Europrivacy.com
Privacy Audit and Certification

Europrivacy™/®
Certification Scheme General Specification and Requirements

Identifier:	EP-CS.1
Version:	77
Date:	24 January 2024
Publication status:	**Confidential**
Websites:	http://www.europrivacy.com
	www.eccpcenter.com
Contact:	contact@europrivacy.com

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Table of Contents

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

1. Introduction and Acknowledgements

With the evolution of Information and Communication Technologies (ICT), data protection has become a growing concern for individuals and societies. Formal legislation and regulations have been adopted by the European Union and individual countries to protect fundamental rights and freedoms of natural persons and in particular, their right to the protection of personal data.

The Europrivacy Certification Scheme has been developed to assess the compliance of personal data processing operations by Data Controllers and Processors with the obligations of the European General Data Protection Regulation (GDPR), and to be easily extendable to complementary data protection obligations, such as national regulations and/or domain-specific obligations.

The Europrivacy criteria have been approved by the European Data Protection Board (EDPB) to serve as a formal European Data Protection Seal applicable to data processing activities performed by data controllers or processors.

The use of the Certification Scheme methodology and criteria enables the reduction of risks for all parties. Where personal data processing is subject to close monitoring based on clear requirements, risks for the data subjects, data controllers, and data processors are lessened.

The Certification Scheme and its criteria have been designed to be used:

a) as a formal European Data Protection Seal under Art. 42 GDPR;
b) as a mechanism for international data transfers by Data Importers[1];
c) as a certification mechanism compliant with the GDPR and recognisable by other jurisdictions[2];
d) for internal audits and voluntary certifications without the benefits and advantages of an official GDPR certification, to the condition that there is no risk of confusion with regular certification under the GDPR;
e) for documenting compliance and reducing risks of non-compliance, without necessarily pursuing formal certification.

The Europrivacy Certification Scheme has been developed with the support of European Research projects co-founded by the European Commission and the Swiss Ministry for Research and Education. The initial Certification Scheme has been developed by Archimede Solutions SARL. The role and function of Scheme Owner have been delegated to the European Centre for Certification and Privacy (ECCP) in Luxembourg. ECCP is in charge of overviewing, improving, and updating the Certification Scheme with the support of an international board of experts in data protection, ICT security, and certification (hereafter referred to as “Europrivacy International Board of Experts”).

The Certification Scheme is primarily intended to certify compliance of personal data processing under ISO/IEC 17065. It has been optimised to take full advantage of ISO/IEC 17065’s ability to be extended towards complementary certification requirements, such as ISO/IEC 17021-1. Where applicable, Europrivacy can also be applied to different scopes of certification, provided it complies with the applicable regulations and complementary requirements.

[1] The use of Europrivacy as a mechanism for international data transfer under Art. 46 GDPR is pending EDPB approval. Data Importers not subject to the GDPR must adopt an adequate contractually binding instrument.
[2] The formal recognition in other jurisdictions may be subject to complementary requirements.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

2. Scope and Purpose of the Certification Scheme

2.1. Scope of this Document

This document presents the general specifications and requirements of the Europrivacy Certification Scheme (hereafter referred to as the "Certification Scheme"), including its policies, processes, and procedures to be applied and respected by certification bodies (hereafter referred to as the "Certification Body"). This principal document is completed by a set of complementary documents providing more detailed information, which are also part of the Certification Scheme.

Sections 2 to 5 are focused on the general overview of Europrivacy, including definitions and references.

Sections 6 to 11 are focused on the certification process, including the criteria.

Sections 12 to 17 are focused on the organisational requirements for the Certification Body.

Sections 18 to 19 are focused on the Certification Scheme management, including accreditation and licensing.

2.2. Purpose and Scope of Europrivacy Certification

Europrivacy has been designed to provide a clear and comprehensive Certification Scheme on compliance of data processing with personal data protection regulations, with a focus on the GDPR. It intends to provide an independent, impartial, and reasonable assurance level of data processing compliance with the GDPR and the corresponding Data Subjects' fundamental rights, and where applicable, with complementary requirements, such as national regulations and domain-specific requirements.

It has been designed to respect international law, ISO principles, and World Trade Organisation requirements.

The Certification Scheme has been researched and structured to be applicable to diverse data processing activities performed by data controllers and/or data processors (hereafter 'Applicant'). It has been developed with specific attention to the risks emerging from the use of innovative technologies, such as the Internet of Things and Artificial Intelligence. Its architecture enables to extend its core criteria with complementary national and domain-specific requirements.

Europrivacy has been structured to be reliable and cost-efficient for SMEs. Where applicable, it complements and leverages on other certifications, such as ISO/IEC 27001 and 27701, in order to avoid duplicating certification efforts and costs.

The scope of Europrivacy certification is subject to some restrictions:

- The Applicant shall have designated a Data Protection Officer (or equivalent function that can be external) in charge of monitoring the compliance of the data processing activities to be certified;
- The Applicant shall have a record of its personal Data Processing activities;
- ECCP keeps a list of application domains that are excluded from the scope of regular Europrivacy certification. In case of doubt on the applicability of the certification to specific domains, the Applicant or the Certification Body shall contact ECCP.

Europrivacy certification intends to provide an independent, impartial, and reasonable assurance level of data processing compliance with the European General Data Protection Regulation and, where applicable, with complementary data protection requirements, such as national regulations or domain-specific requirements, by using Certification Extensions (See Section 11.1).

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

2.2.1. Normative Scope of Certification

The Europrivacy Certification Scheme has been designed to address the requirements of the GDPR, namely:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The Certification Scheme focuses on the obligations of the GDPR whose non-compliance could put the Data Subjects' rights and freedoms, their personal data, or the Applicant at risk.

Delivering GDPR certification in conformity with Articles 42 and 43 GDPR requires compliance with:

- the applicable European Data Protection Board guidelines, including:
  - Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679);
  - Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679;
  - Guidelines 7/2022 on Certification as a Tool for Transfers;
- the applicable obligations provided by EU Member States' data protection laws.

While the Certification Scheme is primarily focused on compliance with the GDPR, the Applicant and the Certification Body can agree to extend the Normative Scope of certification by adding complementary requirements, such as:

- European Directives and Regulations, such as the ePrivacy and NIS Directives[3] ;
- National data protection regulations;
- Domain-specific or ISO/IEC requirements.

Regardless of the Extension, the certification shall always demonstrate compliance with the regular GDPR requirements too. Extension of the Normative Scope shall be clearly communicated with the certificate, as provided in 11.1.

The Certification Scheme is intended to be adapted to subsequent evolutions and updates of the above-mentioned regulations, including, where applicable, to the jurisprudence and to the evolution of the technological environment.

2.2.2. Material Scope of Certification

The Certification Scheme has been researched, developed, and specified to deliver comprehensive, homogeneous, and systematic assessments of data protection compliance. While **its primary focus is to certify processing operations of personal data**, the Certification Scheme has been designed to be as comprehensive as possible by aligning with applicable ISO requirements for assessing products, processes, services (ISO/IEC 17065), as well as with ISO/IEC 17021-1, with a focus on data protection.

According to the Target of Evaluation, specific and complementary checks and controls specified by the Scheme Owner shall be applied by the Auditors. This mechanism enables to apply the Certification Scheme to diverse data processing activities by addressing domain- and technology-specific requirements.

2.2.3. Geographic Scope of Certification

The geographic scope of the Certification Scheme is not formally limited and can be used by Applicants , but:

a. European Data Protection Seals delivered under the GDPR to Applicants located outside of the EEA are subject to complementary requirements.[4]
b. The Certification Criteria can be difficult and potentially impossible to satisfy in countries whose legal environment does not provide adequate protection to personal data and data subject rights.

2.2.4. Clarity of the Scope and Target of Evaluation of Certification

The Normative Scope of certification, as well as the Targets of Evaluation of each delivered certificate, shall be clearly specified and designated. Delivered certificates are published in the Europrivacy Registry of Certificates (hereafter 'Registry') and can be easily accessed and verified thanks to the certificate identifier and the website address attached to each and every mark of conformity.

[3] Directive (EU) 2002/58/EC and 2016/1148/EC of the European Parliament and of the Council
[4] The applicability of Europrivacy to non-EEA Applicants is under review by EDPB and pending their decision.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

2.3. Alignment with the European Data Protection Regulations

2.3.1. Adaptation to the Evolution of Data Protection Regulations

As data protection regulations are evolving, the Certification Scheme is expected to be regularly updated to take into account the evolution of the legal environment and jurisprudence related to data protection. It is also intended to enable continuous improvement process.

The Scheme Owner, supported by an International Board of Experts, is in charge of reviewing and updating the Certification Scheme.

2.3.2. Certification Scheme Requirements

The Certification Scheme has been designed by taking into account the following elements:

a) it shall be accessible to micro-, small- and medium-sized enterprises;
b) it is available via a process that is transparent;
c) it makes clear that the certification does not reduce the responsibility of the Applicant for complying with its data protection regulatory obligations;
d) it follows the criteria approved by the European Data Protection Board and/or the competent Data Protection Authority;
e) it is compliant with the relevant requirements of the applicable ISO/IEC standards;
f) the Applicant is expected to provide the Certification Body with all information and access to its processing activities that are necessary to conduct the certification procedure;
g) the Certification lasts for a maximum period of three years;
h) certification renewal is granted on condition that the Applicant meets the conditions and requirements established for the said renewal.

2.3.3. Certification Bodies Requirements

The Certification Body shall comply with the applicable accreditation requirements and regulations.

According to the GDPR, the Certification Body should specifically:

a) **demonstrate an appropriate level of expertise in data protection**;
b) **demonstrate independence and impartiality**;
c) **comply with the ISO/IEC 17065**[5] **requirements** for delivering certifications, including adequate procedures and structures:
   - to issue, periodically review, and withdraw certifications, seals, and marks;
   - to control that certified entities are transparent to data subjects and the public;
   - to handle complaints about infringements of the certification, and/or about the manner in which the certification has been, or is being, implemented;
d) **comply with the applicable accreditation requirements established by the competent Data Protection Authority**, such as:
   - demonstrating adequate processes for data protection when processing personal data;
   - being accredited by the competent Data Protection or Accreditation Authority.

External bodies, such as laboratories and Auditors, performing part of certification activities on behalf of a Certification Body shall demonstrate adequate expertise in data protection, as well as appropriate knowledge of the Certification Scheme relevant to their work.

National and European Data Protection Authorities do not need a formal licence, provided they comply with applicable regulations, the Certification Scheme requirements, and that they use the latter with the agreement of the Scheme Owner.

[5] ISO/IEC 17065/2012 or posterior (latest version available).

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

2.4. Continuous Improvement Process

Ensuring effective data protection requires to take into account the evolution of the norm (jurisprudence, EDPB publications, etc.), the technological environment (which may affect, for instance, the risk of deanonymisation of data), and the lessons learnt through the practice.

The Certification Scheme and its related resources, including its criteria and checks and controls, can be reviewed and updated whenever required through a continuous improvement process to address these changes and to avoid the emergence of gaps between the Certification Scheme requirements and the legal requirements.

It also leverages the experience of the Auditors and Technical Experts who are invited to submit improvement suggestions to the Scheme Owner. Submitted suggestions for improvement are reviewed by the International Board of Experts of the Scheme Owner and approved enhancements are released in updated versions. Any adaptations shall contribute to enhancing the applicability and reliability of the certification process and shall not weaken it.

The following drawing summarises the process:

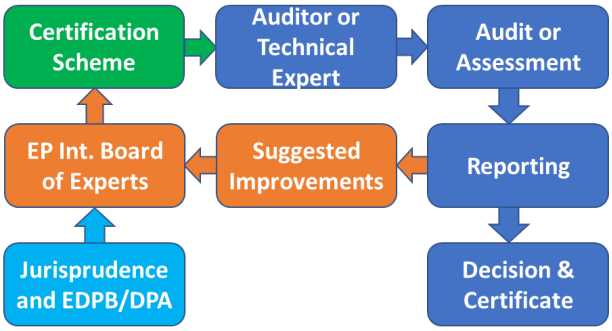

Figure 1 Europrivacy Certification Scheme Continuous Improvement Process

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

2.5. Inherent Limits to Certification

2.5.1. General Limitation

A Europrivacy certificate is the final outcome of a certification process, indicating that a certification has been performed according to the requirements and procedures of the referred Certification Scheme and that the certified Target of Evaluation has successfully met the specified requirements of the Certification Scheme for the Target of Evaluation during the assessment and/or audit process, and the Applicant has committed to comply with them for the duration of the Certificate.

A certification process is based on the findings identified by the Auditor after following a clearly specified and systematic methodology. It relies on samples analysed and/or targeted audits performed at a given period of time. A certificate is a professional and impartial indication of conformance verified by an independent third party, but it cannot guarantee that the certified Target of Evaluation is and will be free of any Non-Conformity. Legal conformance remains the sole responsibility of the Applicant who must continuously ensure that its certified Target of Evaluation complies fully with the requirements of the Certification Scheme and the applicable data protection regulations.

A certification is neither a recommendation for the use of a product, process, service, or management system nor a guarantee that it is totally free from any exploitable vulnerability.

As a reminder:

1) The Scheme Owner's primary role is to maintain and update the Certification Scheme;
2) The Certification Body is responsible for assessing, auditing and taking the decision to certify the evaluated Target of Evaluation as compliant with the Certification Scheme requirements;
3) The Applicant remains solely responsible for the compliance of its personal data processing with the data protection regulations.

Neither the Certification Body nor the Scheme Owner is liable for any loss or damage whatsoever and howsoever arising as a result of the use of a certified product, process, service, or any other element covered by a certification.

The Europrivacy certificate does not free the certificate holder from its legal responsibility, including any non-compliance with applicable data protection regulations.

The use of the Certification Scheme is conditional on the acceptance of the Europrivacy General Terms and Conditions that are made available online on the Europrivacy website: https://europrivacy.com

2.5.2. GDPR Specific Limitations

Certification delivered under Articles 42 and 43 of the GDPR shall comply with the European Data Protection Board's policy, guidelines, and requirements, such as:

- Requiring that the scope of certification focuses on personal data processing.

2.5.3. Restrictions to Unregulated Use of the Certification Scheme and Criteria

Europrivacy is intended to deliver certifications conforming to the GDPR requirements and to the applicable national data protection regulation. Its criteria can be used as a basis to deliver certifications outside the scope of the GDPR to the condition that it prevents the risk of confusion with GDPR certifications. For instance, the delivered certificates shall use a different name and mark of conformity. Such certifications shall be subject to complementary rules to be specified by the Scheme Owner in a separate document. They shall also comply with applicable law and intellectual property rights. Certifications delivered outside of the GDPR are not recognised as GDPR certifications.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

3. Reference Documents

3.1. Normative and Prescriptive References

The Certification Scheme refers to several documents, including external reference documents, such as ISO standards and data protection regulations, as well as internal reference documents that complement and further detail the Certification Scheme.

3.1.1. Europrivacy Complementary Normative Documents

The Certification Scheme is complemented by several documents maintained by ECCP and its International Board of Experts, including:

a) Europrivacy General Terms and Conditions;
b) Europrivacy Certification Scope Limitations;
c) Europrivacy Guidelines on the Use of Criteria, Checks and Controls;
d) Europrivacy list of Criteria, Checks and Controls to be used by the Auditors for Europrivacy certifications;
e) Europrivacy Certification Scheme Extensions and Adaptations (that are optional);
f) Management of Competencies of Personnel Involved in Europrivacy Certifications;
g) Europrivacy Rules and Guidelines on the Use of Certificates, Logos and Marks of Conformity;
h) Europrivacy Communication and Marketing Rules.

The normative documents are complemented by a number of informative documents, including guidelines and templates. All Europrivacy formal and official documentation is maintained up-to-date and made available on the Europrivacy Community and Resources website: https://community.europrivacy.com

3.1.2. Main External Normative References

Where applicable, the following normative references shall be used by the Certification Body when applying the Certification Scheme and the certification process:

- European Regulation (EU) 2016/679 of the European Parliament and of the Council, also known as the European General Data Protection Regulation (GDPR);
- Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679);
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (2016/679);
- Guidelines 7/2022 on Certification as a Tool for Transfers;
- ISO/IEC 17065, Conformity assessment – Requirements for bodies certifying products, processes and services (and where applicable its national additions);
- ISO/IEC 17021-1, Conformity assessment – Requirements for bodies providing audit and certification of management systems;
- ISO/IEC 17030, Conformity assessment – General requirements for third-party marks of conformity;
- The complementary national laws related to data protection that are applicable to the Target of Evaluation;
- Where required by the national accreditation procedure, the European Regulation (EC) 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products.

Where included in the scope of certification, it can refer to complementary norms such as:

- National regulations;
- European directives and regulations;
- ISO standards, such as ISO/IEC 27001 or 27701;
- Domain-specific norms, standards, and requirements.

The Certification Body shall always consider the latest versions of these norms at the time of the assessment process.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

3.2. Rules and Principles Regarding Reference Documents

3.2.1. Applicable Versions

Except otherwise stated, all references to a document shall be understood as implicitly referring to its latest version. The release of a new version of a document should be considered as replacing all previous versions of the same document at the date of its publication, or at the end of the transition period if such a period is specified.

Certification and audit processes shall use the latest available version of the Certification Scheme and related documents at the date when the assessment process starts. When new versions of documents are released during an assessment process, it should take it into account and as far as possible comply with this new version, but it is acceptable to complete an ongoing assessment process according to the official version at the time it started.

3.2.2. Diffusion and Control

The Certification Scheme's specific normative and informative documents remain under the control of the Scheme Owner assisted by its International Board of Experts. The Scheme Owner makes relevant documents available in an electronic format to the authorised Certification Bodies and third parties.

The external reference documents are independently managed and should be accessed through their corresponding external source website.

The Certification Body and its Auditors are responsible for checking and ensuring that they are using the appropriate version of the documents.

3.2.3. Reference Language

The Certification Scheme is developed and reviewed by international experts in data protection. Its reference language is English. All Scheme documents may be translated into other languages. Documents whose translation has been validated by the Scheme Owner may serve as official versions. However, in all cases of conflict of interpretation, the English version shall be authoritative.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

4. Terms and Definitions

In this Certification Scheme and all documents pertaining to it, the following verbal forms are used:

"**shall**" and "**must**" indicate a requirement;

"**should**" indicates a recommendation;

"**may**" indicates permission;

"**can**" and "**could**" indicate a possibility or a capability.

(Adopted from ISO/IEC 17065:2012)

4.1. Specific Definitions and Contextual Use of Certain Terms

In this Certification Scheme, certain terms shall be understood as follows:

"Adaptation" refers to complementary rules and procedures of the Certification Scheme specified in a distinct document to address specific Targets of Evaluations.

"Applicant" refers to the Client of a Certification Body applying for certification or taking part in a certification process. The Applicant can be understood as encompassing the notion of "Client" in ISO standards. The Applicant shall be the Data Controller or Data Processor of the Target of Evaluation.

"Auditee" refers to the part(s) of the Applicant's organisation that will receive the Audit Team.

"**Data Protection Management System**" (DPMS) refers to the part of the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain, and improve data protection in conformity with the applicable data protection regulations. It encompasses the framework of resources set in place by an Applicant to protect the personal data it processes, including *"organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources."* (Source: ISO/IEC 27000)

"**Data protection regulations**" in plural and written in lowercase refer to both European and complementary applicable national regulations.

"**Examination**" refers to the visit or remote assessment of premises where data processing is performed or managed, or to the direct observation of an object or system, in order to verify and determine if requirements specified in Criteria are met. It may include visual observations and questions asked to stakeholders involved in the data processing.

"**Extension**" refers to a set of complementary criteria specified to assess compliance with complementary regulations, such as other national data protection regulations or other European Regulations or Directives.

"**Inspection**" when used by the present Certification Scheme refers to Examination as above defined.

"**Normative Scope**" refers to the legal and normative obligations against which an assessment and certification are performed.

"**Target of Evaluation**" refers to the data processing to be assessed and certified in a given certification process. The Target of Evaluation shall be clearly specified, and its eventual certification shall be clearly communicated and easily understandable by the data subjects.

"**Test**" and **"Testing"** refer to the performance of a data processing or a procedure in order to verify and determine if requirements specified in Criteria are effectively met. By default, tests are performed in situ, but where applicable, they can be performed remotely or in a laboratory.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

4.2. General Definitions

Except otherwise defined, the terms used in the Certification Scheme shall be understood according to the applicable definitions provided by the GDPR, the European Data Protection Board (EDPB) Guidelines and other relevant normative sources, such as ISO. In case of conflict of interpretation, EDPB definitions shall prevail over any other definitions.

The following list presents the most relevant terms and definitions related to this document.

Accreditation: *"An attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity."* (Source: EDPB Guidelines 4/2018)

Anonymous information: *"Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."* (Source: GDPR Recital 26)

Certificate: *"A statement of conformity."* (Source: EDPB Guidelines 1/2018)

Certification: *"The assessment and impartial third-party attestation that the fulfilment of certification criteria has been demonstrated."* (Source: EDPB Guidelines 4/2018)

Certification Body: ***"****A third-party conformity assessment body operating a certification mechanism.****"*** (Source: EDPB Guidelines 4/2018)

Certification Scheme: *"A certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply."* (Source: EDPB Guidelines 4/2018)

Checks and Controls: specific requirements against which the Target of Evaluation is assessed.

Consent: refers to a *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* (Source: GDPR Article 4). The consent requires that "*a data subject is freely giving his consent to data processing, after having been sufficiently and clearly informed on the way his or her data will be used."* (Source: GDPR Articles 13 and 14)

Criteria or Certification Criteria: *"The criteria against which a certification (conformity assessment) is performed."* (Source: EDPB Guidelines 4/2018) Europrivacy complements its formal Core Criteria with complementary Checks and Controls.

Cross-border Processing: "means either:

A) processing of personal data which takes place in the context of the activities of establishments in more than one country of Controller or Processor where the Controller or Processor is established in more than one country; or
B) processing of personal data which takes place in the context of the activities of a single establishment of a Controller or Processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State." (Source: GDPR Article 4)

Data Breach: *"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed."* (Source: GDPR Article 34)

Data Controller: *"The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data"* (Source: GDPR Article 4)

Data Exporter: refers to the data controller or processor transferring data to another data controller or processor located in another country that is not subject to the same data protection regulation.

Data Importer: refers to the data controller or processor receiving data from another data controller or processor located in another country that is not subject to the same data protection regulation.

