Europrivacy.com
Privacy Audit and Certification

Europrivacy™/®
Main Changes in Version 77 of the Certification Scheme General Specification and Requirements

Identifier:	EP-CS.MC.V77
Version:	1
Date:	8 March 2024
Publication status:	**Confidential**
Websites:	www.europrivacy.com
	www.eccpcentre.com
Contact:	admin@europrivacy.com

Table of Contents

Introduction

The "*Europrivacy Scheme General Specification and Requirements*" (hereafter referred to as the "Certification Scheme") specifies the applicable rules and methodology for implementing Europrivacy certification. The present document explains what the main changes from the previous version 68 to the new version 77 are.

The new version 77 addresses the comments received from partners, users, and accreditation authorities. It is available in the **Europrivacy Resources and Community Website** and is applicable to all Europrivacy certification delivered after March 1st 2024, provided that no more recent version has been released.

Europrivacy Resources and Tools

The Applicants, Implementers, and Auditors can leverage several resources and tools to prepare and support Europrivacy certifications, including:

1. The **Europrivacy public website** provides general information and guidance on the certification process. It also provides tools such as a cost-saving estimator with GDPR certified compliance. www.europrivacy.com
2. The **Europrivacy Online Academy** provides online courses on the Europrivacy certification scheme, including an introductory course for Data Protection Officers. https://academy.europrivacy.com
3. The **Europrivacy Resources and Community Website** provides a whole set of online resources and documents to facilitate both the pre-certification and certification processes, as well as to support the continuous enhancement of data protection compliance. The use of the community website is not mandatory, but it can facilitate the process and save time for the Applicant. https://community.europrivacy.com

Europrivacy Useful Documents

It is recommended to use and refer to the following useful documents:

- EP-G.INTRO – Europrivacy Introduction and Overview
- EP-G.AP – Europrivacy Guidelines for Applicants to Certification
- EP-CS.1 – Europrivacy Certification Scheme General Specification and Requirements
- EP-C.ALL – Europrivacy List of Criteria, Checks and Controls
- EP-P.TC – Europrivacy General Terms and Conditions

General Adaptations

Reorganisation of the structure of the Certification Scheme

The sections of the Europrivacy Certification Scheme General Specifications and Requirements have been reorganised in four parts to increase user-friendliness:

- 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.

This enables DPOs and implementers to focus on the two first parts of the document and ignore the rest of it.

Simplifying and enhancing the wording

A comprehensive review of the text has been performed to enhance the wording, by removing unnecessary details and enhancing the clarity of the content.

Removing overlapping specifications

The previous version contained a certain number of overlapping specifications, addressing the same topic from different sections. The new version has done effort to remove overlapping specifications.

Dissociation of Data Protection Management Systems

It was decided to focus the core Certification Scheme on ISO/IEC 17065 certification process and to move the reference to the extendibility of the Certification Scheme to Data Protection Management Systems (and associated references to ISO/IEC 17021-1) into a distinct and separate document.

Clarifying the Applicability of the Certification outside of Europe

The new version includes complementary provisions to pave the way for certifications outside of the European Union (EU) and European Economic Area (EEA). The applicability of the Certification Scheme outside of EEA is subject to an ongoing review and expected validation by EDPB.

Section-Specific Adaptations

Scope of Certification and Target of Evaluation

The new sub-section 2.2.3 clarifies the Geographic Scope of Certification and its applicability of the Certification criteria beyond the European Union (subject to EDPB approbation).

"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.*

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."*

Restrictions to Unregulated Certification

The new sub-section 2.5.3 restricts the use of Europrivacy Certification Scheme and Criteria for unregulated certifications. It stresses the obligation to avoid any risk of confusion, including the need to use a different name and mark of conformity, and to comply with applicable legislation and intellectual property rights. It also clarifies that certification delivered outside of the GDPR requirements is not recognised by EU jurisdictions.

Expansion of Definitions

New section 4 includes new and revised definitions of the terms: Adaptation, Auditee, Examination, Extension, Inspection, Test and Testing, Data Exporter, Data Importer, Data Protection Authority.

An important element is the definition of the concept of "**Examination**", which 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 visual observations and questions asked to stakeholders involved in the data processing.

In order to avoid any confusion with the ISO acceptance of the term "inspection" which is subject to specific rules under ISO, the Certification Scheme has replaced the term "inspection" by the term "Examination". Under the new version, reference to "inspection" (for instance in the suggested means of verification of the criteria) shall be understood as referring to "Examination".

"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.

Criteria, Checks, and Controls

The new section 6.2 includes a new dimension attached to the criteria in order to differentiate criteria that are applicable to Applicants acting as Data Importer located outside of the EEA:

"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 transfer7, 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."*

NOCAR

The sub-section 6.2.2. clarifies that the NOCAR is required by Applicants based in the EEA. Applicants based outside of the EEA do not need to prepare a NOCAR.

Testing Procedure

The new section 8.3 clarifies that: *"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."

Sampling

The new sub-section 8.3.1 clarifies that: *"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." It also includes a reference to an online calculators Sample Size Calculator – Qualtrics: https://www.qualtrics.com/blog/calculating-sample-size/.

Examination Principles

The new section 8.4.1 clarifies that *"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."*

Multi-site Assessments

New section 8.4.6 further details the applicable rules to multi-site assessment.

Suggested Means of Evaluation

New section 8.6.1 provides more details on the assessment process, including the suggested means of evaluation. In particular:

"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

Handling of Minor Non-Conformities

The new sections 8.6.5, 8.6.6 and 8.6.7 further detail the applicable rules in case of minor non-conformities.

"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."

Delivering Certification without or before Accreditation

New section 9.3 clarifies the applicable rules to certification delivered before or without accreditation. It sets limits and reminds the fundamental requirement to avoid any risk of confusion with regulated certifications.

Transfer of Certificates

New section 9.4 clarifies the rules for transfers of certifications to another certification body. The **Certification Body** that takes the token shall comply with and perform the planned surveillance audits.

Clarification of Europrivacy Extensions and Adaptations

New Section 11 clarifies the notions of:

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

It clarifies the implications of such Extensions and Adaptations in terms of audit time and effort adaptation, and impact on marks of conformity.

Additional Statement for Applicants Acting as Data Importers

In view of the increasing importance of ensuring data protection in data transfers, a new section has been introduced (section 15.6.10) to ensure that Data Importers that are based in third countries not benefitting from an adequacy decision and Certification Bodies duly examine the **applicable legislation and practices to determine whether the obligations under the Europrivacy Certification can be met.**

Certification Bodies Licensing and Accreditation

The new section 19 provides a revised specification of the process and rules applicable to licensing and accreditation procedure of certification bodies. It includes:

General Principles

The new section 19.1 specifies the general requirements for Certification Bodies, including that: *"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."

Licensing Procedure

The new section 19.2 further details the licensing procedure. It also clarifies the license duration and specifies that *"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."*

Accreditation or Agreement Procedure

The new section 19.3 clarifies that *"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."***
It also clarifies that: *"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."*

Annex 1 – Summary Table of Applicable Criteria

The new version includes a new Annex with a table that summarises the applicability of the Europrivacy Criteria according to the location and activity of the Applicant.

