulations. These mechanisms allow organizations, whether acting as data controllers or data processors, to obtain certification attesting to the compliance of such processing activities with the principles and requirements of the GDPR.

To ensure the consistent and effective application of these mechanisms across the European Union, the European Data Protection Board has issued various guidelines on their implementation and supervision. The most relevant include:

- Guidelines 1/2018 on certification and the identification of certification criteria in accordance with Articles 42 and 43 of the GDPR: They provide a detailed interpretation of the requirements for obtaining certification, defining criteria and procedures for their implementation.
- Guidelines 4/2018 on the accreditation of certification bodies in accordance with Article 43 of the GDPR: They specify the requirements and accreditation criteria for bodies responsible for issuing certifications, thereby ensuring consistent standards across the EU.
- Guidelines 07/2022 on certification as a tool for international data transfers: They detail how certification may be used to ensure compliance with requirements relating to transfers of

personal data to third countries or international organizations. It should be noted that, beyond the mere obtaining of a certificate, these mechanisms promote a culture of proactive compliance and transparency, encouraging organizations to adopt personal data protection practices that go beyond the minimum requirements established by regulation, for the benefit of both individuals and the sustainable development of the digital economy.

Who Is It For?

Europrivacy certification is intended for entities that carry out personal data processing and wish to demonstrate, in a transparent and verifiable manner, compliance with the GDPR in relation to their various processing activities and, where applicable, with complementary national or sector-specific obligations. In particular, it is aimed at:

- Data controllers and data processors. Organizations that manage personal data and need to demonstrate their compliance through an independent assessment, whether they are established within or outside the European Union.
- Organizations of any size. Although particular attention is given to entities handling large volumes of data or processing sensitive information, Europrivacy is open to both large corporations and SMEs, provided they have a Record of Processing Activities (RoPA) and a Data Protection Officer (DPO).
- Entities with cross-functional activities. Organizations operating across multiple sectors that need to certify not only compliance with the GDPR, but also the integration of specific controls tailored to their particular context, whether due to national obligations or the use of emerging technologies, such as Artificial Intelligence (AI).
- Organizations interested in implementing emerging technologies. Those using innovative solutions such as the Internet of Things (IoT), artificial intelligence or blockchain, among others, and requiring a hybrid approach combining universal criteria with complementary controls specific to their risks and technological challenges.

Benefits of Certification

Evidence of Compliance

Firstly, Europrivacy is a means of demonstrating regulatory compliance, as it is based on the requirements of the GDPR and uses a comprehensive and verified methodology to ensure that processing activities are aligned with personal data protection regulations. In this regard, objective evidence is provided to demonstrate an organization's commitment to data protection, such as:

- Regulatory alignment. Europrivacy is based on Article 42 GDPR, ensuring that each assessment is aligned with regulatory requirements. In this sense, the seal certifies specific data processing activities; therefore, the entirety of the activities carried out by each data controller or processor is not subject to certification.
- Robust and multidimensional methodology. With the support of various European projects, the certification methodology is deployed on the basis of a set of 213 criteria and 659 requirements, which enable the systematic identification of the level of compliance.
- Independent assessment. The involvement of qualified third parties ensures an objective evaluation free from conflicts of interest.

Reputation and Trust

The second key aspect lies in Europrivacy's ability to strengthen reputation and trust among data subjects, as well as business partners and clients. As it has been approved by the European Data Protection Board and involves the issuance of a formally approved data protection seal, this mechanism

(i) certifies compliance and (ii) immediately communicates a commitment to high standards of privacy and security, thereby reinforcing the credibility and prestige of certified organizations.