Data Minimisation: *"The obligation for the Data Controller to collect only those data that are strictly necessary to perform the functionality requested by the data subject. In other words, collected data must be*

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

adequate, relevant and not excessive in relation to the purposes for which they are processed, in order to prevent unnecessary and potentially unlawful data processing." (Source: GDPR Article 5(1)(c)).

Data Portability: The right of data subjects to retrieve and transfer their personal data for other use or to other service providers. It is defined by the GDPR as *"the right for the data subject to receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and, where technically feasible, the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided. The right to portability is applicable only if the processing is carried out by automated means and based: a) on the consent of the data subject; b) or on a contract to which the data subject is party; c) or it is necessary to take steps at the request of the data subject prior to entering into a contract.*" (Source: GDPR Article 20)

Data Processor: According to Article 2 (e) of Regulation (EC) No 45/2001, a processor shall mean *"a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller."* The essential element is therefore that the Processor only acts "*on behalf of the Controller*" and under the latter's instructions. It is to be noted that according to GDPR Art. 28, *"the Processor shall not engage another Processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby allowing the Controller to object to such changes."*

Data Processing: *"Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."* (Source: GDPR Article 4(2))

Data Protection Authority (DPA): An independent public authority in charge of monitoring the application of the data protection regulation and protection of the rights of the data subjects. In the EEA, Data Protection Authorities are referred to as "Supervisory Authority".

Data Protection Officer (DPO): An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR (Source: EDPS Glossary). The Data Protection Officer is the person in charge of: informing and advising the Controller (or Processor) on data protection issues; monitoring compliance with the GDPR; awareness-raising and training of staff involved in data processing operations; and cooperating with the Data Protection Authority. (Source: GDPR Article 39).

Data Retention: Data retention refers to the fact that Controllers or Processors retain personal data for certain purposes.

Data Subject: Any *"identified or identifiable natural person to whom the data relates."* (Source: GDPR Article 4(1)).

Data Transfer: Data transfer refers to the transmission/communication of data to a recipient in whatever way.

High Risk Data Processing: Data processing activities whose nature constitute a higher risk for the rights and freedom of natural persons by processing special categories of personal data or data relating to criminal convictions, or by specifically targeting personal data of minors of age, or is likely to result in a high risk for the rights and freedom of natural persons.

Mark of Conformity (or Seal): *"A seal or mark can be used to signify the successful completion of the certification procedure. A seal or mark commonly refers to a logo or symbol whose presence (in addition to a certificate) indicates that the Target of Evaluation of certification has been independently assessed in a certification procedure and conforms to specified requirements, stated in normative documents such as regulations, standards or technical specifications."* (Source: EDPB Guidelines 1/2018)

Mechanism: *"A software element that performs control and management tasks"* (Source: ISO/IEC 12087-1)

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Personal Data: *"Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such 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."* (Source: GDPR Article 4)

Personal Data Breach: *"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."* (Source: GDPR Article 4)

Privacy: Privacy is the ability of an individual to be left alone, out of public view, and in control of information about oneself. The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12), as well as in the European Charter of Fundamental Rights (Art. 7), and the European Convention of Human Rights (Article 8). (Source: EDPS Glossary). The concept of privacy overlaps but does not coincide with the concept of personal data protection. The notion of data protection has a different scope, as it refers to any personal data, including personal data that are made publicly available. Personal data protection also refers to a whole set of data subjects" rights.

Privacy Risk: Effect of uncertainty on privacy. In the context of the GDPR, privacy risks are mainly related to the protection of personal data and its potential impact on data subject rights and freedoms.

Procedure: *"specified way to carry out an activity or a process"* (Source: ISO 30000)

Pseudonymisation: *"Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of 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."* (Source: GDPR Article 4) Pseudonymisation can serve in data minimisation, for instance, to ensure that when processing personal data, the identity of the data subjects is restricted and accessible only to those who have a legitimate need.

Purpose: refers to the purpose for which personal data are processed.

Recipient: *"A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of processing."* (Source: GDPR Article 4)

Retention Period: *"Period of time during which personal data are stored by the Controller or the Processor. According to the 'storage limitation' principle, personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*." (Source: GDPR Article 5).

Scheme Owner: *"An identifiable organisation which has set up certification criteria and requirements against which conformity is to be assessed."* (Source: EDPB Guidelines 4/2018)

Special Categories of Data: *"Special Categories of Data are personal data that are particularly sensitive and require a higher level of protection. It encompasses any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*" (Source: GDPR Article 9)

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

5. General Principles and Guidelines for Certification

5.1. Purpose of Certification

The Certification Scheme **aims to provide confidence to all parties** that a Certified Target of Evaluation is compliant with the Certification Scheme requirements and, more generally, with the GDPR and applicable complementary national data protection regulations. Consequently, the Certification Body shall aim to maintain confidence in its processes through strong principles of impartiality, competence (including data protection competencies), responsibility, openness, confidentiality, responsiveness to complaints and appeals, as well as a risk-based approach.

5.2. Core Values and Key Principles

5.2.1. Building Trust and Confidence

Auditors shall always bear in mind that Europrivacy has been designed to build trust and confidence that the Target of Evaluation is compliant with the applicable requirements.

5.2.2. Integrity

Auditors and personnel of the Certification Body involved in a certification process should perform their work with honesty, diligence, and responsibility. They should apply the Certification Scheme requirements with professionalism and impartiality.

5.2.3. Independence

Auditors should be independent of the activity being audited wherever practicable and should in all cases act in a manner that is free from bias and conflict of interest.

5.2.4. Impartiality

Certification Bodies shall ensure impartiality in their certification processes and remain fair and unbiased in all their dealings. A Certification Body's decisions shall be based on objective evidence of conformity (or Non-Conformity) and it shall ensure that its decisions are not influenced by other interests or by other parties. (More details in Section 13)

5.2.5. Evidence-based Approach

Audit findings and conclusions should be based on the evidence relevant to the audit criteria. Evidence should be recorded and verifiable.

5.2.6. Fair Presentation

Audit findings, conclusions and reports should reflect truthfully and accurately the audit activities. Their communication should be truthful, accurate, objective, timely, clear, and complete.

5.2.7. Confidentiality

The Certification Body and the Scheme Owner shall adopt procedures and implement an effective policy to protect the confidentiality of information acquired in relation to the certification process. Auditors and all personnel of the Certification Body shall protect the confidentiality of collected information.

Any documents or information shared by the Certification Body and/or the Scheme Owner with the Applicant shall be protected and handled as confidential by the Applicant, except where such document or information is explicitly intended to be made public. (More details in Section 15)

5.2.8. Openness

The Certification Body shall comply with the ISO principle of openness by providing adequate public access to clear information about its certification processes and procedures.

It shall, however, always strive to preserve and protect confidential information, such as Applicant-related information and documents shared as confidential information.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

5.2.9. Non-discrimination Conditions

The policies and procedures of the Certification Body shall be non-discriminatory. The Certification Body shall make its services accessible to all Applicants whose activities fall within the scope of its operations and for which it has the required and adequate resource.

The decision to accept or refuse an Applicant shall be based on the provisions of the Certification Scheme. The Certification Body can decline to accept an application or maintain a contract for certification from an Applicant when objective and proportionate reasons exist. Examples of reasonable grounds that a Certification Body can take into account for such a decision include:

- Applicant participating in illegal activities;
- Applicant with a history of repeated non-compliances with the Certification Scheme and/or with data protection regulations;
- Applicant heavily relying on Data Processors that cannot be controlled and/or are located in countries with too weak personal data protection regulations or policies;
- Applicant engaged in legal litigations related to data protection;
- Applicant which constitutes a risk of disrepute to the Certification Scheme;
- Applicant whose compliance would be too complex or difficult to assess and certify;
- Certification Body's lack or absence of the required resources or of availability to provide a reliable evaluation of the Target of Evaluation.

5.2.10. Addressing Emerging Technologies

Europrivacy has been designed to encompass risks related to emerging technologies, as well as to leverage state-of-the-art technologies to support certification processes.

5.2.11. Continuous Improvement

Europrivacy Certification Scheme has been designed to apply and benefit from a continuous improvement methodology.

5.2.12. Safeguarding the Core Values and Key Principles

In the event of justified suspicion of undue influence, which could jeopardise the preservation of the above-mentioned principles, the Executive Board of the Certification Body should be informed. If the issue is not resolved by the Certification Body, the Scheme Owner should be informed with the relevant evidence of undue influence.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

6. Evaluation Criteria

The evaluation criteria shall be applied in compliance with the latest version of the Europrivacy Certification Scheme requirements. They shall be applied by the Certification Body:

a) keeping in mind the Data Subjects' rights and potential risks for their personal data;
b) in a consistent and homogeneous manner;
c) in a verifiable and auditable manner);
d) taking into account:
- the size of the organisation;
- the nature of the data processing activity;
- the identified risks to data and data subjects.

6.1. Summary of Key Evaluation Criteria

The Certification Body shall comply with and apply the applicable criteria indicated in Articles 42 and 43 of the GDPR.

The detailed Europrivacy evaluation criteria, checks and controls aim at evaluating the following aspects of the Target of Evaluation:

a) **the identification of personal data processed**, including the identification of any special categories of data if applicable;
b) the compliance with the requirements for the **information on data processing provided to the data subjects**, including:
   - ease of access and understandability;
   - clear purpose for the personal data collection;
   - Data Controller's privacy policy;
   - data subjects' rights, including the rights to access, to rectify or to erase personal data, to object to data processing, to request a restriction of such processing, to withdraw consent, and to data portability;
   - information on the Data Controller and, if applicable, on the Data Processors;
c) the **lawfulness of processing** and, where applicable, in compliance with the "Prior Informed Consent" requirements, including a clear indication of the purpose for collecting data, or alternatively existence of other legal bases for processing personal data (such as a legal mandate given to a public administration);
d) the compliance with the **requirements regarding minors of age**;
e) the compliance with the **principle of personal data minimisation by design and by default**;
f) the compliance with the **principle of transparency** as specified by the GDPR, which requires that any information and communication relating to the processing of personal data to be easily accessible and easy to understand and that clear and plain language be used.
g) the **personal data flow analysis, including Data Processor and cross-border data transfer** issues, ensuring that:
   - personal data are adequately protected when transferred to a third country (e.g., on the basis of adequacy decisions, appropriate safeguards, etc.);
   - appropriate safeguards are provided by Controllers or Processors not established in the EU to receive personal data from EU based organisations;
h) the **personal data life cycle and minimisation of the personal data retention periods**;
i) the **effective implementation of the data subjects' rights**, including:
   - the right to access, to rectify, or to erase personal data;
   - the right to object to data processing or to request a restriction of such processing;
   - the right of the users to withdraw their consent;
   - the right to data portability;
j) the presence and **conformity of indirect data collection**, such as cookies and/or automated profiling;
k) the implementation of suitable measures to safeguard the data subjects' rights and freedoms and legitimate interests in the context of **automated individual decision-making**;
l) the **security and effective protection and integrity of collected data**, such as:

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

- use of backup solutions;
- use of firewalling and antivirus solutions;
- use of trustable access control mechanisms to the data (whether physically or remotely) defined around roles and responsibilities;
- use of trustable encryption protocols;
- use of trustable authentication mechanisms;
- use of a data protection by design approach;

m) the implementation by the Controller of **appropriate technical and organisational measures to protect data**, including:
- clear roles and responsibilities;
- designation of a **Data Protection Officer** (DPO) with:
    - adequate qualification;
    - required autonomy of action and access to the direction;
    - effectivity of action (demonstration of its activity and action);
    - involvement in all issues relating to the protection of personal data;
- that any natural person acting under their authority does not process data except on the Controller's instructions;
- **procedure to record all data breaches in an internal register and to inform supervisory bodies** without undue delay/within 72hrs of becoming aware of any personal data breach (unless it is unlikely to result in a risk for the data subject);
- procedure to communicate personal data breach to the data subject(s) without undue delay, where the breach is likely to result in a high risk to the rights/freedoms of natural persons;
- where applicable, such as potentially risky data processing, the performed **Data Protection Impact Assessment (DPIA)** with the DPO, and the consultation of the supervisory authorities prior to processing data if a DPIA has indicated a high risk;
- that Controllers (and where applicable their representatives) maintain **written records of processing activities**;
- for Controllers not established in the EU, the obligation to designate in writing a representative established in one of the EU Member States;

n) if **Data Processors** are being used, the procedures and agreements in place enabling the Controller to ensure their Processors provide sufficient guarantees to implement appropriate technical and organisational measures, including:
- the existence of a written contract and contractual obligations with all the Processors, covering the Data Processor's obligations;
- that the Processor shall implement appropriate technical and organisational measures to ensure appropriate security of processing;
- that the Processor shall not engage with another Processor without prior written authorisation from the Controller;
- that the Processor shall not process personal data except on instructions from the Controller;
- that the Processor (and its representatives) shall cooperate with Supervisory Authorities;
- that the Processor shall ensure that any natural person acting under their authority does not process data except under the Controller's instructions;
- that the Processor shall inform the Controller without undue delay after becoming aware of any personal data breach;
- that the Processor shall comply with conditions laid down in Chapter V of GDPR to ensure personal data is adequately protected when transferred to a third country;
- that the Processor shall be liable for the damage caused by non-compliant processing where it has not complied with obligations of the GDPR specifically directed to Processors (see above) or where it has acted outside or contrary to lawful instructions of the Controller;

o) **Where included in the agreed Normative Scope, complementary national and/or domain-specific normative requirements and criteria**.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

6.2. Europrivacy Detailed List of Criteria, Checks and Controls

The above-mentioned criteria are translated into detailed lists of criteria, checks and controls maintained by the Scheme Owner and made available to Supervisory Authorities and licensed third parties.

The list of criteria, checks and controls shall be used by the Certification Bodies for systematically assessing the compliance of the data processing in the Target of Evaluation.

Each applicable criterion, check and control shall be sufficiently completed and documented with adequate evidence to assess the conformity with the requirement.

Criteria, Checks and Controls Applicability

The Europrivacy criteria, checks and controls are individually differentiated and linked to distinct categories in order to determine and ease their applicability.

A column indicates if the criteria, checks and controls are applicable to:

- **C** Data Controllers
- **P** Data Processors
- **CP** Both Data Controllers and Processors

In order to address proportionality and to differentiate high-risk data processing from regular ones, another column differentiates the criteria, checks and controls in the following categories:

- **A** **Mandatory by default for all certification processes**.
- **B** Not required for certifying simple data processing, **but mandatory for certifying any High-Risk Data Processing, defined as data processing that:**
  - processes **special categories of personal data** or data relating to criminal convictions, or;
  - specifically **targets personal data of minors of age**, or;
  - is likely to result in a **high risk for the rights and freedom of natural persons**[6].
- **E** **Exemptions**: for determining if an exemption to a criterion can be justified.

Another column specifies if the criteria, checks and controls are:

- **S** **Specific** to each data processing (i.e., lawfulness of a data processing);
- **G** **Generic** and common to several data processing (i.e., adequate qualification of the DPO).

In addition, in the Core Criteria, another column specifies if the criterion is required to certify Data Importers based outside of the European Economic Area (EEA) that are not directly subject to the GDPR but are willing to use certification as a mechanism for international data transfer[7], where:

- **R** indicates that the criterion **is required** for Data Importers based outside of the EEA;
- **NR** indicates that the criterion **is not required** for Data Importers based outside of the EEA.

The criteria, checks and controls may be subject to **conditionality clauses** starting with the term "**IF**" and ending with the term "**THEN:**". If the condition is not satisfied, the associated requirements are not applicable and can be skipped.

Each check and control may contain and combine several requirements, which are connected to each other with the words "AND" and "OR" in order to clarify their relationship. The use of "AND" between two or more conditions requires that all conditions are satisfied; the use of "OR" requires that at least one of the conditions is satisfied.

[6] The Certification Body shall consider the related guidelines of the EDPB in that matter.
[7] Non-EEA Applicants are subject to the GDPR when directly collecting personal data in the EEA (Art. 3 GDPR).

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

6.2.1. Core Criteria and Complementary Checks and Controls

Europrivacy has been designed to deliver a homogeneous and consistent certification process applicable to diverse categories of data processing activities. Beyond the core GDPR obligations, Targets of Evaluation may be subject to complementary national or domain-specific regulations. As a consequence, the Europrivacy core criteria are complemented by contextual requirements in order to take into account the national regulations applicable to the Applicant and the specificities of the data processing.

Europrivacy Core Criteria

The list of Europrivacy core criteria constitutes the backbone of all certification processes and shall be applied by the auditors of the Certification Body to each and every Target of Evaluation.

Complementary Requirements

Europrivacy takes into account three sets of complementary requirements related to:

- **National regulations**: assessed through the National Obligations Compliance Assessment Report (NOCAR) and/or complementary national criteria Extensions;
- **Security requirements**: assessed through the Technical and Organisational Measures checks and controls (TOM) or through ISO/IEC 27001;
- **Technology- and domain-specific requirements**: assessed through the Complementary Contextual checks and controls.

The applicability of these complementary requirements is determined by objective factors, such as: the location of the Applicant for the national requirements, and the nature of the data processing in the Target of Evaluation for the technology and domain-specific requirements.

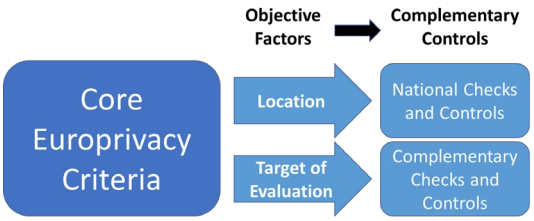

Figure 2 Complementary checks and controls determined by objective factors

Relationship between the Core and Complementary Requirements

The Europrivacy Core Criteria require to assess the compliance of the Target of Evaluation with the applicable complementary requirements.

The following figure illustrates the normative basis of the Certification Scheme and the complementarity between the Europrivacy Core Criteria and the complementary requirements.

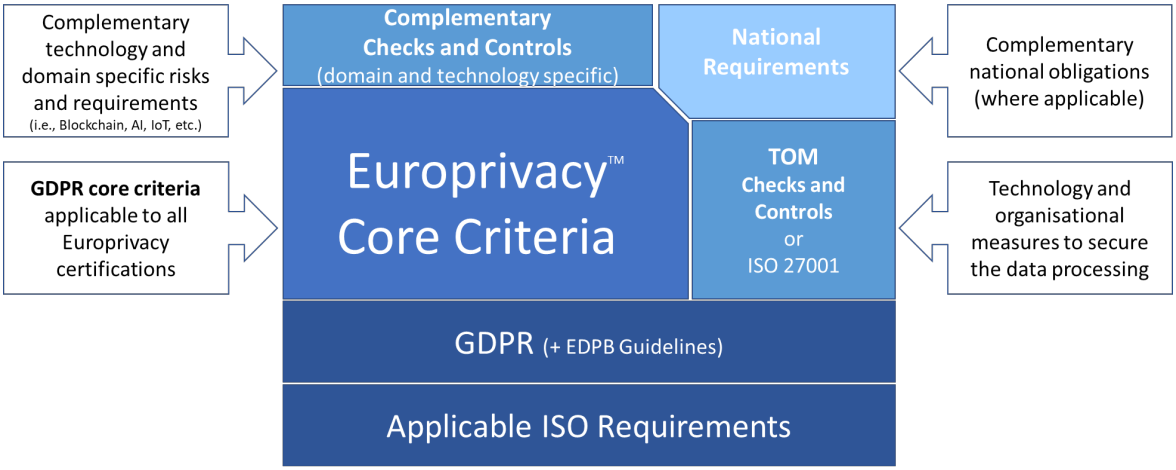

Figure 3 Europrivacy Core Criteria and Complementary Checks and Controls

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

6.2.2. Complementary National and Normative Requirements

The Applicant applying from the European Economic Area (EEA) shall request an expert with adequate legal expertise to **assess the conformity of its Target of Evaluation with the complementary national obligations of the country of application** that exceed the regular obligations under the GDPR. The results of the assessment should be reported in a written report: the ***National Obligations Compliance Assessment Report* (NOCAR)**. In the absence of a NOCAR, the Certification Body can alternatively perform a compliance assessment of the Target of Evaluation with the applicable national obligation in the country of application, subject to the same level of requirements as for the NOCAR. The Scheme Owner provides online resources, including lists of identified complementary national requirements. These lists of national requirements shall be taken into account by the expert when performing the assessment.

Europrivacy Certification can be extended to address complementary non-EU data protection regulations, as well as complementary EU regulations. In such case, complementary requirements and criteria can be specified and provided through dedicated Europrivacy Certification Scheme "Extensions" (see Section 11.1).

6.2.3. Complementary Technical and Organisational Measures Requirements

Europrivacy certification requires that adequate Technical and Organisational Measures (TOM) are in place to protect the processed and stored data.

The Complementary Technical and Organisational Measures Checks and Controls have been specified to assess the adequacy of the data processing security. These checks and controls complement the Core Criteria and are mandatory, except if the Target of Evaluation:

a) is covered by a valid ISO/IEC 27001 certification; and
b) does not perform any High-Risk Data Processing.

6.2.4. Complementary Contextual and Domain Specific Requirements

The Complementary Contextual Checks and Controls contain various subsets of checks and controls corresponding to specific technologies or application domains. The Certification Body shall apply and assess all the subsets of checks and controls that are applicable to the data processing activities included in the Target of Evaluation.

6.2.5. Development of Complementary Checks and Controls

The Scheme Owner provides complementary lists of checks and controls, as well as a mechanism to complement the predefined checks and controls with complementary ones.
Each check and control shall be:

- **Adequate** to assess compliance with the corresponding legal requirement;
- **Auditable** by ensuring that the requirement can be effectively assessed and demonstrated;
- **Objective and factual** by focusing on verifiable facts and evidence in order to minimise the subjectivity in the assessment;
- **Clearly worded** to avoid any ambiguity or room for interpretation;
- **Homogeneously applicable** by striving to make it applicable with the same relevance to diverse data processing activities and data controllers;
- **Efficient** to deliver a reliable assessment of compliance, without unnecessary workload;
- **Party Neutral** (as defined by ISO) by ensuring it can be used by the Applicant itself, by the Certification Body, as well as by a second or third party.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Process and Requirements for Specifying New Checks and Controls

In order to develop complementary checks and controls, the Certification Body shall:

1. Check first on the Scheme Owner's document repository whether adequate complementary lists of checks and controls are available to assess these requirements;
2. If these complementary normative requirements are not adequately covered by the existing checks and controls, the Certification Body can either (A) exclude the complementary requirement from the Normative Scope, or (B) it can analyse this additional norm(s) in order to identify and extract the complementary requirements;
3. In case of B, it shall complete the template made available by the Scheme Owner to list the relevant requirements and to specify corresponding checks and controls;
4. It shall send the new list of complementary checks and controls to the Scheme Owner;
5. When performing the evaluation, it shall apply the list of checks and controls to the Target of Evaluation;
6. It shall report the result of the complementary assessment in the corresponding section of the overall compliance assessment.

The template can also be used by the European or national Data Protection Authorities to communicate complementary requirements and checks and controls to the Scheme Owner.

The Scheme Owner takes care of collecting, reviewing, and sharing these additional checks and controls with other certification bodies in order to ensure consistency.

6.2.6. Lists of Criteria, Checks and Controls

The mandatory criteria, checks and controls are:

- *"A - Application and Target of Evaluation – Preliminary Checks and Controls"*, to validate the adequacy of the application and its Target of Evaluation;
- *"G - GDPR Core Criteria"*, to assess compliance with the core data protection requirements;
- *"C - Complementary Contextual Checks and Controls"*, to assess compliance with complementary domain specific and technology specific requirements;
- *"T - Technical and Organisational Measures Checks and Controls"*, to assess the measures in place to secure the processed data (can be substituted by an ISO/IEC 27001 certification if the Target of Evaluation does not include any High-Risk Data Processing);
- *"S – Complementary Surveillance Checks and Controls"*, to be used in surveillance audits and recertifications.

When a check and control is relevant and applicable to the Target of Evaluation, it shall be applied. The exclusion of checks and controls shall be justified.

Annex 1 provides a synthetic view of applicable criteria according to the location and activity of the Applicant for delivering a certification under Art. 42 and 43 GDPR.

Where applicable, the Certification Body can consider complementary checks and controls as long as it enables to better assess the compliance of the Target of Evaluation with the applicable data protection regulations.

Europrivacy is supported by complementary informative documents and checklists to facilitate and enhance the certification process, including:

- *"D - Documentation checklist for Europrivacy certification"*, to facilitate the documentation preparation and review;
- *"N - National Data Protection Obligations"* profiles listing the main complementary data protection requirements per country, to support the preparation of the National Obligations Compliance Assessment Report (NOCAR);
- Complementary checklists, such as *"P - Policy Checklist"* to check if the policies and procedures in place are complete;
- Templates (i.e., DPO Statement, NOCAR, inventories of processed data, data processors, data storage locations, etc.).

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7. Reference Process for Certifying Data Processing

Europrivacy certification is voluntary, and the role of the Certification Body is to check, via the certification process, whether the data processing to be certified meets the certification requirements.

Before applying for the certification, the Applicant should work on its data processing activities making them compliant with the applicable data protection regulations. The Applicant is encouraged to document conformity of its data processing with the data protection regulation, as well as with the Europrivacy criteria and requirements prior the process. The use of self-assessment tools and qualified consulting firms can contribute to speeding up the certification process. ECCP makes available a number of resources to Applicants, law firms and consulting firms to prepare Europrivacy certifications.

The reference process for certifying data processing is based on the ISO/IEC 17065 model and requirements. The evaluation process is focused on the Target of Evaluation.

A certification can be granted for a maximum period of 3 years. Recertification can be granted, subject to the outcome of monitoring activities.

The reference process for certifying data processing involves the following steps:

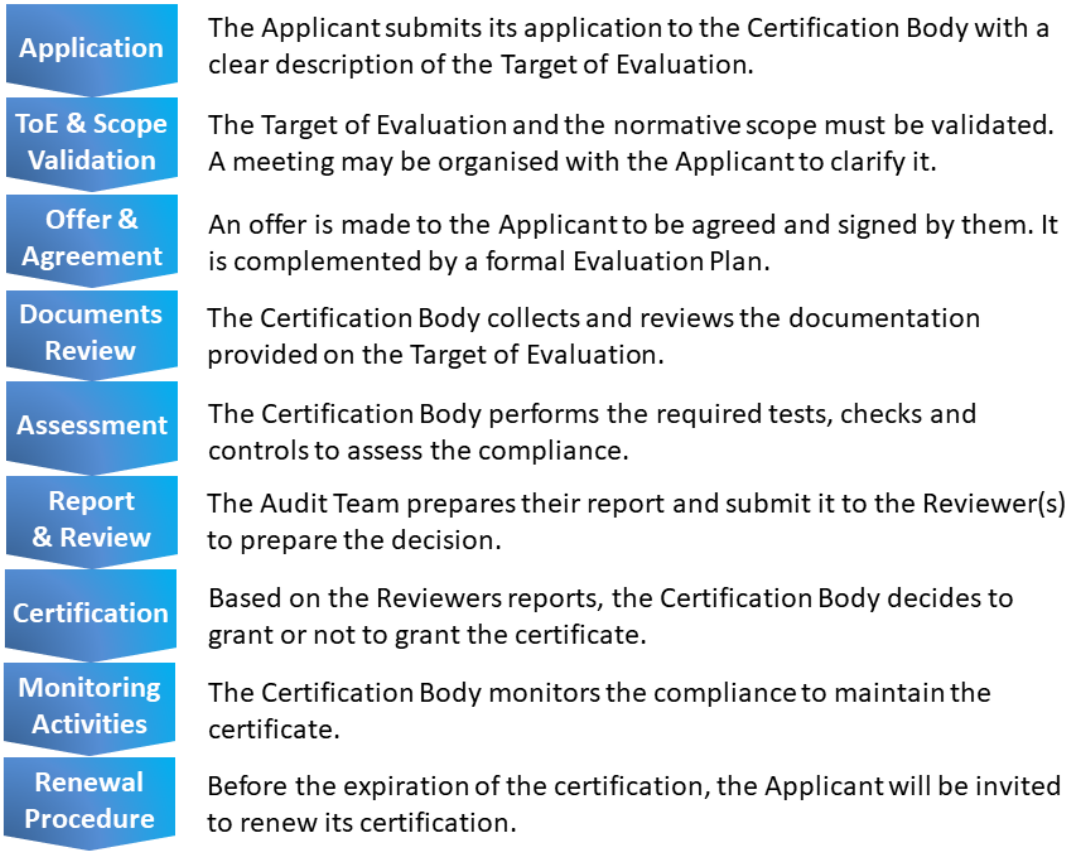

Figure 4 Reference certification process

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.1. Adaptable Process Model

7.1.1. Adaptable Process Model Overview

While the prime focus of the Europrivacy Certification Scheme is to assess personal data processing, it has been designed to be as comprehensive as possible. It is adaptable to different scopes, such as data protection management systems, that are subject to additional requirements and accreditation procedures specified in dedicated Adaptations (see section 11).

While the Certification Scheme can be applied to a large variety of data processing activities, its application for certifications under Articles 42 and 43 of the GDPR shall strictly comply with the related policy, directives and restrictions set by the European Data Protection Board.

7.1.2. Combined Applications

The Europrivacy Certification Scheme can be extended to encompass complementary obligations in data protection specified in Extensions (see Section 11). In such cases, the certification process should be considered as a single Certification process rather than a dual or combined certification.

7.1.3. Applicants and Applicability

The certification process is open to public and private entities acting as Data Controller or Data Processor. Under Articles 42 and 43 of the GDPR, the certification is only applicable to processing operations of personal data by Controllers and Processors and may be subject to restrictions set by the European Data Protection Board.

7.2. Pre-certification Activities

7.2.1. Application Process

The application process shall gather the required information to determine the Target of Evaluation of the certification and shall be properly documented.

The Applicant shall be the Data Controller or Data Processor of the data processing that is in the intended Target of Evaluation of the certification.

In principle, the Applicant should complete and submit an application form signed by its authorised representative(s). Alternatively, the application can be performed by the means of a face-to-face meeting between an authorised representative of the Applicant and the Certification Body.

The application process shall collect and document information on:

a) the Applicant, including its legal denomination, address(es), website and domain of activity;
b) the description of the data processing activities;
c) the desired Normative Scope and Target of Evaluation of the certification;
d) where applicable, information on complementary national or domain specific regulations applicable to the Target of Evaluation with regards to data protection;
e) the authorised contact person(s);
f) whether consultancy has been provided for the Target of Evaluation, and if so by whom.

Additionally, as requested by the EDPB guidelines, the Target of Evaluation must be described in detail in the Application phase with:

- **Interfaces and transfers to other systems and organisations;**
- **Protocols used and other relevant assurances;**
- **Identification of any involved Data Processors with their tasks and responsibilities.**

Once the Certification Body and the Applicants are covered by appropriate confidentiality contractual clauses, the Application shall be completed with copies of the relevant contractual clauses between the Applicant and its Data Processors.

Beyond the information provided by the Applicant, the Certification Body may collect complementary information to be added to the Application with documented indications of the source.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.2.2. Preliminary Commitment of the Applicant

By signing the Application form, the Applicant shall agree to comply with the Europrivacy General Terms and Conditions attached to the Certification Scheme. It shall also commit to respect and facilitate the certification process by providing the required information, support, and necessary access to the Auditors.

7.2.3. Clarifying and Specifying the Target of Evaluation

The Target of Evaluation shall be specified and checked with care. The Applicant and the Certification Body shall:

a) **specify the Target of Evaluation** by:
   a. **naming it with a clear title**;
   b. **describing the data processing**;
   c. **illustrating the personal data flows in a diagram or a drawing**, including the identification of personal data flows with external data processing;
   d. **identifying the categories of data** processed within the Target of Evaluation;
   e. **identifying and describing all data processing operations and systems** pertaining to the Target of Evaluation;
   f. **indicating where the data processing starts and ends**;
   g. **where applicable, identifying and describing the interfaces of the data processing in the Target of Evaluation with independent processing operation;**
   h. **specifying the protocols used** and other relevant assurance measures;
b) **justify any exclusion of interdependent data processing** from the Target of Evaluation;
c) **list all the Data Processors** involved in the Target of Evaluation, with a description of their tasks, responsibilities, and relevant contractual clauses;
d) **where applicable, identify**:
   a. **any joint-controller**;
   b. **the recipients** of data or categories of recipients;
   c. **data transfer** to third countries or to international organizations;
e) **determine if any complementary requirements, such as national and domain-specific norms, shall be addressed by the certification**.

The role of the Applicant as Data Controller or Data Processor of the Target of Evaluation shall be clarified. Where the Applicants act as Joint Controller, the implication on the Target of Evaluation and the certification shall be carefully analysed.

The final specification of the Target of Evaluation and Normative Scope shall remain under the control of the Certification Body and shall be aligned with the ability of the Certification Body to effectively assess the compliance of the elements included in the scope. The Certification Body may decide to adapt the Target of Evaluation and Normative Scope during the course of the certification process.

The Certification Body shall ensure that it can adequately assess the Target of Evaluation.

The Certification Body shall ensure that the Target of Evaluation is adequately specified to convey clear information to the data subjects. It shall prevent any misleading certification or excessive broadness of the Target of Evaluation. It shall refuse any Target of Evaluation that is ambiguous, misleading, or risks to be misinterpreted by data subjects or by other third parties.

7.2.4. Clarifying the Normative Scope

When specifying the Target of Evaluation, the Applicant and the Certification Body shall evaluate and determine if complementary national or domain specific data protection regulations shall be included in the Normative Scope of the intended Certification.

It shall take into account the potential risk of misinterpretation by the data subject, as well as the context, such as industry and application domain-specific expectations regarding data protection.

The Normative Scope of the Certification should be clearly specified.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.2.5. Application Review and Validation

The Certification Body shall review the information received through the Application Process to ensure that:

a) the Application form is complete;
b) the information about the Applicant and the Target of Evaluation is sufficient to make a decision and to assess the required effort for the certification process;
c) the Target of Evaluation is well-defined and any other points influencing the certification activity are taken into account (time required to complete audit, language, safety conditions, threats to impartiality, etc.);
d) there is a mutual understanding and agreement between the Certification Body and the applicant organisation regarding the Target of Evaluation;
e) the Normative Scope to be used is adequate to avoid any misleading certification;
f) the means are available to perform all evaluation and auditing activities and in particular that the **Certification Body has access to the adequate technical and legal expertise for the requested certification;**
g) **the Europrivacy Checks and Controls are adequate to assess the Target of Evaluation.**

Certification under GDPR Article 43 requires that the application and the specification of the Target of Evaluation comply with a set of specific requirements. In order to validate the conformity with these requirements, **the Certification Body shall apply the dedicated list of Europrivacy checks and controls to validate the Application and Target of Evaluation**[8].

7.2.6. Quick Check and Clarification with the Applicant

Where relevant, the Certification Body should propose a meeting or teleconference to clarify the intended Target of Evaluation. The meeting can also serve to better understand the context and specificities of the data processing involved, to determine the feasibility of the certification, to better assess the certification effort, as well as to discuss and agree on the intended certification process.

7.2.7. Determining the Criteria and Evaluation Methodology

As requested by the EDPB, the Certification Body shall identify evaluation methods to assess the Target of Evaluation and shall refer to them in the certification agreement with the Applicant.

The Certification Bodies shall have consistent evaluation methods for comparable Targets of Evaluation, such as:

- a method for assessing the necessity and proportionality of data processing with regards to the purpose and the data subject's consent.
- a method for assessing the comprehensiveness of risk assessment by the Data Controller and its Data Processors.
- a method for assessing the remedies, safeguards, and procedures to ensure the protection of personal data processing in the Target of Evaluation.

The Certification Body shall ensure that there is appropriate and accessible documentation of its Methods and Findings.

The Certification Body shall determine the Europrivacy criteria and evaluation methodology applicable to the Target of Evaluation.

The certification Agreement shall refer to the Europrivacy certification criteria, which are mandatory. It shall clarify if any additional normative requirements, such as national and domain specific regulations, will be used for assessing the conformity of the Target of Evaluation.

7.2.8. Assessing the Risks and Personnel Requirements

Once the Normative Scope has been clarified, the Certification Body shall identify the main risks in terms of data protection, as well as the effort of work required to assess, audit, and certify the Target of Evaluation. It should assess if it has the required personnel and resources to perform the certification process.

[8] "A – Application and Target of Evaluation – Preliminary Checks and Controls"

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.2.9. Application Decision

After reviewing the Application, the Certification Body shall take a decision to accept or decline it. It shall assess if it can deliver a reliable certification of the Target of Evaluation.

If the decision is negative, it shall inform the Applicant with explanations regarding its decision and may recommend other qualified Certification Bodies.

If the decision is positive, it shall determine the competencies that are required to perform the certification process according to the Review and shall prepare an Offer.

7.3. Offer

7.3.1. Estimating the Required Assessment Time and Effort

The Certification Body shall estimate the anticipated audit time required to ensure that all the areas of interest of the data processing activities are adequately assessed with the needed intensity. It shall take into account the following factors:

a) the number of criteria applicable to the Target of Evaluation;
b) the potential inclusion of complementary criteria Extensions to assess compliance with complementary norms and regulations;
c) the geographic scope of the Target of Evaluation and the number of sites to be inspected.

The Scheme Owner provides resources and tools to help estimate the required effort and time.

7.3.2. Preparing the Offer

Upon reaching a decision to accept the Application, the Certification Body shall prepare a written Offer that contains at least:

a) the proposed Normative Scope, objectives and criteria for the certification;
b) information on the whole certification process, including:
    - methodology used to certify and maintain certification;
    - a link to the Certification Scheme's official website;
c) the terms and conditions, including:
    - the Applicant's obligations mentioned in the Certification Scheme;
    - the clarification of the roles and responsibilities of the various parties;
d) a cost estimate (or at least a cost model and a cost per hour indication) of the services;
e) a confidentiality clause applying by default to all documents exchanged with the Applicant, including the Offer itself.
f) In order to simplify the administrative process, the Certification Body can also decide to submit an initial Certification Programme proposal as part of the Offer to the Applicant.

7.3.3. Offer Submission

The submitted Offer shall be limited in time with a clear deadline.

If the Applicant agrees with the conditions, it shall sign the Offer and/or the related certification agreements, and shall proceed with the payments within the indicated timeframe.

If the Applicant does not sign the agreement or does not pay the opening invoice within the deadline, the Offer can be considered refused. The Certification Body shall be free to take other commitments and shall have no more obligations to follow on the submitted Offer, except if required by law. It shall also have no obligation to accept a new application.

7.3.4. Offer Acceptance

The formal acceptance of the Offer by the Applicant shall be formalised by the authorised signatures of the designated signatories of the Applicant, and their formal acceptance of the proposed terms and conditions.

If the Offer requires an initial payment before the commencement of the certification process, the agreement shall be considered as complete only after the Applicant has paid the necessary payment.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.3.5. Invoices and Payments

Audit findings can impact the certification process, the number of required work hours and the final cost of the certification. Certification Bodies should inform Applicants about any anticipated deviation from the initial Offer.

The Applicant shall commit to paying in due time all invoices sent by the Certification Body for the certification process. The Certification Body can suspend or cancel the certification process in case of non-payment or excessive delay in payment by the Applicant.

7.4. Audit Team Composition and Associated Functions

In parallel to the submission of the Offer, or at the latest at the point that the Applicant accepts the Offer, the Certification Body shall make the necessary arrangements for the assessment process. It should assign at least a Lead Auditor and a Project Manager (who can be the same person as the Lead Auditor) and identify complementary members of the Audit Team where required, including complementary Auditor(s) and Technical Expert(s) as appropriate.

The Reviewer(s) are not part of the Audit Team and can be identified at a later stage.

As specified in the EDPB Guidelines for certification, evaluation can be *"carried out by external experts who have been recognised by the Certification Body."*

7.4.1. Required Qualifications

The Audit Team shall gather the required expertise and skills to perform the audit and apply the Certification Scheme to the selected Target of Evaluation. Each team should more specifically include:

- Expertise in data protection regulation;
- Adequate knowledge and understanding of Europrivacy Certification Scheme requirements;
- Adequate technical expertise for analysing the adequacy of the Technical and Organisational Measures in place to protect the processed data.

Auditors shall have successfully completed the Europrivacy Assessment Course and passed the corresponding exam on the Europrivacy Online Academy website (https://academy.europrivacy.com).

The Audit Team selection shall respect the specific requirements related to qualification specified in the Section on Management of Personnel and Resources (see Section 14) and the document "Management of Competencies of Personnel Involved in Europrivacy Certification Process".

7.4.2. Overall Certification Team Composition

A certification team may be comprised of several roles and functions, including:

As part of the formal Audit Team:

- Lead Auditor;
- Additional Auditors (optional);
- Technical and/or Legal Experts (optional, if the Auditors have adequate expertise for the assessment of the Target of Evaluation).

Additional functions complementing the Audit Team:

- Project Manager;
- Reviewer.

The functions of Project Manager and Lead Auditor can be combined and carried out by a single person, or allocated to two distinct persons.

The presence of Co-Auditors is optional.

Additional functions may be included, such as Guides provided by the Applicant, and Observers.

The Certification Body shall ensure that Lead Auditors and Reviewers have an adequate level of expertise in data protection to assess and validate the certification process conclusions.

The following figure summarises the key functions on the Certification Body side for the audit process:

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

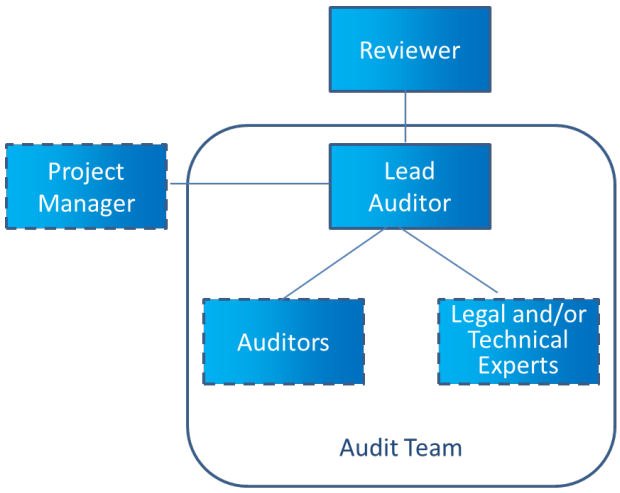

Figure 5 Regular Audit Team structure

7.4.3. Project Manager

The Project Manager shall serve as the Applicant's main contact and is responsible for monitoring the activities related to the Applicant's certification process. The Project Manager shall ensure that:

- all required contractual documents are signed and collected;
- all required information for the certification process is collected from the Applicant;
- the audit plan and related meetings are properly organised;
- the audit report is completed, reviewed and shared with the Applicant;
- all relevant information, documentation and reports are archived in the Data Protection Management System of the Certification Body;
- all invoices and payments are properly completed;
- where appropriate, the certificate is delivered and published in the online Registry.

The Certification Body may decide to transfer some or all of these duties to the Lead Auditor.

7.4.4. Lead Auditor

After acceptance of the Offer, the Certification Body shall designate a Lead Auditor whose prime responsibility will be to coordinate and perform the audit, as well as to produce the audit report to be submitted to the Reviewers.

The Lead Auditor shall have a comprehensive knowledge of the Certification Scheme specifications and requirements by successfully completing their qualification as auditor on the Europrivacy online academy: https://academy.europrivacy.com

7.4.5. Auditors

Additional Auditors may join the Audit Team under the authority of the Lead Auditor. They shall have appropriate knowledge of the Certification Scheme and comply with the requirements specified by the Certification Scheme by successfully completing their qualification as auditor on the Europrivacy online academy: https://academy.europrivacy.com.

7.4.6. Technical and Legal Experts

Technical and Legal Experts may complement an Audit Team by providing additional expertise. When performing an audit, they shall act under the authority of the Lead Auditor and shall focus on their specific mission.

The Certification Body shall inform the Applicant in advance about the involvement of the Technical Experts in certification activities.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.4.7. Evaluators

Members of the Audit Team can serve as Evaluators to coach and assess the Lead Auditor and/or Audit Team members. Evaluators can be designated by the Scheme Owner and/or by the Certification Body and/or the competent national authority. The evaluators shall work and behave as regular Auditors or Technical Experts in the certification process for the Applicant. They will report on their observations, clarifications and recommendations for improvement to the Audit team and where applicable to the Certification Body and/or the Scheme Owner.

7.4.8. Observers

Observers may be invited to join the Audit Team. Observers may include members of the Applicant's organisation, consultants, accreditation body personnel, data protection authority personnel, representatives of the Scheme Owner, regulators, or other persons whose participation is justified.

Observers shall be bound by confidentiality obligations before attending the audit.

When a Certification Body plans to invite Observers to an audit, it shall inform the Applicant in advance, in order for the Applicant to have the possibility to object to such presence.

The Observer shall not have any direct involvement in the audit and certification process. If Observers identify non-compliance with the Certification Scheme by the Audit Team, they shall communicate their observations to the Lead Auditor and or to the Audit Team in the context of a strictly bilateral debriefing.