Adaptability and Compatibility with Other Certifications

The third key pillar lies in its ability to offer an innovative and flexible model that adapts to the complexity of the current digital environment, as it provides:

- Hybrid approach. It combines universal criteria with complementary controls specific to sectors or emerging technologies – such as artificial intelligence, IoT or blockchain.
- Extensibility and flexibility. It allows the integration of national obligations and adaptation to complementary regulatory frameworks, avoiding duplication and optimizing certification.
- Integration with international standards. Its consistency with international standards facilitates its combination with other schemes (such as ISO/IEC 27001 or ISO/IEC 27701), enhancing competitiveness in the global market.
- Innovation and continuous updating. The incorporation of updates based on technological developments and the criteria of data protection authorities ensures that the scheme remains relevant and at the forefront.

Differences from Other Privacy Certifications

In the current data protection landscape, the existence of various certification systems has led organizations to adopt mechanisms that ensure regulatory compliance. In this context, the Europrivacy seal stands out due to:

- Official recognition. It has been developed in strict accordance with the EDPB guidelines and has been recognized as a European Data Protection Seal. This recognition ensures that the certification is applied uniformly across the EU, on the basis of compliance with GDPR requirements.
- Proactive approach. Europrivacy is not merely a regulatory verification process, but rather seeks to actively promote a culture of privacy within organizations.
- Applicability and territorial scope. Due to its European nature and alignment with EDPB guidelines, Europrivacy has uniform validity and applicability across all EU jurisdictions, resulting in a highly beneficial approach for organizations with cross-border operations.
- Factor to be taken into account in the imposition of administrative fines. Article 83(2) GDPR provides that, when deciding whether to impose an administrative fine and its amount, due account shall be taken, among other factors, of adherence to certification mechanisms approved pursuant to Article 42 GDPR as a mitigating factor.

Scope of Certification

The scope of Europrivacy certification is defined by the organization, which must determine the processing activities to be subject to assessment and certification. Taking the above into account, the organization may define the scope of certification based on its specific circumstances and objectives.

To be eligible for certification, the organization must have a minimum structure in place, including the appointment of a Data Protection Officer (DPO), whether internal or external. This requirement is essential to ensure the internal capacity necessary to monitor and maintain regulatory compliance.

It should be noted that certain application domains are excluded from regular certification (e.g., the processing of genetic information), in the sense that they are subject to specific obligations that vary significantly depending on national legislation. To avoid misinterpretations, Europrivacy maintains an updated list of domains excluded from the standard scope of the scheme.

Implementation, Certification and Maintenance Process

Implementation and Certification

The process for obtaining Europrivacy certification follows a systematic approach that ensures independent assessment and validation of regulatory compliance. The main steps are:

- Certification application: The organization must complete the Europrivacy Application Form, detailing the scope of the processing to be certified.
- Initial review of the application: The certification body verifies that the application and scope comply with the requirements of the scheme and the EDPB guidelines.
- Conformity assessment: A formal audit is carried out in which an independent auditor reviews the documentation, policies, processes, and security measures applied to the data processing.
- Identification of non-conformities: If non-conformities are identified, they are classified as minor or major, and a timeframe is provided for their remediation.
- Final auditor's report: Once the non-conformities have been addressed, a final report is issued validating the compliance of the data processing with the requirements of the Europrivacy scheme.
- Certification decision: The certification body reviews the report and, if the requirements are met, issues the Europrivacy certification.
- Publication of the certificate: The certification is registered and published in the Europrivacy Register of Certificates, allowing for its validation and recognition at the European level.

Maintenance and Renewal of Certification

To ensure the continuity of Europrivacy certification, organizations must comply with a maintenance and renewal process consisting of the following phases:

- Maintenance of compliance: The certified organization must ensure that the data processing continues to comply with the certification criteria and with any regulatory updates.
- Supervisory audits: Annual surveillance audits are carried out to verify ongoing compliance. These audits must be conducted as follows:
    - First surveillance audit: within 12 months following certification.
    - Second surveillance audit: within 24 months following certification.
- Review in case of regulatory or organizational changes: If significant changes occur in the applicable regulations, the organization must update its documentation and ensure compliance with the new requirements.
- Renewal of certification: The certification is valid for three years. Before its expiry, the organization must undergo a recertification process, which involves an audit similar to the initial one in order to assess continued compliance with the Europrivacy scheme.