7.4.9. Guides

When performing on-site audits, the Auditor(s) shall be accompanied by a Guide, unless otherwise agreed to by the Lead Auditor and the Auditee.

The duty of the Guide is to facilitate the work of the Auditor(s) by easing their access to premises, employees, documents, information and any other relevant resource deemed relevant by the Auditors for the certification process. The Guide may be in charge of:

a) organising and planning the visits and interviews;
b) ensuring the safety and security of the Audit Team members;
c) witnessing the audit on behalf of the Applicant;
d) providing clarification or information as requested by an Auditor.

The Auditee shall ensure that the Guide has adequate authority and competencies to perform its duty.

The Audit Team shall ensure that Guides do not influence or interfere in the audit process or outcome of the audit.

7.4.10. Translators and Interpreters

Translators and interpreters may be required and may have an impact on the duration of the audit. Certification Body shall select translators and interpreters who are both impartial and not in a position to unduly influence the audit.

7.4.11. Reviewers

The main function of the Reviewer(s) is to review the Auditor's report and findings and to make a decision on the certification. The Reviewer function shall be carried out by a person or group of persons (e.g., a committee) who have not been involved in the process for evaluation. Reviewers can serve as Lead Auditors or Auditors in other certification processes, but not in the certification process under their review.

The Reviewer(s) shall be employed by, or shall be under contract with, the Certification Body or an entity under the organisational control of the Certification Body. Any Reviewer not directly employed by the Certification Body shall meet the same eligibility requirements placed on employees of the Certification Body.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

7.5. Use of Prior Certification of Parts of the Target of Evaluation

According to EDPB, prior certifications of parts of the Target of Evaluation can be considered in the certification process, but their recognition shall require at least:
- **the availability of the complete certification report, or**
- **adequate information for assessing the previous certification activities and its results.**

ISO/IEC 17065 requires that the Certification Body uses only *"evaluation results related to certification completed prior to the application for certification."*[9] **It is allowed to reuse documented evidences**.

7.6. Assessment Plan

The Certification Body shall determine an Assessment Plan that is adequate to address the specificities of the Target of Evaluation. It shall take into account potential additional requirements, such as domain specific and/or national obligations included in the Normative Scope of the requested certification.

The Assessment Plan shall specify:

a) The Target of Evaluation;
b) The composition and roles in the Certification Team;
c) A tentative overall planning of assessment activities.

7.7. Duty to Inform the Data Protection Authority

Before starting the Certification process, a Certification Body operating in another Member State of the European Economic Area shall inform the competent Data Protection Authority.

[9] See Clause 7.4.5 ISO/IEC 17065

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

8. Assessment of Conformity and Reporting

8.1. Assessment Activities

The Target of Evaluation shall be evaluated against the requirements and criteria specified in the Certification Scheme, within the limits of the agreed Target of Evaluation and Normative Scope. Each Criterion applicable to the Target of Evaluation shall be assessed.

The assessment of conformity can include activities such as documentation and files review, sampling, testing, Examination, interviews, and audits, as appropriate. The assessment of the criteria shall be performed in accordance with the "Europrivacy Guidelines on the Use of Criteria, Checks and Controls".

The Certification Body shall carry out the assessment activities using its internal resources and shall manage outsourced resources in accordance with the Assessment Plan. The assessment shall be performed by an Audit Team gathering adequate legal and technical expertise.

8.2. Documentation Review

8.2.1. Documentation Access

The Certification Body shall receive access to the documentation, files, and records required to assess the compliance of the Target of Evaluation. Where applicable, documentation and evidence can be collected through electronic means and made available in a secured online repository.

It is acceptable that for security reasons, some documents may be only accessible on-site by the Applicant (i.e., firewall configuration). However, **documentation and evidence can be kept and stored by the Certification Body on a need basis**.

ECCP provides a reference list of documentation to be accessed by the Certification Body for the certification process. It can be used by the Applicant to gather and facilitate access to the required documentation.

8.2.2. Preliminary Documentation Review

Before starting the formal assessment, the Project Manager or the Lead Auditor shall ensure that **all the required documentation exists and will be accessible to the Audit Team**. A reference list of required documentation is made available by the Scheme Owner and can be adapted by the Certification Body.

The initial documentation review does not aim at assessing the compliance of the Target of Evaluation, but should verify that:

- the **DPO has an adequate expertise**, which must be validated before validating the documents provided by the DPO;
- the **documents are clearly identifiable** with dates and/or version number;
- the **documentation is complete and sufficient for the assessment process**.

Where documentation appears insufficient, the Applicant shall be informed and the planning of the assessment process should be discussed and reconfirmed by the Certification Body and the Applicant.

8.3. Testing Procedure

The Certification Body can perform Tests in order to assess the compliance of processing with Certification Scheme requirements. The reference to Tests or Testing in the suggested means of verification does not refer to, nor does it require, the use of testing laboratories.

Demonstrating compliance with ISO/IEC 17025 is not required by the Certification Body, but where Tests are outsourced to an external testing laboratory, the latter shall respect the ISO/IEC 17025 requirements.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

8.3.1. Use of Samples

The Certification Body can use representative samples in order to assess the compliance with requirements.

In order to ensure that sampling approaches remain meaningful and reliable in the certification process, the Auditor should:

a) establish the objectives of the sampling plan;
b) select the size and composition of the population to be sampled;
c) select a sampling method;
d) determine the size of the sample;
e) conduct the sampling activity;
f) compile, evaluate, report and document the results.

Auditors can use both judgement-based sampling and statistical sampling.

When applying a judgement-based sampling approach, the sample size shall include at least one item per digit of the total number of items under consideration, with a minimum sample size of three items.

When applying a statistical sampling approach, the Auditor can adapt the acceptable confidence level percentage to the associated level of risk and impact in case of noncompliance. By default, the Auditor should use at least a 95% confidence level with a maximum 5% of margin of error.[10]

8.3.2. Technical Tests

Whenever relevant, a set of technical Tests shall be performed to identify any vulnerability related to data protection and/or to perform checks and controls required by the Certification Scheme (e.g., Vulnerability Assessments, Penetration Tests). The process shall be handled by Technical Experts or laboratories with the required expertise. The Technical Experts and laboratory shall act under the supervision of the Lead Auditor who may require specific Tests and findings.

8.4. Examinations and On-site Assessments

8.4.1. Examination Principles

Examination refers to the visit or remote assessment of premises where data processing is performed or managed, or to the direct observation of an object, in order to verify and determine if requirements specified in Criteria are met. It may include, but is not limited to: visual observations, requests for demonstrations, and questions asked to stakeholders involved in the data processing.

8.4.2. On-site Assessment and Audits – General Principles

According to the Target of Evaluation, on-site assessments (also referred to as “Audits”) may be required. On-site assessments can utilise technologies for remote Examination.

The Certification Body shall organise on-site assessments whenever there is a clear need to do so or where the Lead Auditor estimates that such action is required to deliver a reliable opinion on the Target of Evaluation’s compliance.

A decision to perform on-site assessments should be communicated to the Applicant early in the process, in principle with the Assessment Plan, after the application has been processed and all necessary documents have been revised. However, decisions to perform on-site assessments may be taken at a later stage, for instance after initial tests and assessment results have been delivered to the Lead Auditor.

The audit criteria are those specified in the Certification Scheme, including the list of detailed checks and controls against which conformity is determined.

[10] Online calculators can be used (e.g., Sample Size Calculator - Qualtrics).

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

8.4.3. Audit evidence shall be made up of records, statement of facts, and other information related to the criteria, and shall be verifiable.Preparation for On-site Assessment

The Project Manager shall assign a qualified Lead Auditor or an Audit Team to perform the on-site assessment or audit. The Certification Body shall ensure that the Audit Team's qualification is adequate for the type of activity performed by the Applicant.

The Lead Auditor shall send the Audit Plan to the Applicant's representative at least two weeks prior to the assessment or audit for confirmation and acceptance. The Audit Plan shall mention a preliminary list of requirements, resources, and documents to be prepared by the Applicant for the on-site audit.

8.4.4. On-site Assessment Process

The steps of the on-site assessment or audit should include the following:

a) an opening meeting, during which the Lead Auditor presents:
   - the assessment/audit plan, including the objectives, the scope, and main points to be checked;
   - a summary of the evidence and findings from previous steps;
b) the documentation analysis and evaluation;
c) the identification of relevant sources of information;
d) the collection of information by appropriate sampling, tests, Examinations, and verifications, including as applicable on-site visits and interview with employees;
e) establishing the assessment/audit evidence from the previous steps;
f) the evaluation of the collected information and evidence against the Certification Scheme requirements;
g) the formulation of the assessment/audit findings;
h) the reviews of assessment/audit findings and evidence to formulate the assessment or audit conclusions;
i) a closing meeting, where the Lead Auditor presents the assessment or audit conclusions.

8.4.5. On-site Assessment Summary Report

The Certification Body shall prepare a formal assessment or audit summary report in order to present the findings and conclusions of the assessment or audit, as well as to provide information on any identified Non-Conformities.

8.4.6. Multi-site Assessment

The Target of Evaluation can cover personal data processing distributed across several sites under the effective control of the Applicant. The Certification Body shall determine if multi-site assessments are required to demonstrate compliance with the criteria.

Where a multi-site assessment is required, the Certification Body can apply site sampling among sites performing similar data processing activities. Site sampling is only applicable where the Applicant has effective control and monitoring on the relevant sites.

The sites shall be selected by taking into account:

a) the level of risk for the processed data;
b) the diversity of the sites;

and where applicable:

c) results of previous audits;
d) reported complaints.

Moreover, where applicable, at least 25% of the sites shall be selected at random.

The minimum number of sites to be assessed shall be proportionate to the square root of the number of sites, with the following ratio:

- Initial audit: simple square root, rounded up to the next lower whole number.
- Surveillance audit: 60% of the square root result rounded up to the next lower whole number.
- Re-certification: 80% of the square root result rounded up to the next lower whole number.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

When performing multi-site assessment, the onsite audit time reduction per sampled site can be reduced to 50% of regular audit time.

8.5. Use of Audit Results from Other Certification Bodies

Where the Certification Body is taking account of certification already granted to the Applicant by another Certification Body, it shall obtain and retain sufficient evidence, such as reports and documentation on corrective actions regarding any Non-Conformity. The Certification Body shall justify and record any adjustments to the existing audit programme and follow up on the implementation of corrective actions concerning previous Non-Conformities.

8.6. Assessing Compliance

8.6.1. Suggested Means of Evaluation

Criteria mention suggested means of evaluation. **According to the Target of Evaluation different means of evaluation may be applicable, and more than one means of evaluation may be required**. For instance, assessing the procedure for the right of the Data Subject to request access to Personal Data can be done by checking how such requests have been handled by the Applicant. However, if the Applicant has not received any request yet, a documentation review of the rules, policies and procedures of the Applicant and/or testing the effectivity of the procedure would be valid alternatives.

The Auditor shall use the most efficient means of evaluation and collect sufficient evidences to determine with a high level of confidence the conformity or non-conformity of each applicable Criterion.

In accordance with ISO/IEC 17007, *"it should be left to the users of the normative document to decide what conformity assessment activity (if any) will be utilized, who will carry out the conformity assessment and under what conditions."* **For each Criterion, the Auditor shall use one or more means of evaluation, until sufficient evidence is collected to determine if the requirements are met**.

By default, the following order of priority is recommended:

a. documentation review, including files and records review;
b. interviews;
c. Examinations;
d. Tests;
e. other means of verification, to the condition they are efficient and reliable.

The order of priority can be adapted where a means of evaluation is not applicable or where a different order can increase the efficiency and reliability of the assessment. The use of other means of verification shall be recorded and justified.

Interviews shall be performed as part of the Target of Evaluation assessment.

More details on the evaluation of the criteria are provided in the Europrivacy Guidelines on the Use of Criteria, Checks and Controls, as well as in the FAQ section of the Europrivacy Resources and Community website: https://community.europrivacy.com

8.6.2. Recording Evidence

In order to assess the status of a Criteria, Checks and Controls, the Auditors shall collect and record clear evidence that demonstrates the compliance or non-compliance with the requirement.

The Certification Body shall be able to demonstrate that its findings are based on clear evidence.

8.6.3. Finding and Status of Criteria, Checks and Controls

Most checks and controls are assessed and determined according to one of the following status categories:

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Status Code	Meaning / Explanation
?	Missing Information / Don't know
OK	Conformity: Requirement has been **controlled** and appears to be respected and no non-conformities have been identified.
OK+	Good practice moving beyond simple conformity
Obs	Observation
Min NC	A **Minor Non-Conformity** (non-critical) has been identified.
Maj NC	A **Major Non-Conformity** (critical) has been identified.
NA	Control is **Not Applicable** for the targeted certification

Figure 6 Categories of Status for the Findings

When controls are qualified as non-applicable, the reason should be justified and documented.

8.6.4. Qualification of Non-Conformities

Where the assessment of a Criteria (or Check and Control) results in identifying a "non-fulfilment of a requirement" it constitutes a Non-Conformity.

All Non-Conformities shall be listed with a distinct identification number and shall be clearly described with the reference to the specific norm and requirements that are not respected. Each one shall be qualified either as "Minor" or "Major" Non-Conformity.[11]

"Major" Non-Conformities

A Major Non-Conformity is a Non-Conformity which breaches the compliance of the data processing activities in the Target of Evaluation with the fundamental data protection requirements, the data subject rights, or the Europrivacy Certification Scheme requirements as stated in this document.

Any Non-Conformity where the Applicant breaches its legal obligations, as specified in the GDPR, constitutes a Major Non-Conformity.

"Minor" Non-Conformities

A Minor Non-Conformity is a non-critical Non-Conformity which does not qualify as a Major Non-Conformity.

Observations

The assessment process may result in identifying situations that do not constitute formal Non-conformities with the assessed requirements, but that may be considered as borderline or suboptimal. In such case, the Assessor shall qualify the status as "Observation" and write down the findings and concern.

8.6.5. Impact of Non-Conformities

It is prohibited to deliver a certification in any of the following cases:

- **in the presence of any not closed Major Non-Conformity;**
- **in the presence of more than five Minor Non-Conformities pending verification;**
- **if the certification would be misleading for third parties and data subjects.**

In case of remaining Minor Non-Conformities, the Applicant shall present a remediation plan and commit to address the identified Minor Non-Conformities before the subsequent Surveillance Audit.

Where Minor Non-Conformities have been identified and a corrective action plan has been accepted by the Certification Body, it is authorised to postpone the reassessment of up to 5 Minor Non-Conformities for which evidence on conformity shall be only required by the next Surveillance Audit.

For any Major Non-Conformities, the Certification Body shall have **reviewed, accepted, and verified the correction** and corrective actions in order to consider it as resolved and closed.

[11] The differentiation is required to comply with ISO/IEC 17021-1.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

For any Minor Non-Conformities, the Certification Body shall have either **reviewed, accepted, and verified the correction** in order to consider it as resolved and closed, or it shall have **accepted the Applicant's plan for corrective actions** to be assessed and validated at the next audit.

Minor Non-Conformities identified in a previous assessment that have not been addressed by the Applicant can be requalified by the Certification Body as "Major Non-Conformities."

If Non-Conformities have arisen during the evaluation process that prevent the certification, and if the Applicant expresses interest in continuing the certification process, the Certification Body shall:

a) provide information regarding the additional evaluation tasks needed to verify that Non-Conformities to be remediated have been corrected;
b) agree with the Applicant on the required delay (which should not exceed 6 months) in order to correct the identified Non-Conformities.

If the Applicant agrees to completion of the additional evaluation tasks and, **where appropriate, for ensuring the reliability of the compliance assessment, the process of evaluation shall be repeated to complete the additional evaluation tasks**, in conformity with ISO/IEC 17065 requirements. Documented evidence can be reused.

8.6.6. Correction Action Plan

If the Applicant expresses interest in continuing the certification process, a Correction Action Plan shall be elaborated as follows:

The Certification Body shall communicate to the Applicant the list of identified Non-Conformities and how these relate to the requirements of certification.

The Applicant shall prepare and propose a Correction Action Plan with corrective actions for each identified Non-Conformity, which provides the reasoning for the Non-Conformity (e.g., a root course analysis). The Correction Action Plan shall list potential Non-Conformities and classify them according to their degrees of severity ("Major" or "Minor" Non-Conformity). Appropriate actions to be taken and application modalities shall be detailed. Corrective actions proposed by the Applicant shall be appropriate and comprehensive for the certification process to continue, if they are not the Certification Body shall ask the Applicant to propose new corrective actions.

The Correction Action Plan shall be completed by the Applicant within an agreed period of time that should not exceed 6 months.

8.6.7. Consequence of Persisting Non-Conformities

The consequence of persisting Non-Conformities on the certification is defined according to the nature and the severity of the Non-Conformity as well as its occurrence and the risk of fraud.

Appropriate measures regarding the correction plan can be:

a) Continuation of certification under conditions;
b) Reduction of the scope of certification;
c) Suspension or withdrawal of the certification.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

8.7. Assessment Report

After the conclusion of the assessment activities, the Lead Auditor is responsible for generating an Assessment Report for the Applicant.

The Assessment Report **may identify areas for improvement but shall not recommend any specific solutions** to avoid delivering consulting.

The Report should *"describe how the requirements are met and if not initially met, describe the corrections and corrective actions and their appropriateness, thus providing the reasons for granting and maintaining the certification.* *This includes the outline of the individual decision for granting, renewing or withdrawing of a certificate. It should* ***provide the reasons, arguments and proofs resulting from the application of criteria*** *and the conclusions, judgments or inferences from facts or premises collected during certification." (EDPB)*

The Report shall contain an accurate, concise, and clear record of the assessment in order to inform the Applicant and to enable an informed certification decision to be made. It shall include:

a) identification information, including:
   - the name of the Certification Body;
   - the name of the Applicant;
   - the address of the Applicant;
   - the name of the Applicant's representative;
b) a disclaimer statement, indicating that auditing is based on a sampling of the available information;
c) where applicable, information on the audit plan:
   - the type of audit (initial/surveillance/recertification/special audits);
   - the audit criteria;
   - the audit objectives;
   - the Target of Evaluation, particularly the identification of the organisational or functional units or processes audited and the time of the audit;
   - if applicable, an indication of combined, joint or integrated audits;
d) information on potential deviations:
   - any deviation from the audit plan and their reasons;
   - any significant issues impacting on the audit programme;
e) the information on the Audit Team composition;
f) where applicable, the dates and places of audit activities;
g) the assessment and audit findings:
   - findings with reference to the relevant evidence describing how the requirements are met;
   - **if requirements were not initially met, description of the corrections and corrective actions and their appropriateness;**[12]
   - conclusions, consistent with the requirements of the type of audit;
   - if applicable, significant changes affecting the management system of the Applicant;
   - any unresolved issues, if identified;
h) where applicable, the observations and recommendations made by the Audit Team;
i) where applicable, the assessment of how the Applicant is managing its certification and mark of conformity;
j) where applicable, the report on the corrective actions taken by the Applicant to address the previously identified Non-Conformities;
k) a statement on the conformity and the effectiveness of data protection with a summary of the evidence relating to:
   - the capability of the management system to effectively protect personal data;
   - the internal audit and review of the technical and organizational measures in place;
l) a conclusion on the appropriateness of the Target of Evaluation;
m) confirmation that the audit objectives have been fulfilled.

The Assessment Report shall formally confirm that:

[12] It is highly recommended to collect information on the root causes of the identified Non-Conformities.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

a) the Normative Scope and the Target of Evaluation is clear enough to avoid any risk of misleading understanding of the certification;
b) the Applicant and its representatives were transparent and collaborative in the certification process;
c) the personal data of the Target of Evaluation are:
   - processed lawfully, fairly and in a transparent manner in relation to the data subject;
   - collected for specified, explicit and legitimate purposes;
   - not further processed in a manner that is incompatible with those purposes;
   - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
   - accurate and, where necessary, kept up to date;
   - kept in a form, which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
   - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Ownership and copyrights of the Assessment Report shall be retained by the Certification Body.

8.7.1. Information for Granting Initial Certification

At the end of the assessment process, the Lead Auditor shall prepare and provide the following information to the Reviewer(s) who shall review the findings and prepare the decision:

a) the Assessment Report(s);
b) *"comments on the Non-Conformities and, where applicable, the correction and corrective actions taken by the Applicant;*
c) *confirmation of the information provided to the Certification Body used in the application review;*
d) *confirmation that the audit objectives have been achieved;*
e) *a recommendation whether or not to grant certification, together with any conditions or observations."*[13]

8.7.2. Conclusion Grading

For each audit, the Lead Auditor should summarise its conclusions by using the following grading:

A. **Conformance with the Certification Scheme**: this will normally permit the Applicant to benefit from a formal Europrivacy certification and labelling;
B. **Conformance with the Certification Scheme, with areas of improvement**: this will normally permit the Applicant to benefit from a formal Europrivacy certification and labelling with a commitment to address and improve the identified areas of concern. Defaulting in addressing the areas of improvement may lead to non-maintenance of the certification at the next Surveillance audit;
C. **Non-Conformities to be redressed before certification**: this requires that the Applicant address the Non-Conformities before a potential certification can be granted and provides a credible plan of remediation;
D. **Existence of too many Non-Conformities:** this will normally lead to a formal refusal of the certification and the end of the certification process. In all cases, no certification can be agreed without redressing the Non-Conformities as required.

[13] See clause 9.5.3.1 in ISO/IEC 17021:2015

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

9. Review Process, Decision, and Publication

9.1. Review Process

9.1.1. Duty to Document the Findings Prior to the Review

The Lead Auditors shall document assessment activities, evidence, and findings before submitting their report for review.

9.1.2. Review Process

Certification Body shall have a process to conduct an effective review prior to making a decision for granting certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing certification. The Certification Body shall check that:

a) the information provided by the Audit Team is sufficient to satisfy the requirements and to cover the Normative Scope of the certification;
b) for any Major Non-Conformity, it has reviewed and agreed with the corrective actions;
c) for any remaining Minor Non-Conformity, it has reviewed and accepted the Applicant's plan for corrective actions.

If the review and the certification decision are completed by distinct persons, the recommendations for a certification decision shall be documented.

9.2. Certification Decision

9.2.1. Certification Decision Key Requirements and Process

Once the review process has been completed, the Certification Body shall take a formal decision on the certification. **As requested by ISO, *"the Certification Body shall be responsible for, and shall retain authority for, its decisions relating to certification;"***[14] It *"shall assign at least one person to make the certification decision based on all information related to the evaluation, its review, and any other relevant information."*[15] The Certification Body may also delegate this competence to the Reviewer(s).

The Certification Body shall ensure that:

a) the **persons or committees that make the formal decisions on the certification**[16] **are different from those who carried out the audits**;
b) the individual(s) appointed to conduct the certification decision **have appropriate competence and understanding of the Certification Scheme requirements**;
c) the individual(s) appointed to conduct the certification decision **is *"employed by, or under contract with the Certification Body"***[17].

9.2.2. Decisions

Decisions are made by the Certification Body and can lead to:

a) granting or refusing certification;
b) expanding or reducing the scope of certification;
c) suspending or restoring certification;
d) withdrawing certification or renewing certification.

The period of validity of a certificate shall not exceed three years, renewable through recertification.
The Certification Body shall record and document its certification decisions, including its requests for complementary information.

[14] Section 7.6.1 in ISO/IEC 17065:2012.
[15] Section 7.6.2 in ISO/IEC 17065:2012.
[16] Such as granting, refusing, expanding or reducing the scope, suspending or restoring certification, withdrawing certification or renewing certification.
[17] Or with an entity under the organisational control of the Certification Body that has equivalent requirements.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

9.3. Delivering Certification without or before Accreditation

Formal GDPR certification requires the Certification Body to be granted formal accreditation or Data Protection Authority agreement under Art. 43 GDPR in conformity with EDPB guidelines.

Except where prohibited by law, the Certification Body can start and perform assessments before receiving its formal accreditation or agreement. However, the deliverance of formal certificates under Art. 43 GDPR requires the agreement or accreditation by the competent national authority.

Voluntary certifications delivered outside of the scope of Art. 43 GDPR shall be clearly differentiated and prevent any risk of confusion with formal GDPR certifications.

9.4. Transfer of Certificates

Active certificates can be transferred to another Certification Body during the course of their validity through the following procedure:

a) The Applicant shall complete the Application form of the new Certification Body;
b) The Applicant shall provide the new Certification Body with access to all relevant documentation of its current certification cycle;
c) The new Certification Body shall review the accessed documentation and perform a surveillance or recertification audit in order to take a decision on the certification.

Transfer shall respect the duration and frequency of surveillance audits of the transferred certificate.

9.5. Suspending, Withdrawing, or Reducing the Scope of Certification

9.5.1. Duty to Comply with Authorities Decisions

As required by Art. 58 GDPR, *"the Certification Body shall accept decisions and orders from the competent Data Protection Authority to withdraw or not to issue certifications to an Applicant if the requirements for certification are not or no longer met."*

9.5.2. Procedure for Suspension, Withdrawal, and Scope Adaptation

The Certification Body shall have a transparent procedure for suspension or withdrawal of certificates, or potential adaptation of the Normative Scope and/or Target of Evaluation. This is applicable in situations where an Applicant persistently and seriously fails to maintain compliance with the Certification Scheme requirements or engages in other actions, such as contractual breaches or activities that risk misleading third parties. Examples of valid reasons to suspend, withdraw, or modify the scope of a certificate include, but are not limited to:

a) the Applicant's certified data processing persistently or seriously fails to meet certification requirements, such as:
   - failure to adequately address identified Non-Conformities;
   - insufficient technical and organisational measures to protect the personal data;
b) the Applicant's unreasonable actions or inaction prevents surveillance audits or recertification audits to be performed according to the required frequency or as scheduled;
c) Violation of the terms of the signed certification agreement, such as:
   - non-payment of fees or invoices;
   - incorrect use of the certification mark and/or reference to certification;
d) Applicant's voluntarily requesting temporary suspension;
e) Evidence received that could affect the status of the certificate, such as:
   - evidence of non-compliance of the certified data processing;
   - evidence of non-effective technical and organisational measures in case of serious incidents/accidents.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

9.5.3. Management of Certification Suspension

In case of certification suspension, the Certification Body shall assign one or more persons to formulate and communicate to the Applicant any actions needed to end suspension and restore certification in conformity with the Certification Scheme.

These persons shall have sufficient knowledge and understanding of the Certification Scheme requirements and issues at stake to handle the process and to resolve the suspension if the necessary actions are taken.

Under suspension, the certification of the Applicant's data processing is temporarily invalid.

The Certification Body shall specify a deadline for the Applicant to address and resolve the issue that has caused the suspension. In most cases, the suspension would not exceed six months and can be adapted.

If the issue that caused the suspension is resolved by the Applicant, the certification shall be restored. However, if the issue is not resolved by the Applicant in the time established by the Certification Body, the latter shall either reduce the scope of certification or withdraw the certification.

9.5.4. Adaptation and Reduction of Certification Scope

When a certified Applicant has persistently or seriously failed to meet the certification requirements for specific parts of the Target of Evaluation or Normative Scope, the Certification Body may consider modifying and reducing them in order to exclude the parts not meeting the requirements, provided that:

a) any such reduction shall be in line with the Europrivacy requirements;
b) the modified Target of Evaluation and Normative Scope shall not be misleading and shall be sufficiently consistent and understandable by third parties and by the public.

9.5.5. Obligation to Update Certification Documents and Information

If a certification is terminated, suspended or withdrawn, reinstated or reduced in scope, the Certification Body shall:

a) take actions specified by the Certification Scheme;
b) **where required, inform the competent Data Protection Authority and/or national accreditation authority**[18];
c) ensure that the decision is clearly communicated to the Applicant;
d) request the Applicant to comply with the decision and to adapt its communication accordingly;
e) make all necessary modifications and updates to formal certification documents, public information, authorisations for use of marks, etc.
f) update the Europrivacy Registry of Certificates.

The work performed by the Certification Body to comply with the Certification Scheme shall be charged to the Applicant.

9.5.6. Termination

The Certification Body may decide to terminate the certification process in cases such as:

a) the conditions to perform a reliable certifications process were not met;
b) the Applicant provided misleading information or did not cooperate;
c) the Applicant and the Certification Body jointly decide to terminate the certification process.

In case of termination, including premature termination, the Certification Body shall complete the work related to the decision (such as reporting, recording and documenting the decision, updating the online Registry, etc.) and the Applicant shall cover the related justified costs.

[18] In case of Withdrawal or Suspension, the Certification Body shall also provide the reasons for its decision.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

9.6. Certification Notification and Documentation

9.6.1. Duty to Inform the Data Protection Authority under Article 43

"Article 43(1) requires certification bodies to inform their Supervisory Authority before issuing or renewing certifications to allow the competent Supervisory Authority to exercise its corrective powers *under point (h) of Article 58(2). Additionally, Article 43(5) also requires certification bodies to* ***provide the competent Supervisory Authority with the reasons for granting or withdrawing the requested certification.***" More generally, according to Articles 42 and 43 GDPR, ***"the Certification Body is required to provide the Supervisory Authority with the information (…) necessary to monitor the application of the certification mechanism.***" (EDPB Guidelines 1/2018)

9.6.2. Certification Decision Notification

The Certification Body shall notify the Applicant of the decision to grant or not to grant certification. If the certification is not granted, it shall identify and inform the Applicant of the reasons for the decision.

9.6.3. Prior Requirements before Delivering Certification Documentation

Prior to issuing the certification documentation, the Certification Body shall ensure that:

a) the certification process has been documented and recorded by the Certification Body;
b) the decision to grant or extend the scope of certification has been made;
c) certification requirements have been fulfilled, including the payment of the certificate's fee to the Scheme Owner;
d) the certification agreement has been completed and signed by the Applicant.

Before delivering a certification, the Applicants shall have expressly accepted to comply with the Certification Scheme requirements and with the Europrivacy General Terms and Conditions.

Once the above conditions are met, the Certification Body shall:

a) record the certification in the Europrivacy Registry of Certificates;
b) transmit the certification documentation to its Applicant.

9.6.4. Certification Documentation Content

The certification documentation shall identify the following:

a) **the name and address of the certified Applicant**;
b) **the name and identification of the certified Target of Evaluation**, including version and/or model where applicable;
c) a **short specification of the Target of Evaluation**, including:
   - the type of data processing activities;
   - if relevant, the geographic scope of the certification;
d) whether the Applicant is acting as a **Data Controller, Data Processor, or Joint Data Controller**;
e) where applicable, the name of the **joint controller(s)**;
f) where applicable, any Extension or Adaptation applied to the certification;
g) the **issuance and expiration dates**, including where applicable dates of expanding or reducing the scope of certification, or renewing certification;
h) **the expiration date**;
i) a **unique identification code** of the certificate;
j) **the Europrivacy logo or mark of conformity** provided that its use is neither misleading nor ambiguous;
k) the reference to the **Certification Scheme version** (revision date or version number) used for the certification;
l) the **name and address of the Certification Body**;
m) the **name, title and signature of the person(s) who took the certification decision** or chaired the body that took the decision.
n) if applicable, a means to distinguish the revised documents from any prior obsolete documents.

The certification documentation can take the form of a Certificate, as specified in Section 15.6.4, provided it includes the above mentioned content.

The Scheme Owner can request electronic copy of the delivered and signed certification documentation.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

9.7. Europrivacy Registry of Certificates

"Accredited Certification Bodies must make public permanently and continuously which certification was carried out on which basis (or certification mechanisms or scheme), how long the certifications are valid under which framework and conditions." **(EDPB)**

In order to be valid, a Europrivacy certificate shall be registered and published on the official online Europrivacy Registry of Certificates, which is maintained by the Scheme Owner. The Certification Body shall register and update information in the official Registry.

9.7.1. Public Information Included in the Europrivacy Registry of Certificates

The Registry of delivered Europrivacy certificates shall contain at least the following information on successful certification:

a) the name of the Applicant;
b) the name of the Target of Evaluation, and where applicable its model and/or version;
c) the description of the Target of Evaluation and potential scope exclusions;
d) the reference to the certification scheme and criteria (including version) to which conformity has been certified;
e) the evaluation methods and tests conducted for the evaluation of the criteria (onsite evaluation, documentation review, technical tests, etc.);
f) the summary of the results of the evaluation;
g) the identification of the Certification Body;
h) the date of emission, renewal and termination of the certificate;
i) the duration of validity of the certificate.

Additional information can be stored in the Registry for the purpose of supporting the validation process by the Data Protection Authority and for enhancing the Certification Scheme.

9.7.2. Private Information Provided to the Scheme Owner

On request, the Certification Body shall provide the Scheme Owner with the following information:

a) a copy of the certification reports in pdf format;
b) a pdf file of the certification document with the signature(s) of the authorised person(s);
c) the number of hours of work charged to the Applicant for the assessment;
d) whether, considering the size and complexity of the Target of Evaluation, the calculated audit time was sufficient and adequate to complete a fully reliable assessment;
e) suggestion for improving the certification scheme and/or the list of checks and controls.

9.7.3. Additional Information to be Stored by the Certification Body

The Certification Body shall keep all documentation on the performed certification *"complete, comprehensible, up-to-date and fit to audit"*, including the following:

a) the application form and information;
b) the contractual agreement for the certification;
c) if applicable, the audit programmes;
d) the justification for the auditor time determination;
e) the verification of correction and corrective actions;
f) the documentation of the certification decisions;
g) the relevant records to demonstrate the credibility of the certification, including evidence of the competence of Auditors and Technical Experts;
h) if and where applicable:
   - the initial surveillance and (re)certification audit reports;
   - the justification of the methodology used for sampling of sites;
   - the records of complaints and appeals, and any subsequent correction or corrective actions;
   - the previous certification documents, including the Target of Evaluation;
   - the committee deliberations and decisions.

9.7.4. Data Protection Authority Access to the Registry

Under Article 43 of the GDPR, the competent Data Protection Authority shall have access to the private information transmitted to the Scheme Owner and/or stored in the Registry.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

10. Maintenance and Renewal of Certification

Regular monitoring measures are obligatory for maintaining certification. The period of monitoring of each certification shall be documented.

10.1. Maintaining Certification – General Principles

In principle, the Europrivacy certification is granted for renewable periods of three years. Over this period of time, **the Applicant shall commit:**

- **to ensure compliance of its certified Targets of Evaluations with the applicable Certification Scheme requirements and Criteria; and**
- **to inform the Certification Body of any change or concern regarding its compliance**.

The Certification Body shall maintain certification based on a demonstration that the Applicant continues to comply with the Certification Scheme requirements. **Monitoring and surveillance activities shall be fully supported by the Applicant**.

Identification of any Major Non-Conformity shall lead to a suspension and potential withdrawal of the certification. If an Applicant does not conform to the Certification Scheme requirements (such as the Surveillance activities, the payment of fees, etc.), the certificate shall be suspended or withdrawn by the Certification Body. Such a decision may also be executed by the Scheme Owner and/or by a competent national authority where applicable.

10.1.1. Certification Process Cycle

The initial certification cycle begins on the date of the certification decision and ends on the certification expiration date. Successful certifications and recertifications must be followed by:

a) a first Surveillance Audit within 12 months following the certification date;
b) a second Surveillance Audit within 24 months following the certification date;
c) if applicable, a Recertification Audit within 36 months following the certification date.

A successful recertification completed before the end of the certification period opens a new cycle of 36 months for the certification. If the recertification decision is adopted during the last three months before the expiry date of the previous certificate, the starting date of the new certificate can be established on the date following the expiration date of the previous certificate.

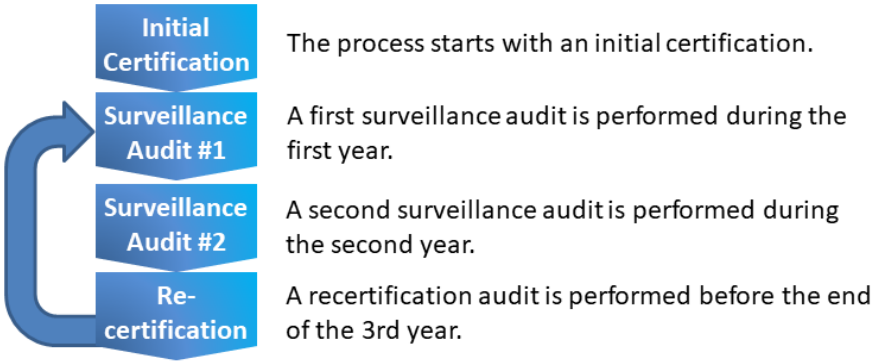

Figure 7 Certification Cycle

10.1.2. Monitoring and Surveillance Audits

Monitoring activities are performed to determine if the Applicant's Target of Evaluation continues to comply with the Certification Scheme requirements between recertification audits.

The Certification Body shall plan and develop its monitoring and surveillance activities on a yearly basis so that key data protection requirements applicable to the Target of Evaluation are monitored on a regular basis.

Surveillance audits can be on-site audits and/or remote audits based on adequate tools and methodologies.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

10.1.3. Priority Focus of Surveillance Activities

Surveillance Activities do not require to reassess all criteria, but shall more specifically focus on:

a) **a review of internal audits, assessment reports** (i.e., risk assessment, Data Protection Impact Assessment, etc.), and top management review by the Applicant since the last assessment;
b) **a review of the progress of work and actions taken by the Applicant** on:
   - the Non-Conformities identified during the previous audit;
   - the regulatory and normative requirements change since the last assessment;
   - the complaints handling;
   - the planned activities for capacity building and continual improvement;
c) **assessing**:
   - the continuity of the lawfulness of the data processing;
   - the effectiveness of the measures in place to respect data subjects' rights;
   - the effectiveness of the Technical and Organisational Measures;
   - the effective use of records and registries;
   - the continuity of the operational control;
   - the adequate use and communication of marks and other references to certification;
d) **the review of any changes to the data processing covered by the Target of Evaluation**.

The Certification Body shall select a set of checks and controls to be verified during the Surveillance Audit. Additionally, it shall apply the specific list of complementary checks and controls for surveillance Audit (*"S – Complementary Surveillance Checks and Controls"*).

10.1.4. Changes Affecting the Certification

Changes to the applicable data protection regulation, such as legislative revision, national or supranational court decisions, EDPB decisions, or European Commission decisions, shall be monitored and addressed by the Certification Body. If these changes impact delivered certifications, the Certification Body shall:

1. Assess the level of impact on the validity of the certification;
2. Elaborate an Action Plan specifying:
   - the identified normative changes;
   - the identified certificates;
   - the proposed adaptation measures such as: targeted reassessment, transition period, suspension, revocation, etc;
3. Where applicable, contact the relevant Data Protection Authority and request validation for the proposed Action Plan;
4. Implement the Action Plan after it has been agreed by the Data Protection Authority.

10.2. Recertification

Europrivacy certificates have a three-year life period and require a recertification assessment to be renewed.

10.2.1. Information for Granting Recertification

Decision to renew a certification shall be based on the results of the recertification assessment, including measures taken by the Applicant to maintain the conformity of the Target of Evaluation and, if applicable, complaints received about this conformity.

10.2.2. Recertification activities (Renewal of Certification)

The purpose of a recertification is to confirm the continued conformity of the Target of Evaluation with the Europrivacy certification requirements. **Recertification shall review and take into account the conclusions of the previous audit reports** of the most recent certification cycle.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

11. Extension of the Certification Scope

The Certification Scheme can be extended to address complementary scopes in two ways:

a) Certification Criteria Extensions;
b) Europrivacy Certification Scheme and Scope Adaptations.

11.1. Europrivacy Certification Criteria Extensions

The Applicant can request to extend the initial GDPR Normative Scope of certification, in order to assess compliance with complementary non-EU national data protection regulations or with other European regulations. The Scheme Owner identifies and specifies each Extension in a separate document with the corresponding complementary criteria to be assessed by the Certification Body. All Criteria Extensions are made available on the Europrivacy Resources and Community website: https://community.europrivacy.com

11.1.1. Adapting the Audit Time and Effort

The assessment time and effort shall be adapted accordingly, in proportion to the number of additional criteria required by the Extension, compared to the regular number of criteria to be assessed without Extension. For instance, if a regular Europrivacy certification of the Target of Evaluation would require the assessment of 50 criteria and the Applicant wants to extend the certification to a national regulation that would require the addition of 5 criteria to the assessment process, then the cost of the certification should be increased by 10%.

11.1.2. Impact on Marks of Conformity

A Criteria Extension enables to deliver a double Certification:

a) a certification of conformity with the regular Criteria;
b) a second certification of conformity according to the additional criteria.

Each one is communicated with a different mark of conformity to be specified by the Scheme Owner.

11.2. Europrivacy Certification Scheme Adaptations

In non-EU jurisdictions, data protection certification can be adapted to different activities, such as management systems of personal data protection. Europrivacy allows to address these adapted cases by the means of Certification Scheme Adaptations, which specify complementary rules and requirements that shall be applied by the Certification Body. The Certification Scheme Adaptations are listed in the document “Europrivacy List of Certification Scheme Adaptations” and are made available on the Europrivacy Community website: https://community.europrivacy.com

From an accreditation perspective, a Certification Scheme Adaptation is considered as a distinct Certification Scheme and is communicated with a different mark of conformity to be specified by the Scheme Owner.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

12. Structural and Organisational Requirements

12.1. Organisational Structure and Top Management

In line with ISO/IEC 17065 rules and principles, the Certification Body shall document its organisational structure, including:

a) the roles and responsibilities of its personnel involved in certification activities.
b) the identification of top management authority responsible for:
   - developing and supervising:
     - management system of the Certification Body;
     - certification requirements;
   - certification-related policies, processes, and procedures;
   - certification activities;
   - assessing, monitoring, and ensuring adequate:
     - personnel competence requirements;
     - performance and responsiveness to complaints and appeals;
     - resource allocation for certification activities;
   - taking decisions on:
     - evaluation and review of certifications;
     - formal decision on certification;
   - delegation of authority to committees or individuals;
     - contractual arrangements.

12.1.1. Data Protection Officer Function

The Certification Body shall have a designated person or office in charge of ensuring internal compliance with data protection regulations, including duties related to the function of the Data Protection Officer.

12.1.2. Operational Control

In conformity with the ISO requirement, the Certification Body working with branch offices and/or any third parties shall establish an appropriate process to monitor and control the certification activities done on its behalf.

12.2. Some Key Roles and Responsibilities

12.2.1. Applicant Exclusive Responsibility

It is the certified Applicant (and not the Certification Body) that has the responsibility of fulfilling and complying with the certification requirements. The legal compliance remains the sole and exclusive responsibility of the Applicant, who shall ensure that its certified Target of Evaluation fully complies with the requirements of the Certification Scheme, and more generally with the applicable data protection regulations.

12.2.2. Certification Body Role and Responsibility

The Certification Body has the responsibility for collecting and assessing sufficient audit evidence upon which to base a certification decision in conformity with the Certification Scheme. According to the audit conclusions, the Certification Body shall make a decision to grant certification if there is sufficient evidence of conformity, or not to grant certification if there is insufficient evidence of conformity.

Within the limits of the law, the Certification Body shall not be liable for any loss or damage whatsoever and howsoever arising as a result of the use of the certified product, process, service, or management system.

12.2.3. Scheme Owner Role

The Scheme Owner is in charge of maintaining and updating the Certification Scheme, as well as delivering, suspending, and withdrawing Europrivacy license to Certification Bodies. The Scheme Owner is also responsible for maintaining the Europrivacy Registry of Certificates, as well as public information on the Certification Scheme. It is not responsible for the certification decisions (which are the responsibility of the

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

relevant Certification Body), nor of the continuous compliance of the Target of Evaluation with data protection regulations (which is the sole responsibility of the Applicant).

The rights and abilities of the Scheme Owner shall be acknowledged and ensured in the contractual obligations binding the Certification Body and its Applicants.

12.2.4. Data Protection Authority Role

Under Art. 43 of the GDPR, the national Data Protection Authorities are in charge of overviewing and controlling the compliance of the certification process with the GDPR.

12.3. Legal and Contractual Matters

As required by ISO/IEC 17065, the Certification Body shall be a legal entity responsible and legally accountable for its certification activities.

12.3.1. Certification Agreement with the Applicant

The Certification Body shall adopt a legally enforceable agreement (or set of agreements) with each Applicant for the provision of certification activities in accordance with the relevant requirements of the Certification Scheme. Certification agreements shall clarify the responsibilities of the Certification Body and its Applicants, and shall apply to all the sites of the Applicant that are relevant for the scope of certification.