This process ensures that the certification remains valid and reliable, guaranteeing that organizations maintain the highest standards in data protection.

Recommendations and Reference

To optimize the Europrivacy certification process, it is recommended to carry out a prior self-assessment, clearly define the processing to be certified, maintain up-to-date documentation, and rely on data protection experts. In addition, it is essential to stay informed about regulatory changes and to prepare for supervisory audits in order to ensure the continuity of compliance.

Some useful resources to learn more about Europrivacy include the **Europrivacy Community**, which provides access to guidelines and templates, **the official Europrivacy website** with information on certification, and the **European Data Protection Board** (EDPB), which issues updated guidelines.

ECIJA, having successfully completed the recognition process carried out by the entity managing Europrivacy, is a global expert partner. This means that **it has certified professionals capable of preparing for certification processes and auditing the requirements for obtaining the Europrivacy seal, enabling us to effectively support companies throughout the process of obtaining the seal**.

For further information about Europrivacy, please contact: europrivacy.barcelona@ecija.com.

Key developments in 2025

Among the most relevant developments is the publication by Europrivacy of Interprivacy, an international data protection certification system aimed at demonstrating compliance with the main privacy regulations at a global level. Unlike Europrivacy, which is focused on the European GDPR, Interprivacy adopts a geographically neutral approach and is designed to certify simultaneous compliance with different international regulatory frameworks, such as the GDPR, Convention 108+, the EU–U.S. Data Privacy Framework, the CBPR/APEC framework, or Ibero-American standards, among others.

This scheme is particularly relevant for organizations with cross-border activities, as it facilitates the establishment of a single global compliance framework, contributes to reducing legal risks, and simplifies privacy management, particularly with regard to international data transfers.

Alongside Interprivacy, it is also particularly relevant to note that Europrivacy has published a series of **regulatory extensions and other complementary schemes** that allow the assessment and certification of compliance with additional regulatory frameworks, including the NIS2 Directive, as well as other regulations such as ePrivacy, the Data Act, the Data Governance Act, DORA or the Cyber Resilience Act (CRA). These extensions may be combined with Europrivacy certification or used independently, applying a consistent assessment methodology.

However, it should be noted that neither Interprivacy nor these regulatory extensions and complementary schemes qualify as official certifications under Articles 42 and 43 of the GDPR, nor do they constitute seals recognized by the European Data Protection Board.

ECIJA & Asociados Abogados Barcelona, S.L., in addition to its status as an Official Europrivacy Partner, is an official partner for the implementation of the Interprivacy certification scheme, as well as the regulatory extensions and other complementary schemes published by Europrivacy.

Trends in 2026

Over the past year, a progressive increase in the adoption of Europrivacy certification schemes has been observed[1]. This growth reflects greater regulatory maturity and an increasing demand from organizations for formal mechanisms that enable them to demonstrate compliance with data protection regulations in an objective and verifiable manner.

The most recent certifications granted have been mainly concentrated in sectors such as digital services, technology platforms, artificial intelligence-based solutions, as well as regulated sectors such as financial services, insurance, and energy. In particular, processing activities associated with the digital contracting of products and services have been certified at the European level, including functionalities such as web browsing, automated customer service systems, and electronic communications with clients. This

[1] For further information on the certificates granted, the official registry may be consulted: Europrivacy Registry of Certificates | Europrivacy Certification

demonstrates the increasing use of certification in high-volume and commercially relevant digital interaction environments.

At ECIJA, we observe a growing interest in using certification not only as a regulatory compliance tool, but also as a strategic element of competitive differentiation, particularly in relationships between data controllers and data processors. In this context, certification may be particularly useful for data processors, as it allows them to objectively demonstrate their compliance with data protection regulations while also streamlining onboarding and contracting processes with their clients.

Departamento de Privacidad, *Compliance y* Ciberseguridad
Ecija Barcelona
T +34 933 808 255
europrivacy.barcelona@ecija.com
www.ecija.com