12.3.2. Certification Agreement Key Requirements

In conformity with the ISO requirements, the Certification Agreement shall include at least the following obligations for the Applicant:

a) The Applicant shall **commit to comply with the Certification Scheme requirements and related terms and conditions. It shall ensure that its certified Targets of Evaluations comply with the applicable Criteria and data protection regulations**. It shall:
   - **commit to comply with the applicable deadlines and procedures,** including for surveillance audits and payments of audit and certification invoices (regardless of the certification decision);
   - **recognise its full and exclusive responsibility** for complying with the Certification Scheme requirements and the applicable data protection regulations;
   - **acknowledge that the certification does not reduce its responsibility** with regard to the applicable data protection regulations.

b) The Applicant shall **make all necessary arrangements to support the work of the Certification Body**, including by:
   - allowing full transparency and access to all relevant processing activities, sites, premises, processes, procedures, information, data, and personnel necessary to conduct the intended certification;
   - supporting the conduct of the evaluation and monitoring activities, including by providing guides and adopting provisions for accessing and examining relevant documentation, records, equipment, locations, areas, personnel, and access to Applicant's subcontractors, such as Data Processor;
   - recording and investigating any complaints related to its certification;
   - supporting the participation of observers, if applicable.

c) The Applicant shall **provide clear, complete, and transparent information** to the Certification Body (and where requested, to the competent Data Protection Authority) without withholding any relevant information for the certification process.

d) The Applicant shall **make all necessary arrangements to maintain the compliance** of Certified Target(s) of Evaluation with the Certification Scheme and its Criteria, including by:
   - implementing appropriate changes when they are communicated by the Certification Body;
   - ensuring that ongoing certified production, service delivery and/or activity continue to fulfil the related product and Certification Scheme requirements.

e) The Applicant shall **avoid any misleading communication** and any misleading use of the mark of conformity. More specifically, the Applicant:
   - shall make claims only regarding certification that are consistent with:
     - the scope of the achieved and valid certification;
     - the written instructions and guidelines given by the Certification Body;

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

- shall not use or communicate on its certification in any manner that:
    - may be perceived as misleading by third parties;
    - may harm or bring disrepute to the Certification Body or Certification Scheme;
- shall comply with the requirements of the Certification Body and Certification Scheme for communicating its certification, including information related to the Target of Evaluation[19];
- shall comply with the rules specified by the Scheme Owner for the use of logo, certificates, and marks of conformity.

f) The Applicant *"**shall inform the Certification Body, without delay, of any changes that may affect its compliance with the Certification Scheme**."*[20], including in case of incidents such as data breaches.

g) **In case of suspension, withdrawal or termination of a certification, the Applicant shall:**
- **stop using and communicating the related certification**;
- **comply without undue delay with the corresponding obligations** specified in the Certification Scheme and the instructions received from the Certification Body.

h) The Applicant shall **record of all complaints** received and **document the follow-up actions.**

i) The Applicant **shall agree to any supplementary or additional audits, samplings, or other investigations** that the Certification Body may consider as necessary for the certification process or ongoing maintenance of the certification;

j) The Applicant **shall acknowledge and accept that findings may impact the certification process**, including:
- postponement or cancellation of the certification process;
- in the case of significant nonconformities or changes impacting the processing in the Target of Evaluation, the Certification Body may have to repeat part or all the certification process;
- the Certification Body may also need to revise its arrangements and cost estimate.

k) The Applicant **shall refer to Europrivacy certification and use the Europrivacy mark of conformity and labelling only after receipt of the Europrivacy certificate** and in conformity with the rules of use specified by the Scheme Owner;

l) If the Applicant provides copies of the certification documents to others, the documents shall be reproduced in their entirety or as specified in the Certification Scheme.

m) The Applicant shall agree that the information provided for certification process can be accessed by the Scheme Owner, under the seal of confidentiality, for the purpose of controlling, reviewing, or updating the certification process, the same rights are applicable for the accreditation authority of the Certification Body.

n) **The Agreement shall clarify:**
- **the rules of validity, renewal, and withdrawal of the certification**;
- **the structure and procedure for complaints and appeals;**
- **the measures to be taken to address the needs of the customers in case of suspension or withdrawal of the accreditation of the Certification Body.**

12.3.3. Responsibility for Certification Decisions

In line with ISO principles, **the Certification Body is responsible for and retains the authority for its decisions relating to certification**, including the granting, refusing, maintenance of certification, expanding or reducing the scope of certification, renewing, suspending or restoring following suspension, or withdrawing of certification.

There are no obligations for the Scheme Owner to actively monitor individual certifications and/or certified Targets of Evaluation for Non-Conformities. However, where the Scheme Owner is provided with evidence that a certified Target of Evaluation suffers major Non-Conformities, and the Certification Body has not proceeded swiftly to review and act upon the case, the Scheme Owner reserves the right to investigate and unilaterally suspend and/or withdraw any granted certificate.

[19] See also ISO/IEC 17030, ISO/IEC Guide 23 and ISO Guide 27

[20] See clause 4.1.2.2, bullet k in ISO/IEC 17065:2012. Examples of such modifications include: change in the production or management system; changes *"in the legal, commercial, organisational status or ownership; organisation and management (e.g., key managerial, decision-making or technical staff); modifications to the product or the production method; contact address and production sites; major changes to the quality management system."*

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

13. Management of Impartiality and Risks

13.1. Duty of Impartiality

The Certification Body shall demonstrate its independence and that it has procedures in place to prevent conflicts of interest with the certification to be delivered.

The certification process shall be undertaken impartially. **The Certification Body shall not have any prior or present relationship with the Applicant that may compromise its impartiality.**

The Certification Body and its top management *are "responsible for the impartiality of their certification processes and shall not allow commercial, financial or other pressures to compromise their impartiality."*[21]

The Certification Body may be requested to provide evidence of its independence to the competent Data Protection Authority.

13.2. Mechanism for Safeguarding Impartiality

13.2.1. Role and Function of the Mechanism for Safeguarding Impartiality

As requested by ISO, "the Certification Body ***shall have a Mechanism for safeguarding its impartiality."***[22]
The purpose of the Mechanism is to enhance the impartiality of the Certification Body by:

a) reviewing and enhancing the impartiality policy of the Certification Body;
b) addressing and providing guidance on any potential or identified conflicts of interest that may impact the impartiality of certifications.

The Mechanism may be allocated additional tasks and duties as long as they are compatible with the function of ensuring impartiality.

13.2.2. Form of the Mechanism for Safeguarding Impartiality

The Mechanism shall:

a) be formally documented;
b) ensure a diversified and balanced composition of membership;
c) get access to all the information necessary to enable it to fulfil all its functions.

13.2.3. Composition of the Mechanism

The Certification Body shall identify and invite significantly interested parties. Such interested parties can include:

- experts in personal data protection;
- researchers in data protection;
- Applicants of the Certification Body;
- representatives of governmental regulatory bodies such as Data Protection Authorities;
- customers and/or end-users of Applicants or certified Targets of Evaluation;
- conformity assessment experts;
- representatives of non-governmental organisations, such as consumer organisations;
- Auditors;
- Technical Experts.

It is advised to have a diverse set of representatives representing diverse constituencies in the mechanism, such that no single interest predominates. Internal or external personnel of the Certification Body are considered to be a single interest.

[21] Clause 4.2.2 in ISO/IEC 17065:2012
[22] Clause 5.2.1 in ISO/IEC 17065:2012

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

13.2.4. Impact of the Mechanism's Inputs on the Decision of the Certification Body

By default, the Certification Body shall take into account and follow the inputs and guidance provided by the Mechanism.

However, inputs that are in conflict with the operating procedures of the Certification Body or other mandatory requirements shall not be followed. Similarly, inputs that would have a disproportionate impact on the certification process efficiency or effectivity shall not be followed or adapted to mitigate negative effects. Management shall document the reasoning behind the decision to not follow the provided input and shall maintain the document for review by the Scheme Owner and/or by the competent Data Protection Authority.

13.3. Process to Identify and Address Conflicts of Interest

The Certification Body shall have a process to identify, analyse, evaluate, treat, monitor, and document the risks related to conflicts of interest arising from its certification activities, including any conflicts arising from its relationships or from the relationships of its personnel.

13.3.1. Examples of Threats to Impartiality

Threats to impartiality may take several forms, such as:

- Self-interest, including any economic or in-kind interest related to the result of the certification;
- Self-reviewing its own work, for instance, when a Certification Body or a member of an Audit Team has been involved in consultancy for the Auditee;
- Familiarity and complacency that may impact the reliability of the assessment;
- Threats and intimidation;
- Relationships, such as business relationship, ownership or commissioning.

13.3.2. Specific Limitations

In order to preserve their impartiality, the Certification Body and the Auditors shall not:

- provide consultancy or internal audit service to their certified Applicants[23];
- certify an Applicant for which they have delivered consultancy in the last 24 months;
- certify an Applicant for which they have performed an internal audit in the last 24 months;
- be involved in the development, design, manufacturing, distribution, installing, implementing, operating, or exploiting of the data processing to be certified;
- certify other Certification Bodies.

The above-mentioned limitations do not prevent the Certification Body from:

- sharing information with the Applicant and clarifying its findings and expected requirements (it can explain in generic terms what is expected and missing to satisfy the requirements, but it cannot explain how to solve the identified non-compliances);
- using, installing, and/or maintaining a certified product for assessment purpose.

13.3.3. Specific Risks Related to Internal Audits

The carrying out of internal audits by a Certification Body for its certified Applicants constitutes a threat to impartiality. Therefore, **the Certification Body shall not offer or provide internal audits to its certified Applicants**. This applies to any part of the same legal entity and any entity under the Certification Body's organisational control.

[23] See clause 3.2 in ISO/CEI 17065:2012 and ISO/IEC 17021:2011, definition 3.3.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

13.3.4. Specific Risks Related to Consultancy

"The Certification Body and any part of the same legal entity and any entity under the organisational control of the Certification Body shall not offer or provide management system consultancy or similar consultancy services in relation with the scope of the certification."[24]

Similarly, the Certification Body **shall not outsource audits to an organisation providing consultancy services in relation to the scope of the certification**, as this poses an unacceptable threat to the impartiality of the Certification Body. This does not apply to individuals contracted as Auditors.

Personnel who have provided consultancy to or served in managerial capacity for an Applicant, shall not be used by the Certification Body to take part in certification activities for that Applicant for a minimum of two years following the end of the consultancy.

13.3.5. Risks Associated to Linked Legal Entities

The Certification Body shall ensure that its impartiality in certification is not compromised by its linked legal entities. Where a legal entity linked to the Certification Body provides consultancy[25] or develops products or services to be certified, the personnel directly involved in the certification assessment and decision process shall not be involved in the activities of the other entity and reciprocally.

13.3.6. Independence from Consulting Companies

The Certification Body shall not develop joint marketing or be presented as linked with an organisation that provides consultancy. The Certification Body shall take action to correct any inappropriate links or statements by any consultancy organisation stating or implying that certification would be simpler, easier, faster, or less expensive if the Certification Body were used.

This clause does not prevent the participation of the Certification Body in joint communication and marketing activities organised by ECCP to collectively promote Europrivacy related services and the Europrivacy ecosystem of partners (including access to their services). ECCP may also invite its licensed Certification Bodies and Consulting Firms to collaborate, support, and promote the Europrivacy Certification Scheme and ecosystem of qualified service providers.

13.4. Specific Obligations Related to Impartiality

13.4.1. Obligation to Adopt a Formal Impartiality Policy

The Certification Body shall adopt a formal written impartiality policy that includes the following elements:

- a clear commitment and declaration by the top management stressing the importance of impartiality in the exercise of certification activities;
- clear guidelines on how to manage conflict of interest and to ensure objectivity in its certification activities;
- a process to identify, analyse, evaluate, treat, monitor, and document the risks related to conflicts of interest arising from its certification activities including any conflicts arising from its relationships, or from the relationships of its personnel[26].

The Impartiality Policy of certified Certification Bodies shall be accessible to the Scheme Owner.

13.4.2. Personnel's Obligations Regarding Impartiality

The Certification Body's personnel involved in certification activities shall preserve and protect the impartiality of the certification activities. It shall inform the Certification Body of any identified risks or pressure that may influence the impartiality of certifications.

"The Certification Body shall require its personnel, internal and external, to reveal any situation known to them that can present them or the Certification Body with a conflict of interests. The Certification Body records and uses this information as input to identify threats to impartiality raised by the activities of such personnel

[24] Clause 5.2.5 in ISO/IEC 17021-1:2015
[25] See clause 3.2 in ISO/IEC 17065:2012
[26] See clause 4.2.12 in ISO/IEC 17065:2012 and 4.2.1 in ISO/IEC 17021-1:2015; Identifying risks does not imply risk assessments as stated in ISO 31000:2009

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

or by the organisations that employ them, and will not use such personnel, internal or external, unless they can demonstrate that there is no conflict of interest."[27]

13.4.3. Obligation to Document Impartiality Management

Where the Certification Body identifies any threats to impartiality, it shall document and demonstrate how it eliminates or minimises such threats and shall document any residual risk. It shall assess and address both internal and external threats to impartiality.

The Impartiality Monitoring Reports shall be made accessible to the Scheme Owner.

13.4.4. Obligation to Act on Impartiality Issues

The Certification Body shall take action to address any risks to its impartiality. Whenever a risk to its impartiality is identified, the Certification Body shall take action to eliminate the risk(s), or at least to minimise risk(s) to a level that is considered limited and acceptable.

The Certification Body shall take corrective and if required legal action to respond to any threat to its impartiality arising from the actions of other persons, bodies, or organisations.

When a relationship poses an unacceptable threat to impartiality (such as a wholly-owned subsidiary of the Certification Body requesting certification from its parent), then certification shall not be provided.

13.5. Risk Management

13.5.1. Risk Analysis by the Certification Body

Wherever a risk is identified that could impact negatively the impartiality or reliability of the certification process, the top management shall be informed and a risk assessment performed. The risk assessment process can use consultations with appropriate interested parties to advise on matters affecting impartiality including openness and public perception. Such consultations with the appropriate interested parties shall be balanced with no predominating single interest.[28]

Top management shall review any residual risk to determine if it is within the level of acceptable risk.

13.5.2. Risk-based Approach regarding the Applicant

The Certification Body shall take into account the risks associated with providing competent, consistent and impartial certification. **Resource and time allocation should take into account the identified risks**.

When performing the certification process, priority should be given to audit matters that have higher significance and constitute more important risks for the data subjects.

13.5.3. Risk Identification, Liability and Financing

The Certification Body shall demonstrate to the applicable Assessing Body or Data Protection Authority that:

- it has identified, analysed, and assessed the risks related to its activities in certification;
- it has adopted appropriate measures to cover liabilities related to its certification activities in the regions where it operates;
- its financial resources do not expose it to economic pressures.

13.5.4. Scope Limitation

The Certification Body shall clearly specify the scope of each certification.

The certification procedure and activities shall focus on and remain within the agreed scope of certification.

[27] Clause 5.2.13 in ISO/IEC 17021-1:2015

[28] If applicable, the Risk Analysis can be delegated to the Impartiality Mechanism.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

14. Management of Personnel and Resources

14.1. Competencies of Personnel

As requested by the EDPB, the Certification Body shall demonstrate that it has appropriate and ongoing expertise in data protection regulations, including:
- **GDPR requirements;**
- **application of data protection legislation;**
- **technical and organisational data protection measures as relevant.**

14.1.1. Personnel Definition

The "personnel of the Certification Body" refers to all those who are working under the authority of the Certification Body or by the means of a contractual agreement.[29]

14.1.2. Duty to Have Personnel Management Processes

The Certification Body shall have processes to ensure that personnel involved in the certification process have appropriate knowledge and skills. It shall be able to demonstrate it uses Auditors and Audit Team leaders possessing generic auditing skills and knowledge, as well as skills and knowledge appropriate for auditing in specific technical areas.

The Certification Body shall make clear to each person concerned their duties, responsibilities and authorities.

14.1.3. Competence Criteria

The Competence Criteria of personnel certifying under Article 42 of the GDPR shall comply with:
- **the general requirements of the EDPB Guidelines for certification;**
- **the complementary national requirements applicable to the Certification Body.**

The Certification Body shall have a process in place to establish and assess the competence criteria for the personnel involved in certification activities. When setting up an Audit Team, the competence criteria shall take into account the specific requirements of the Target of Evaluation.

A higher level of expertise shall be required from the Lead Auditor in charge of certifying large enterprises, enterprises distributed over several countries, or companies that process special categories of data.

The minimum competence criteria are detailed and specified in the document titled "Management of Competencies of Personnel Involved in Europrivacy Certification Process", which is a binding document and shall be respected by the Certification Body. It documents the criteria of the required knowledge and skills necessary to perform Europrivacy certification tasks.

14.1.4. Personnel Capacity Requirements and Complementary Expertise

The Certification Body shall have access to qualified Auditors and Experts able to apply the present Certification Scheme and to deliver a reliable assessment of compliance with the GDPR and other complementary applicable data protection regulations. The Certification Body shall have access to the necessary technical expertise for advice on matters directly relating to certification activities for all application domains and geographic areas in which the Certification Body operates. Such expertise may be provided externally.

14.1.5. Ability of Decision Makers

Those involved in making decisions in a certification process shall demonstrate that they:
- understand the Certification Scheme;
- are able to assess the outcome of an audit process.

The notion of decision-making in the certification shall be understood as comprehensive and includes a decision to grant, refuse, maintain, renew, suspend, restore a certification, as well as a decision to change the scope of certification.

[29] see clause 6.1.3 in ISO/IEC 17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

14.1.6. Information and Documentation Provided to Auditors and Experts

"The Certification Body shall ensure that Auditors (and, where needed, Technical Experts) are knowledgeable of their audit processes, certification requirements and other relevant requirements. The Certification Body shall give Auditors and Technical Experts access to an up-to-date set of documented procedures giving audit instructions and all relevant information on the certification activities."[30]

14.2. Contractual Obligations of Personnel

14.2.1. Contracts with the Personnel

The Certification Body shall require its personnel involved in the certification process to sign a contract by which they commit:

a) to respect the rules specified in the Certification Scheme;
b) to preserve the confidentiality of accessed information;
c) to prevent any conflict of interests and to declare any situation or relationship that may cause such conflicts.

14.2.2. Personnel Duty of Confidentiality

All personnel acting on behalf of the Certification Body **shall keep confidential all information** obtained or created during the certification process, except if required by law or by the Certification Scheme provisions.

14.3. Management of Competencies

14.3.1. Procedure for the Management of Competencies

The Certification Body shall establish, implement and maintain a procedure and processes for managing the competencies of personnel involved in the management and performance of audits and other certification activities.[31]

The Certification Body shall comply with the competence criteria of personnel specified by this Certification Scheme, as well as with any requirements requested by the competent Data Protection Authority. The Certification Body may adopt additional criteria for competence of personnel with regard to the requirements of the Certification Scheme for each function in the certification process. Where relevant, specific requirements related to specific technical area expertise should be used. The Certification Body shall ensure that it gathers the required competencies in data protection.

As part of the management of competencies, the Certification Body shall:

a) **identify and address training needs** to ensure the personnel involved in certification activities is competent to perform its tasks;
b) document and demonstrate that their personnel has the required competencies to undertake their duties and responsibilities;
c) formally authorise the members of its personnel to perform certification-related functions;
d) monitor and assess the performance of its personnel.

14.3.2. Selection Process

The Certification Body shall have processes in place for selecting, training, and formally authorising Auditors and Technical Experts used in the certification. The initial competence evaluation of Auditors includes their ability to apply required knowledge and skills during audits, including by observing them conducting an audit.

Personal behaviour of the Auditors can affect the ability to perform specific functions. The Certification Body shall consider personal behaviour during the selection and training process. It shall take advantage of personal behaviour strengths and shall minimise the impact of their weaknesses.

For onsite audits, a description of desired personal behaviour for personnel involved in certification activities is described in Annex D of ISO/IEC 17021-1:2015.

[30] Clause 7.2.6 in ISO/IEC17021-1:2015
[31] see Section 7 in ISO/IEC 17065:2012 and Clause 9 in ISO/IEC 17021-1:2015

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

14.3.3. Evaluation Processes

The Certification Body shall have a documented process and competence criteria in place for the initial competence evaluation and ongoing monitoring of competencies and performance of all personnel involved in certification activities. The Certification Body shall demonstrate that its evaluation methods are effective to assess and monitor the competencies of personnel and to ensure they have the selected personnel with adequate level of competencies prior to taking responsibility for the performance of their activities for Europrivacy certifications.

14.3.4. Personnel Records

The Certification Body shall maintain up-to-date records of all its personnel involved in Europrivacy certifications, including auditors, experts, and administrative personnel.

In line with ISO/IEC requirements, the Personnel Record should include the following information[32]:

a) personal details (name, address, etc.);
b) professional experience (employers, positions, etc.);
c) education and qualifications;
d) experience and complementary training;
e) evaluations of their competences;
f) monitoring of their performance;
g) functions and authorisations held within the Certification Body;
h) the date of the last update of each record.

14.3.5. Overall Performance of the Personnel

The Certification Body shall monitor and document the competence and performance of its personnel. It shall regularly review its competencies and identify training needs.
When monitoring the competence of its Auditors, the Certification Body shall:

- periodically evaluate the performance of each Auditor on-site;
- combine on-site evaluations, review of audit reports and feedback from Applicants (or relevant stakeholders);
- minimise the impact on or disturbance to the certification process and to the Applicants.

14.4. Use of External Resources for Evaluation

14.4.1. General Obligation

When a Certification Body performs evaluation activities with external resources, they shall comply with the requirements of the Certification Scheme, including the impartiality requirement.

14.4.2. Use of individual external Auditors and external Technical Experts

The Certification Body shall require from all external Auditors and external Technical Experts to sign a written agreement in which they commit to:

a) comply with the rules, processes and procedures of the Certification Body;
b) preserve confidentiality and impartiality;
c) notify the Certification Body of any existing or prior relationship with any organisation they may be assigned to audit.

14.4.3. Clarification on the Notion of Outsourcing

ISO 9001:2008 sub-clause 4.1 defines an outsourced process as *"a process that the organisation needs for its quality management system and which the organisation chooses to have performed by an external party."* The terms "outsourcing" and "subcontracting" can often be considered as synonyms. However, "outsourcing" does not refer to the use of external personnel individually contracted to operate under the direct authority of the Certification Body, even if their work is charged to the Certification Body by a third party.

[32] See Section 6 in ISO/IEC17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

14.4.4. Use of Outsourcing

The Certification Body may outsource evaluation activities only to bodies that meet the applicable requirements of the Certification Scheme, including:

- **an appropriate level of expertise in data protection;**
- impartiality and confidentiality requirements;
- the applicable ISO/IEC 17065 requirements when certifying data processing related to products, processes and services.

This can include outsourcing to other Certification Bodies.

14.4.5. Prohibition to Outsource Decisions

All Decisions on a certification (see 6.3) shall remain under the direct and effective control of the Certification Body and cannot be outsourced.

14.4.6. Required Process and Agreement for Outsourcing

The Certification Body shall have a process in place for the approval and monitoring of service providers of outsourced services used for certification activities. It shall:

- ensure they have adequate expertise;
- ensure they keep records of the competencies of all personnel involved in certification activities;
- keep a documented record of the validated service providers;[33]
- adopt a legally enforceable agreement with adequate provisions for confidentiality and conflicts of interests, including the obligation to declare any relationship and impartiality issues with Applicants to be certified.

The Certification Body can rely on third parties monitoring and assessment, such as governmental authorities, accreditation bodies or peer assessment bodies.

14.4.7. Responsibility of the Certification Body in Outsourcing

The Certification Body retains responsibility for outsourced activities. It shall ensure that the body in charge of performing the outsourced tasks conforms to the Certification Scheme and applicable ISO requirements, including in terms of competence, impartiality, and confidentiality.

[33] Clause 6.2.2.4 in ISO/IEC 17065:2012, also requires to *"implements corrective actions for any breaches of the contract or other requirements of which it becomes aware;"* and to *"inform the Applicant in advance of outsourcing activities, in order to provide the Applicant with an opportunity to object."*

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

15. Management of Information and Confidentiality

This section applies to the Certification Body.

15.1. Management and Classification of Documents

*"**Certification mechanisms should provide for a standardised documentation methodology.** Thereafter evaluations will allow comparison of the certification documentation with the actual status onsite and against the certification criteria.* (…) *The documentation produced during the evaluation should, therefore, focus on three main aspects:*
*- **consistency and coherence of evaluation methods executed**;*
*- evaluation methods **directed to demonstrate compliance of the certification Object** with the certification criteria and thus with the Regulation; and*
*- that the results of the evaluation have been **validated by an independent and impartial certification body**."*
(EDPB Guidelines 1/2018)

15.1.1. Objectives of Document Classification

The Certification Bodies shall use a clear and consistent classification and identification of each document. The identification and classification of Europrivacy-related documentation shall be structured in order to ensure:

- a well-specified and reliable certification process;
- clear and user-friendly access to updated information and documentation.

15.2. Confidentiality of Information and Data Protection

15.2.1. Duty of Confidentiality and Data Protection

The Certification Body is responsible for adequately managing and protecting information collected and/or generated during the certification process.

The Certification Body and all parties involved in certification processes shall also protect personal data and comply fully with the provisions of the GDPR, and other applicable data protection regulations.

It shall put in place adequate contractual mechanisms to ensure that all its bodies and agents acting on its behalf comply with the above-mentioned obligations.

15.2.2. Personnel Obligations to Preserve Confidentiality

All personnel involved in the certification activities or having access to internal information shall preserve and protect the confidentiality of all confidential information related to the certification.

15.2.3. Scope of Confidentiality

By default, all information provided by the Applicant or related to the Applicant and its certification shall be treated as confidential information, except if the information:

- is publicly available; or
- is qualified as non-confidential by the Applicant; or
- is disclosed with the agreement of the Applicant; or
- has to be disclosed for legal or contractual reasons.

Confidentiality does not apply to information that has to be published on the Registry and does not prevent legitimate access to information by authorised parties, such as Data Protection Authorities.

15.2.4. Legitimate Third-Party Access to Confidential Information

The Certification Body may be required by law to release confidential information and shall comply with such requests.

The Data Protection Authorities and the Scheme Owner may request access to confidential information in order to perform their duty, such as surveillance and complaint processing of certifications. Where justified, the Certification Body shall provide adequate and proportionate access to the requested information, provided that the accessing party is bound by confidentiality obligations.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Access to information that is part of regular surveillance and monitoring of the certification activity does not require any specific notification to the Applicant. In other cases, the Applicant should be informed, unless this is prohibited by law.

15.2.5. Confidentiality and Privacy Compliant Infrastructure

The Certification Body shall ensure secure and confidential processing of information of its Applicants. It shall have:

a) **an adequate infrastructure to securely store, process, and transmit confidential information** and records on Applicants;
b) **a documented policy and procedures on data retention and personal data minimisation**;
c) **a Privacy and Data Protection Policy** publicly accessible from its website.

Only authorised persons, with a contractual or legal obligation to preserve the confidentiality of information, shall have access to the stored data and files.

The Certification Body shall ensure that its online tools and websites comply with the GDPR.

15.3. Information Exchange between the Certification Body and its Applicants

15.3.1. Initial Information Provided to the Applicant

The Certification Body shall provide clear information to the Applicants, including:

a) a **description of the certification process**, including:
   - application;
   - audit and assessment, including surveillance audits, where applicable;
   - decision process for granting, refusing, maintaining, renewing, suspending, withdrawing, or restoring a certificate;
   - process for expanding or reducing the scope of certification;
b) the **normative references** and requirements for the certification;
c) information on **costs and fees for the Applicant**, including for maintaining its certification and for recertification;
d) the **Applicant's obligations**, including to:
   - **comply with Certification Scheme rules and requirements**;
   - **make all necessary arrangements to facilitate the work of the Certification Body** and to provide adequate access to all relevant areas, documentation, files and personnel at all stages of the process;
   - authorise the potential participation of observers for assessing the work of the Auditors;
e) information on the **rights and obligations of certified Applicants**, including when communicating its certification;
f) information and contact for **complaints and appeal**.

15.3.2. Documentation and Information on Tasks and Responsibilities

The Certification Body shall maintain documentation of its tasks and responsibilities regarding its certification activities, including on the application process, for the purpose of:
- information on the status of an application;
- evaluation by the competent Data Protection Authority.

15.3.3. Notice of changes by a Certification Body

The Certification Scheme has been developed to address the European data protection regulations, which are subject to changes, including through evolving jurisprudence. Technological evolution may also impact the technical requirements and the evaluation criteria required by the Certification Scheme. Similarly, the Certification Scheme requirements are expected to evolve over time.

The Scheme Owner with the support of its International Board of Experts shall determine any necessary adaptation of the Certification Scheme.

When a modification of the Certification Scheme is adopted by the Scheme Owner, the Certification Bodies shall verify that the certified Targets of Evaluation of their Applicant(s) comply with the new requirements.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

The Certification Body shall give certified Applicants due notice of any changes to requirements for certification that may impact their certification, and shall provide information on the new requirements.

15.3.4. Notice of changes by a certified Applicant

The Certification Body shall establish adequate contractual arrangements to be informed by the certified Applicant, without delay, of any change that may affect the capability of the certified Target of Evaluation to continue complying with the requirements of the Certification Scheme. It encompasses any change related to:

a) extending the purpose and scope of the data processing;
b) extending the categories of personal data processed in the Target of Evaluation;
c) new Data Processors involved in the Target of Evaluation;
d) new site's location, including the geographic location of server infrastructure processing or storage of personal data;
e) new cross-border transfer of personal data;
f) important legal, commercial, organisational changes, including modification in the effective control and/or ownership of the Applicant and/or its certified Target of Evaluation;
g) important organisational and management decisions that may impact the certified Target of Evaluation, such as change of Data Protection Officer;
h) if applicable, the scope of operations under the certified Target of Evaluation;
i) any major changes to the certified Target of Evaluation, such as the release of a new version;
j) contact address.

In the event of such changes, the Certification Body shall take appropriate actions, which may include the following:

a) evaluation;
b) review;
c) certification decision;
d) issuance of revised formal certification documentation (including monitoring or surveillance activity) to extend or reduce the scope of certification.

Records shall include the follow-up actions and rationale for excluding any of the above activities.

15.4. Public information

The Certification Body shall have clear rules governing the disclosure of public information on its communication platforms.

15.4.1. Public Information Made Available without Request

The Certification Body shall maintain and make public (through publications, electronic media or other means) **without request**, in all the geographical areas in which it operates, general information about:

a) certification assessment process;
b) decision process related to the certification and its scope;[34]
c) types of data processing activities it can certify;
d) the use of the name, logo and mark of conformity attached to delivered certifications;
e) processes in place for handling the requests for information, complaints and appeals;
f) the policy and mechanism of impartiality;
g) contact details of the Certification Body, such as the postal address;
h) the personal data protection policy of the Certification Body and a process to contact its Personal Data Protection Officer.

[34] Such as decisions for granting, refusing, maintaining, renewing, suspending, restoring, or withdrawing certification or expanding or reducing the scope of a certification.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

15.4.2. Public Information Made Available upon Request

In conformity with ISO requirements, the Certification Body shall provide **upon request** complementary information about:

a) *"the geographical areas in which the Certification Body operates;*
b) *the status of a given certification;*
c) *the name, related normative document, scope and geographical location (city and country) of certified Applicant;*[35]
d) *information about (or reference to) the Certification Scheme, including evaluation procedures, rules and procedures for granting, for maintaining, for extending or reducing the scope of, for suspending, for withdrawing or for refusing certification;*
e) *a description of the means by which the Certification Body obtains financial support and general information on the fees charged to applicants and to Applicants;*
f) *a description of the rights and duties of applicants and Applicants, including requirements, restrictions or limitations on the use of the Certification Body's name and certification mark and on the ways of referring to the certification granted;*
g) *information about procedures for handling complaints and appeals."*[36]

The Certification Body may require that interested parties request this information in writing through postal mail and that they include an email address that can be used for reply.

Access to certain information can be limited by legitimate interests on the request of the Applicant (e.g., for security reasons) or for confidentiality or data protection reasons.

The Certification Body can also make the information public without request on its internet website.

15.4.3. Common Registry and Public Information Website

The Scheme Owner is in charge of managing and overviewing the official Europrivacy website with the official reference documents, as well as the Europrivacy Registry of Certificates. Certification Bodies can replicate the public information in their own website as long as it is consistent with the information provided by the Scheme Owner.

Certification Bodies shall keep the central Registry updated with their Applicants and certification processes information and shall avoid any delay in updating the information.

Licensed Certification Bodies shall provide a link from their website to the Europrivacy Registry of Certificates and public information website.

15.4.4. Information Reliability

Information provided by the Certification Body to any Applicant or to the marketplace, including advertising, shall be accurate and not misleading. Any use of Europrivacy-related mark, including trademark and logo, shall respect the Europrivacy rules and guidelines for marketing and communication.

15.5. Obligation to Keep Records of the Certification Process

15.5.1. Duty to Keep Records

The Certification Body shall keep records to demonstrate that all certification process requirements have been effectively fulfilled. The Certification Body shall ensure that these records are transported, transmitted, and stored in a way that ensures confidentiality is maintained.

15.5.2. Access Rights

The Scheme Owner and where applicable, the Data Protection Authorities and/or licensed bodies, may request access to confidential information and records to perform their duties, such as surveillance and complaint management. The Certification Body shall cooperate and provide access to the requested information.

[35] See clause 8.1.2 bullet a to c in ISO/IEC 17021-1:2015
[36] Clause 4.6 bullet a to d in ISO/IEC 17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

15.5.3. Period of Retention

By default, the records on delivered certifications shall be retained for the duration of the related cycle of certification plus ten years. The retention period may be extended when required by law or in order to address legitimate interests of the Certification Body such as to mitigate legal risks or the need to access historical data in the context of envisaged recertifications. Where the retention period is to be extended, the rationale for doing so shall be recorded by the Certification Body. At the end of the retention period, the records shall be erased.

15.6. References to Certification and Use of Marks of Conformity, Licenses and Certificates

15.6.1. Use of Certificates, Labels and Marks of Conformity

The Europrivacy logo and the mark of conformity are and shall remain the property of the Scheme Owner. They can be used by the Applicant only after approval by and under the supervision of the Certification Body.

The Certification Bodies and Applicants **shall comply with the rules of the Certification Scheme governing the use of certificates and mark of conformity, and with its rules and guidelines for communication on Europrivacy.** The main rules are specified by the Scheme Owner and can be complemented with additional rules specified by the Certification Body.

The Certificates of conformity shall:

- **provide clear information** on the certification scheme and the Target of Evaluation;
- **prevent any misleading communication** regarding the scope of the certification;
- **enable traceability** back to the Certification Body and its Registry.

There shall be no ambiguity as to the extent of the certification for which it has been granted. For instance, using a certified data processing to claim that the company as a whole is certified is forbidden and may lead to suspension or withdrawal of the certificate.

The detailed rules and specifications regarding the use of the Europrivacy certificates and marks of conformity are specified in the document "Europrivacy Rules on the Use of Logo, Certificates, and Marks of Conformity", which is a binding document that all parties shall respect.

15.6.2. Right to Control Compliant Use

The Certification Body and the Scheme Owner have the right to exercise control over ownership, use and display of licenses, certificates, marks of conformity, and any other mechanisms for indicating that data processing is certified by the Certification Body.

The Certification Body shall check whether "*incorrect references to the Certification Scheme, or misleading use of licenses, certificates, marks, or any other mechanism that may indicate that product, process or service is certified, found in documentation or other publicity*"[37]. If such a case occurs, it should be dealt with by suitable action by the Certification Body.

15.6.3. Europrivacy Mark and Logo

The Europrivacy logo is composed of the letters "E" and "P" in blue colour, with six yellow stars, as presented in the examples below:

Figure 8 Europrivacy Logo and Mark of Conformity

[37] Clause 4.1.3.2 in ISO/IEC 17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

The term Europrivacy and the logo are trademarks belonging to the Scheme Owner. Their use is subject to written authorisations and to strict rules.

15.6.4. Certificates

"A certificate, seal or mark under the GDPR can only be issued following the independent assessment of evidence by an accredited Certification Body or competent Supervisory Authority, stating that the certification criteria have been satisfied." (Source: EDPB Guidelines 1/2018)

Certified data processing can receive a Europrivacy certificate under the control and approval of the Certification Body. Certificates shall include at least:

a) the **Certification Body logo and Europrivacy logo**;
b) the **name of the Applicant**;
c) whether the Applicant is acting as a **Data Controller, Data Processor, or Joint Data Controller**;
d) where applicable, the **name of the joint controller(s)**;
e) a clear **description of the Target of Evaluation** and its **geographic scope**;
f) where applicable, **any Extension** applied to the certification;
g) the **dates of issuance and expiration of the certificate**;
h) the **unique identifier** of the delivered certificate;
i) the mention *"Detailed information at"* followed by the domain name of the Certification Scheme website and online Europrivacy Registry of Certificates: http://www.europrivacy.com;
j) the **name and address of the Certification Body** issuing the certificate.

The Certificates shall be clear and easily understandable by data subjects. They should preferably not exceed one page.

15.6.5. Mark of Conformity

Where applicable, certified data processing can be labelled with the Europrivacy mark of conformity, under the control and approval of the Certification Body.

The Mark of Conformity shall always include:

a) the Europrivacy logo;
b) the unique certification identifier;
c) the domain name of the Certification Scheme website (http://www.europrivacy.com), which gives **access to the online Europrivacy Registry of Certificates** with detailed information on the delivered certificate thanks to its unique identifier.

The Marks of Conformity for Criteria Extensions are specified by the Scheme Owner and clearly indicate the related normative extension.

Examples of Marks of Conformity are presented below:

Figure 9 Examples of Marks of Conformity

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

15.6.6. Statements of Conformity

Applicants can include statements of certification on their website or on other relevant information and documentation, subject to the Certification Body prior written approval.

The Statement shall always include:

a) the reference to Europrivacy and, where authorised, the Europrivacy logo;
b) the name of the certified Applicant;
c) where applicable, the name of the joint controller(s);
d) a clear indication of the Target of Evaluation and its geographic scope;
e) where applicable, a clear indication of complementary norms or requirements that have been added;
f) the dates of issuance and validity of the certificate;
g) the unique identifier of the delivered certificate;
h) the mention *"Detailed information at"* followed by the domain name of the Certification Scheme website and online Europrivacy Registry of Certificates: http://www.europrivacy.com;
i) the name and address of the Certification Body issuing the certificate.

Where the certification is delivered on a voluntary basis without the Applicant seeking validity under GDPR Art. 42 and 43, the statement of conformity shall clearly state it.

Here is an example of a certification statement:

Statement of Conformity

with the GDPR and Europrivacy

Applicant
COMPANYNAME.SA
123 Address street
1111 City, Country
declares under its sole responsibility that the following data processing is in conformity with the following requirements:

Certification

Target of Evaluation:	Personal data processing by the smart parking solution deployed on the municipal territory of the city ABC.
Normative Scope:	Europrivacy criteria, v. 05.03.2019
Certified on and until:	April 27 2019 – April 26 2022
Certificate ID:	83F4:A014
Detailed information at:	www.europrivacy.com
Certification Body:	CERTIFICATION.SA 567 Address street 2222 City, Country

Signature

Authorized representative:	Mr ABC
Date:	May 3 2019
Signature:	XXXXXX

Figure 10 Certification statement

15.6.7. Statements and Marks of Conformity on Electronic Supports

If a certificate, a statement, or a mark of conformity related to a Europrivacy certification is displayed on electronic support, such as a web page or pdf document, it should include a direct hyperlink to the Certification Scheme main homepage (http://www.europrivacy.com) or to the specific page of the certified Target of Evaluation in the online Registry.

15.6.8. Restrictions on the Use of Certificates and Marks of Conformity

Marks of conformity, certificates, and statements of certification shall not be used in a manner that is likely to cause confusion or misleading communication about the Target of Evaluation of the referred certification.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

15.6.9. Applicant Contractual Obligations

The Certification Body shall, by means of legally enforceable arrangements, require that the certified Applicant:

a) conforms to the requirements of the Certification Scheme and the instructions given by the Certification Body when communicating on its certification;
b) prevents and excludes any misleading communication on its certification, including its effective scope and actual status;[38]
c) receives the approval of the Certification Body before using a mark of conformity in relation to its delivered certification;
d) adapts without any delay its communication to any change in its certification, such as scope reduction, suspension or withdrawal, by amending or discontinuing the use of communication material referencing to the certification;
e) does not use its certification in any way that may harm the reputation and trust of the Certification Body and Certification Scheme.

15.6.10. Additional Statement for Applicants Acting as Data Importers

Where the Applicant acts as a Data Importer based in a third country without an adequacy decision, the Certification Body and the Applicant shall both state in writing that they have no reason to believe that the legislation and practices applicable to the Target of Evaluation may prevent the Applicant from fulfilling its obligations under the certification.

15.6.11. Certification Body Control

The Certification Body "*shall exercise proper control of ownership"* of the use and reference to its delivered certificates, and it shall *"take action to deal with incorrect references to certification status or misleading use of certification documents, marks or audit reports. Such action may include requests for correction and corrective action, suspension, withdrawal of certification, publication of the transgression and, if necessary, legal action."*[39]

The Scheme Owner can request Certification Bodies to investigate cases of misuse or potential Non-Conformity. The Certification Body shall then proceed without undue delay.

In case of factual evidence that a certified Target of Evaluation suffers Major Non-Conformity or could negatively impact the reputation of, and trust in, the Certification Scheme, the Scheme Owner can take provisional or derogatory measures to suspend and/or withdraw a certification without the consent of the Certification Body.

[38] Additionally, ISO expressly requires that communication on a certification avoid any ambiguity between product and process certification and management system certification.
[39] Clause 8.3.5 in ISO/IEC 17021-1:2015

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

16. Quality Management of the Certification Body

Certification Bodies benefiting from a valid and active national accreditation under ISO/IEC 17065 or 17021-1 are deemed to comply with the requirements of this section.

16.1. Certification Body Management System Requirements

The Certification Body shall establish and maintain an adequate management system complying with the requirements of this Certification Scheme in accordance with one of the two options proposed by ISO/IEC 17065, namely:

a) Option A: The Certification Body shall establish a management system with:
   - clear documentation of the general management system;
   - effective control of documents and records;
   - yearly internal audit;
   - yearly management review;
   - corrective and preventive actions;

b) Option B: The Certification Body shall establish a management system in accordance with the ISO 9001 requirements. It shall be capable of demonstrating the consistent fulfilment of these requirements.

"The procedures in the event of suspension or withdraw of the accreditation of the Certification Body shall be integrated into the management system of the certification body, including notification of customers." (EDPS)

16.2. Specific Requirements for Option A

16.2.1. General Management System Documentation

The General Management System documentation shall reference all relevant documentation (including processes and records) to comply with the requirements of the Certification Scheme.

The top management of the Certification Body shall:

a) adopt and maintain a set of **policies and objectives** to comply with the Certification Scheme requirements;
b) ensure that its policies and objectives are **acknowledged by all those involved in certification activities and effectively implemented** across the organisation;[40]
c) **provide evidence of its commitment** to improve and comply with the management system;
d) **appoint a person responsible** for:
   - *"ensuring that processes and procedures needed for the management system are established, implemented and maintained;*
   - *reporting to top management on the performance of the management system and any need for improvement."* [41]

16.2.2. Control of Documents

The Certification Body shall have procedures in place to control the documents related to its certification activities and for its compliance with the Certification Scheme. It shall encompass all relevant documents, regardless of their forms and medium.

The procedures shall determine and specify the required controls to:

a) formally approve documents (before issue and/or entry into force);
b) revise, update and re-approve documents, including:
   - indicating document changes and the current revision status;
   - making available all relevant versions of the applicable documents;

[40] According to ISO/IEC 17065, all personnel involved in certification activities shall have access to the parts of the management system documentation and related information that are applicable to their responsibilities.
[41] Section 8.2.3 in ISO/IEC 17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

- preventing unintended use of obsolete documents and applying suitable identification to them;

c) ensure that:
   - documents remain legible and readily identifiable;
   - external documents are identified and their distribution is controlled.

16.2.3. Control of Records

The Certification Body shall have in place procedures to manage and control its audit records, including their identification, storage, protection, retrieval, retention time, and disposition.

16.2.4. Management Review

The Certification Body's top management shall have procedures in place to review the adequacy and effectivity of its management system at least on a yearly basis.

Review inputs

The input to the management review shall include information related to the following:

a) internal and external audits results;
b) information on relevant appeals and complaints from users of certification activities;
c) feedbacks received from:
   - the Applicants
   - the relevant stakeholders, including the Scheme Owner and/or other qualified authorities;
   - the mechanism for safeguarding impartiality;
d) the reviews of:
   - the impartiality;
   - the appeals and complaints;
   - the personnel qualifications and needs for training;
   - the preventive and corrective actions;
   - the follow-up actions from previous management reviews;
   - the fulfilment of the objectives;
   - the changes that could affect the management system.

Review outputs

The management review shall include a set of decisions and actions for:

a) improving the effectiveness of the management system and its processes;
b) enhancing the compliance with and implementation of the Certification Scheme;
c) assessing resource needs.

16.2.5. Internal Audits

The Certification Body shall establish procedures and perform internal audits[42] on a yearly basis, with the objective to check and improve:

a) its compliance with the Certification Scheme requirements;
b) its management system.

The Certification Body shall plan an audit programme that takes into account the results of the previous audits. It shall ensure that:

a) the internal Auditors are knowledgeable in certification, auditing and in the requirements of this Certification Scheme;
b) the internal Auditors do not audit their own work;
c) the personnel responsible for the audited area is informed of the audit results;
d) the relevant actions resulting from the audit are addressed in a timely and appropriate manner;
e) relevant opportunities for improvement are identified.

The Auditors shall write a synthetic audit report including their general appreciation and the identified divergences. Identified divergences shall be noted into a form for improvement.

[42] ISO 19011 provides guidelines for conducting internal audits.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

16.2.6. Corrective and Preventive Actions

The certification body shall have **procedures in place for managing Non-Conformities** and for taking appropriate actions to eliminate the causes of effective or potential Non-Conformities.
As required by ISO/IEC 17021-1, it shall have processes for:

a) "identifying Non-Conformities (e.g., from complaints and internal audits);
a) determining their causes;
b) correcting the identified Non-Conformities;
c) assessing if actions are needed to ensure that Non-Conformities do not recur;
d) determining and implementing the needed actions in a timely manner;
e) recording the results of actions taken;
f) *reviewing the effectiveness of corrective actions*."[43]

16.2.7. Direction Review Meeting

Once a year, all employees involved in the certification process shall meet to review the implementation of the Certification Scheme and its quality management. Board members shall be invited to attend the Direction Review Meeting.

The Direction Review Meeting shall consider in its agenda:

a) Follow-up of the action points of the previous Direction Review Meeting;
b) Complaints, appeals, Non-Conformities and derogations;
c) Quality management system;
d) Personnel monitoring and capacity building;
e) ICT infrastructure and security;
f) External information and communication.

The Direction Review shall produce a synthetic report, including wherever relevant:

a) An action plan with preventive and improvement actions;
b) A quality management plan;
c) Evaluation of personnel needs (such as recruitment and training);
d) Recommendations to strengthen the ICT infrastructure security.

[43] Section 8.7.4 in ISO/IEC 17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

17. Appeals and Complaints

Certification Bodies benefiting from a valid and active national accreditation under ISO/IEC 17065 or 17021-1 are deemed to comply with the requirements of this Section.

17.1. General Principles

Appeals to a decision can be filed by the Applicant to the Certification Body, or by the Certification Body to the Scheme Owner, whichever has taken the decision.

A third party considering that a certified Target of Evaluation is not complying with the Certification Scheme or with the applicable data protection regulations covered by the certificate can submit their complaint to the certified Applicant, to the Certification Body, or to the competent authority. Complaints shall be based on factual findings and evidence.

According to the communicated evidence, the receiving party shall inform the Certification Body and/or the Data Protection Authority. If the information revealed by the complaint may have an impact on the public trust and reputation of the Certification Scheme, the Scheme Owner shall be informed without any delay.

In case the complaint would not have been properly processed by the Certification Body, the complaining party is invited to inform the Scheme Owner about the issue.

17.2. Appeals and Complaints Policy

The Certification Body shall have a clear mechanism to collect, to document, and to address complaints or appeals.

Submission of, investigation and decisions on complaints/appeals shall not result in any discriminatory actions from the Certification Body against the complainant/appellant.

The complaint and appeal mechanism shall specify:

a) **who can file complaints or objections**, including at least any public administration and the data subjects whose personal data are processed by the certified Target of Evaluation;
b) **the process for receiving, validating, investigating and processing appeals and complaints**, including:
   - a procedure and time limit to confirm if the complaint or appeal is related to a certification delivered by the Certification Body;
   - **the possibility for consultation of interested Parties;**
   - **where applicable, time limits;**
c) **who is in charge** of the process on behalf of the Certification Body;
d) **a process to systematically record, document, and monitor the appeals and complaints**, as well as the actions undertaken to resolve them;
e) **a process to ensure that the appropriate corrective actions are taken**.

The Scheme Owner can establish complementary processes and mechanisms to handle complaints and appeals that shall be supported and respected by the Certification Body and the Applicant.

17.2.1. Duty to Collect and Document Complaints and Appeals

The Certification Body and its employees are responsible for recording all received complaints, appeals, and subsequent actions.

Upon receipt of a complaint or appeal related to certification activities, the Certification Body shall:

a) acknowledge receipt of a formal complaint or appeal;
b) gather and verify all relevant information;
c) give formal notice of the outcome of the process to the complainant or appellant;
d) take any subsequent action needed to resolve the complaint or appeal;
e) inform the Scheme Owner of any major issues that may constitute a risk for the Certification Scheme or for its reputation.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

17.2.2. Duty to Proceed and to Be Diligent

Where complaints are found to be valid, the Certification Body shall address them appropriately and a reasonable effort shall be made by the Certification Body to resolve them.

The Applicant and Certification Body shall provide full support to investigate and provide clarifications in order to process and resolve the complaint. A well-grounded complaint may lead to the suspension or withdrawal of the certificate.

17.2.3. Duty to Use Neutral Persons

In order to ensure an unbiased process, the decisions related to a complaint or an appeal shall be adopted by individuals who:

- were not directly involved in the related certification process;[44]
- did not deliver services to the complaining Party or to the Certified Applicant.

[44] See Section 7.13.5 in ISO/IEC 17065:2012

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

18. Scheme Owner

18.1. Role of the Scheme Owner

The Scheme Owner is in charge of:

a) maintaining, updating, and improving the Certification Scheme, its checks and controls, its terms and conditions, and other related documentation;
b) maintaining public information on the Certification Scheme;
c) maintaining and making available the online official Europrivacy Registry of Certificates, whose content is provided by the Certification Bodies;
d) fixing the terms and conditions for licensing and using the Certification Scheme, including related fees;
e) licensing the right to use the Certification Scheme and associated Intellectual Property Rights (such as brand and mark of conformity), and where applicable suspending or withdrawing such rights;
f) training and qualifying experts to apply the Certification Scheme.

Except where part or all of the following competencies are reserved by law to a national authority, the Scheme Owner may also intervene by:

g) addressing and investigating complaints related to Europrivacy certifications;
h) overviewing Certification Bodies' compliance with the Certification Scheme;
i) facilitating collaboration and exchange of experience and information among licenced Certification Bodies;
j) suspending and/or withdrawing certification
   - granted by Certification Bodies that are not complying with the Certification Scheme; or
   - which have been obtained or used deceptively by beneficiaries; or
   - which are being used in a manner likely to bring the Certification Scheme into disrepute;
k) any other relevant actions that the Certification Scheme deem necessary and/or useful for the Certification Scheme.

While the Scheme Owner can intervene a posteriori to suspend, withdraw or invalidate a certification, it carries no responsibility for the process and decision to certify, which remains under the sole responsibility of the Certification Bodies. The Scheme Owner is neither responsible for any defaults or errors in certification processes (which are the responsibility of the Certification Bodies), nor for any non-compliance by the Applicants. Compliance with data protection regulations and the Certification Scheme is the sole responsibility of the certified Applicants. All Europrivacy Certification Scheme users shall accept that the Scheme Owner is not responsible for any default of licenced Certification Bodies, or any non-compliance by any certified Applicant.

The Scheme Owner may charge the Certification Bodies for the delivered services.

18.2. International Board of Experts

The Scheme Owner shall establish an International Board of Experts gathering experts in data protection, cybersecurity, and certification. This body shall support the Scheme Owner in:

a) reviewing, maintaining, and updating the Europrivacy Certification Scheme;
b) addressing questions transmitted by the Scheme Owner to this body;
c) serving as an impartiality mechanism whenever requested by the Scheme Owner.

18.3. Compliance with Specific GDPR Requirements for Certification

The Certification Scheme shall comply with the GDPR requirements, including the specific provisions regarding certification in Articles 42 and 43 GDPR.

18.3.1. Cooperation with the Data Protection Authorities

The Scheme Owner should inform and maintain close cooperation with the relevant Data Protection Authorities.

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

18.3.2. European Data Protection Board

The Scheme Owner shall consult and follow the decisions and guidance of the European Data Protection Board.

18.3.3. European Commission Acts

The European Commission may adopt acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals, and marks.

18.3.4. Responsibility

Certification does not reduce the responsibility of a Data Controller or a Data Processor for compliance with the applicable data protection regulations and is provided without prejudice to the tasks and powers of the competent Data Protection Authorities.

18.4. Improvement of the Certification Scheme Documents

18.4.1. Certification Scheme Improvement

The Scheme Owner shall lead a regular revision and improvement of the Certification Scheme with the support of an International Board of Experts.

The Certification Body shall establish procedures for revising and updating its evaluation methods *"in the course of changes in the legal framework, the relevant risk(s), the state of the art and the implementation costs of technical and organisational measures."* (EDPB)

18.4.2. Suggestions for Improvements

Certification Bodies and its audit team shall collect and communicate any relevant suggestions for improvement to the Scheme Owner. These suggestions may relate to the Scheme itself and/or to the detailed checks and controls. The Scheme Owner should collect and compile the suggestions received and select the most relevant ones to be discussed by the Europrivacy International Board of Experts and considered for the revision of the Certification Scheme.

18.4.3. Documents Revision or Addition

Whenever required, the Scheme Owner with the support of its International Board of Experts, can revise and adapt Certification Scheme related documents, and/or create new documents.

The Scheme Owner will communicate certification criteria updates to the competent Data Protection Authority, indicating whether it implies substantial changes to the certification criteria.

Revisions of the Europrivacy Certification Scheme are:

a) included into the Europrivacy Online Community and Resources website;
b) made available to the licensed and authorised relevant stakeholders.

When the Certification Scheme requirements are modified and may impact certified Applicants, the Certification Bodies shall communicate these changes to their Applicants and check that their certified data processing activities comply with these changes at their next surveillance audit.

18.4.4. Versioning

Any revised document should be released with an incremented version number.

18.4.5. History and Track Change Version

A version of the document with track changes applied from the previous version should be kept and made available by the editor. A summary of the main changes since the last version can be included in the first part of the document or in a separate document.

18.4.6. Reference Classification

The classification and identification of the official documentation of the Certification Scheme follow the guidelines specified in the document *"Management and Classification of Europrivacy Documents"*.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

18.5. Official Documents Release

18.5.1. Internal Peer Review

Normative documents, informative documents, and reports should be formally and internally peer-reviewed and checked before being formally approved and released.

18.5.2. Official Europrivacy Document Repository

All documents needed to apply the Certification Scheme (including new official versions of existing documents) are made available in the Europrivacy Community and Resources website: http://community.europrivacy.com.

18.5.3. Publication Effects

As soon as a document is updated and published in the Europrivacy Community and Resources website, it shall be considered as the reference document to be used, replacing any previous version.

Certification and audit processes shall use the latest available version of the Certification Scheme and related documents at the date the process starts. When new versions of documents are released during a Certification and audit process, it should take it into account and as far as possible comply with this new version, but it is acceptable to complete an ongoing process according to the official version at the time the audit process commenced.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

19. Certification Bodies Licensing and Accreditation

19.1. General Principles

The use of Europrivacy to deliver certifications is reserved to Certification Bodies that comply with the following requirements:

a) **The Certification Body shall be authorised by the Scheme Owner** to use the Europrivacy Certification Scheme and related resources through a written licensing agreement that clarifies the obligations of the Certification Body when using Europrivacy. The list of authorised Certification Bodies is maintained on the public website of Europrivacy.
b) **The Certification Body shall request and obtain a formal and adequate accreditation or agreement** in conformity with its applicable national regulations.
c) **The Certification Body shall comply with the Certification Scheme specifications and applicable national regulations**, and when delivering a certification under Art. 43 GDPR, with the relevant EDPB Guidelines.

The Certification Body shall apply the Certification Scheme as provided, without any adaptation, limitation or Extension that is not expressly foreseen and authorised by the Certification Scheme.

The accreditation of Certification Bodies for delivering data protection certifications is by default under the authority of its National Data Protection Authority and/or its National Accrediting Authority. The Scheme Owner is entitled to monitor, check, and control the licensing of Europrivacy.

Where applicable, the national regulations and mechanisms can complement, rectify, or replace the prescriptions mentioned in this Section.

19.1.1. Relationship with the Accreditation and Data Protection Authorities

Under Art. 43 of the GDPR, accredited Certification Bodies of the European Union are under the control of their national Data Protection Authority and/or Accreditation Authority. Where such authorities are in charge of monitoring and controlling the work of the Certification Body, the Scheme Owner will respect, support, and collaborate with the competent authority.

19.2. Licensing Procedure

The licensing procedure intends to build trust in Europrivacy certifications by ensuring that only qualified and reliable service providers are authorised to use Europrivacy for delivering services to other companies. The licensing process reduces the risk of inappropriate use of Europrivacy and/or deliverance of unreliable certifications.

The Scheme Owner shall define, maintain, and update the procedure, policy, and set of requirements for companies interested in being authorised to perform and deliver Europrivacy certifications.

Interested companies can apply for a Europrivacy license by submitting an application with a detailed presentation file presenting their experience in certification processes and personal data regulation. The list of requirements for the initial application is provided on demand by the Scheme Owner. The applying company shall commit to comply with the procedure and cover the licensing-related costs and fees.

By default, the application procedure shall follow a two stages process. However, European National Authorities wishing to use the Certification Scheme to deliver certifications can request free licensing from the Scheme Owner through a simplified procedure.

19.2.1. First Stage Process – Eligibility Assessment and Licensing

At the first stage, the Scheme Owner shall perform an initial evaluation of the applications received according to a procedure and requirements adopted by the Scheme Owner. It shall assess elements that may have an impact on the reputation, development, impartiality, quality and reliability of the intended certification activities, such as:

a) capacity to deliver high quality services to a large number of Applicants;
b) track record and experience of the applying company in certification;

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

c) qualification of the personnel of the applying company, including expertise in data protection law, cybersecurity, and certification;
d) location and regulatory environment, and business practices that may impact the impartiality, independence and reliability of the certification process;
e) quality and ambition of the strategy for delivering Europrivacy related services.

In order to assess the risk on impartiality, independence and reliability of the certification processes, the Scheme Owner may use indicators related to the respect of the state of law, the level of corruption and the freedom of press and information in the country where the applying company's headquarters are located. Adequacy decisions under Chapter V of the GDPR will be taken into account.

The Scheme Owner may also take into account other parameters, such as reputation and trust, long term sustainability of the Certification Scheme, market structure and demand.

If the applying company appears to comply with the criteria, the Scheme Owner will:
a) organise a meeting with the applying company;
b) decide if the applying company is eligible to become an official partner;
c) if the decision is positive, provide the applying company with the formal licensing agreement to be signed.

19.2.2. Second Stage – Readiness and Accreditation

The second stage of the licensing procedure requires the Certification Body to:
a) sign the licensing agreement;
b) complete its readiness process (training of its experts, development of a webpage, etc.);
c) request a formal accreditation or agreement from a national authority.

19.2.3. Duty of Licensed Certification Bodies

Licensed Certification Bodies shall:
a) comply with the Certification Scheme rules and requirements and ensure that certified Targets of Evaluation comply with the applicable Europrivacy Criteria;
b) work in close cooperation with the Scheme Owner, and where applicable with their National Data Protection Authority and/or Accrediting Authority;
c) report and provide transparent information on their certification activities;
d) monitor on a yearly basis the continuous compliance of active certifications with the Certification Scheme requirements;
e) promote the Certification Scheme and contribute to its positive reputation;
f) submit suggestions to the Scheme Owner for improving the Certification Scheme, including its Criteria, checks and controls.

19.2.4. Monitoring Licensed Certification Bodies

The monitoring of licensed Certification Bodies can take several forms, such as:
a) reviewing certification documentation (including records and findings);
b) providing Observers or Embedded Auditors for audits performed by the Certification Body;
c) requesting qualifications from the Auditors;
d) any other action or process deemed necessary by the Scheme Owner.

Certification Bodies shall fully cooperate and provide without undue delay the information and documentation requested as applicable by their National Data Protection Authority, their Accrediting Authority, or by the Scheme Owner.

19.2.5. License Duration

The Scheme Owner is encouraged to monitor and review its licensing agreements on a yearly basis and can decide to suspend or end the licensing agreement if a Partner or a Certification Body does not meet the requirements.

19.2.6. License Expiration

Where a license granted to a Certification Body expires or is ended, it has no retroactive effect on certifications already granted by that Certification Body, except where there is reason for the Data Protection Authority or for the Scheme Owner to consider such certifications unreliable. In such cases, a Certificate may

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

be suspended until it is reviewed and validated by another licenced Certification Body. The Data Protection Authority, the Accrediting Authority and/or the Scheme Owner may suggest a replacement Certification Body to the Applicant.

19.3. Accreditation or Agreement Procedure

In order for a certification to be valid under the GDPR or other national data protection regulations, the Certification Body shall have received a formal accreditation or agreement delivered by a competent national authority.

Accreditations delivered under Art. 43 GDPR shall be based on ISO/IEC 17065.

19.3.1. Accreditation Requirements

Accreditation requires a formal evaluation of the Certification Body ability to comply with and apply the Certification Scheme. It requires to assess, inter alia:

a) The required expertise and experience of the applying Certification Body, including:
   - ISO related expertise and experience;
   - Data protection related expertise and experience.

b) The conformity with the infrastructure and procedures requirements, including:
   - Applicable ISO and Europrivacy related requirements;
   - Data protection related requirements.

c) The Human Resources ability, skills, and qualifications, including the availability of qualified auditors with adequate knowledge and expertise in:
   - ISO certification processes;
   - GDPR and applicable data protection regulations;
   - Cybersecurity;
   - Europrivacy Certification Scheme criteria, rules and procedures.

The Certification Scheme rules and procedures are deemed to be detailed and comprehensive enough so that the Certification Body does not need to demonstrate compliance with ISO/IEC 17020 and 17025.

The Certification rules and procedures are homogeneous and remain the same, regardless of the industry sector and level of complexity of the Data Processing. As a consequence, deliverance of accreditation does not require to be industry specific.

Accreditation may be subject to complementary national requirements.

The Scheme Owner may specify complementary guidance for the accreditation procedure.

19.4. Process for Suspension and Withdrawal

The prime objective of any certification is to ensure that the public can develop trust in certified Targets of Evaluation. When this trust is jeopardised, licenses and certificates can be suspended or withdrawn.

19.4.1. Suspension and Withdrawal of Accreditations and Licenses

The National Data Protection Authority and/or the Accrediting Authority are competent to suspend or withdraw the accreditation of a Certification Body. Similarly, in case of major non-compliance or repeated minor non-compliances with the Certification Scheme, the Scheme Owner may suspend or withdraw the license granted to a non-complying Certification Body.

19.4.2. Suspension and Withdrawal of Delivered Certifications

The above-mentioned authorities can also suspend or withdraw certifications granted by a Certification Body in any situation that would put the certification at risk of disrepute or misleading the public. Examples of situations that may lead to suspension or withdrawal of certificates include:

a) the Certification Body appears to have disrespected or ignored obligations and requirements specified in the Certification Scheme;
b) a beneficiary of the certification appears not to comply with the Certification Scheme;

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

c) a beneficiary of the certification appears to have concealed information related to its data protection policy and practice;
d) the existence or use of a certificate that may mislead the public about compliance of certified data processing with data protection regulations.

19.4.3. Suspension and Withdrawal Decision Process

Suspension of a license or a delivered certificate may be implemented immediately if justified to protect the public and/or the reputation of the Certification Scheme. The decision-making body shall take reasonable steps to expeditiously inform the beneficiary of reasons for the suspension and to enable the beneficiary to provide clarifications and/or propose a set of corrective measures.

By default, withdrawal of a license or a delivered certificate shall be implemented only after the beneficiary has had a reasonable time to provide clarifications and/or propose a set of corrective measures. Beneficiaries potentially subject to withdrawal will have at least a 30-day period to present clarification/corrective measures before the qualified body makes a decision on whether to withdraw certification. The 30-day period runs from the point that the decision body communicates notice of the commencement of the withdrawal process to the targeted beneficiary.

When making decisions to suspend or withdraw certification, the decision body shall take into account the principle of proportionality, as well as the importance of maintaining public confidence in the Certification Scheme's reliability and trustworthiness.

All Certification Bodies and Applicants shall agree to comply with and accept the decisions of the Data Protection Authority, the Accrediting Authority and/or the Scheme Owner and agree to waive any entitlement to compensation related to decisions concerning the grant, suspension, or withdrawal of certification or licence to the extent permitted by law.

Europrivacy – http://www.europrivacy.com All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Annex 1 – Summary Table of Applicable Criteria

The following table summarises the applicability of the Europrivacy Criteria according to the location and activity of the Applicant.

		Applicant in the EEA		Applicant outside the EEA		
		Subject to the GDPR according to Art. 3 GDPR			NOT Subject to the GDPR under Art. 3 GDPR	
		Not exporting data	**Data Exporter**	**Data Controller subject to the GDPR**	**Data Importer only**	**Data Importer with onward transfers**
		Art. 42 and 3(1) GDPR	Art. 42 and 3(1) GDPR	Art. 42 and 3(2) GDPR	Art. 46 and 42 GDPR	Art. 46 and 42 GDPR
Criteria	**G.1**	YES	YES	YES	YES, except for G.1.1.3, G.1.1.4	YES, except for G.1.1.3, G.1.1.4
	G.2	YES	YES	YES	YES, except for G.2.2.1	YES, except for G.2.2.1
	G.3	YES	YES	YES	YES, except for G.3.2.1, G.3.2.2, G.3.2.3	YES, except for G.3.2.1, G.3.2.2, G.3.2.3
	G.4	YES	YES	YES	YES, except for G.4.1.4	YES, except for G.4.1.4
	G.5	YES	YES	YES	YES	YES
	G.6	YES	YES	YES	YES	YES
	G.7	YES	YES	YES	YES, except for G.7.1.2, G.7.1.3 and G.7.1.4	YES, except for G.7.1.2, G.7.1.3 and G.7.1.4
	G.8	YES	YES	YES	NO	NO
	G.9	YES	YES	YES	YES, except for G.9.1.3	YES, except for G.9.1.3
	G.10.1	NO	YES	YES	NO	NO
	G.10.2	NO	NO	NO	YES	YES
	G.10.3	NO	NO	NO	NO	YES
	T Criteria	YES	YES	YES	YES	YES
	C Criteria	YES	YES	YES	NO	NO
	S Criteria	YES	YES	YES	YES	YES

 All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.