



EuroprivacyTM Academy
GDPR Audit and Certification Courses

Europrivacy Academy

Europrivacy Introductory Course



www.academy.europrivacy.com

Europrivacy Academy

Europrivacy Introductory Course

v.3 of 2024



About Europrivacy

Europrivacy is a certification scheme developed to assess and certify the conformity of data processing with the European General Data Protection Regulation (GDPR) and complementary national regulations. It received endorsement from the European Data Protection Board (EDPB) as the European Data Protection Seal applicable in all EU jurisdictions.

Europrivacy enables a reliable and systematic conformity assessment that is compliant with ISO principles. It is easily extensible to complementary regulations and emerging technologies. It provides an efficient methodology to perform internal audits, to identify residual Non-Conformities, and to prepare data processing for certification. It can be used by Data Protection Officers, internal auditors, consultants, and certification bodies.

Europrivacy is maintained and supervised by the Europrivacy International Board of Experts in data protection to keep it updated following the evolution of the jurisprudence on personal data protection, including EDPB publications. Europrivacy is administratively managed by the European Centre for Certification and Privacy (ECCP) in Luxembourg and is applied by qualified Certification Bodies, as well as law firms and consulting firms to support their clients in complying with the data protection regulations.

About the Europrivacy Academy

The Europrivacy Academy provides training courses to those interested in obtaining an official qualification as Europrivacy experts. The Europrivacy Academy focuses on the Europrivacy Certification Scheme methodology and rules. It is assumed that students are already familiar with data protection regulations. Courses of the Europrivacy Academy offer a customised learning experience to a wide variety of interested professionals.

About the Handbook

The Europrivacy Academy – Europrivacy Introductory Course Handbook is a complementary document provided to participants of the Europrivacy Introductory Course on the Europrivacy Academy. This short Handbook is intended to provide a complementary support and summary of the certification process together with the main definitions. As passing the exam is necessary to obtain a certificate of expertise, the Handbook provides a mock exam that can familiarise students with the type of the final exam and questions they must prepare for.

Introduction

The Europrivacy Certification Scheme specifies a clear and efficient methodology to assess and formally certify the conformity of data processing activities with the General Data Protection Regulation (GDPR) and other complementary national and/or domain-specific obligations. It applies to a large scope of data processing activities, from processes and services to data protection management systems.

The present Handbook provides a short overview of the certification process, the main definitions, and most important concepts. This Handbook also includes a section to prepare candidates for their exam on the Europrivacy Academy. The mock exam includes 10 questions that are based on the content of the four modules. With the answer sheet attached, students can check whether they are prepared to take the exam.

All references to any document must be understood as a reference to its latest version. When a new version of a document is released, it replaces all previous versions of the same document at the date of the publication or at the end of the transition period. Certification and audit processes must use the latest available version of the Europrivacy Certification Scheme and related documents at the date the process starts. When new versions of documents are released during a certification and audit process, the certification procedure should take it into account and as far as possible comply with this new version. Nevertheless, an ongoing process can be completed according to the official version of the time it commenced.

In case of any doubt relating to the application and/or interpretation of the Certification Scheme requirements, the latest version of the Certification Scheme is the document to refer to.

The Certification Scheme specific normative and informative documents remain under the control of the Scheme Owner assisted by its International Board of Experts.

Europrivacy experts are responsible for obtaining the latest version of the utilised documents through the Europrivacy Community website. Documents provided through the Europrivacy Academy are strictly for training purposes and do not constitute an official material for carrying out certification activities.

Table of contents

About Europrivacy	3
About the Europrivacy Academy	3
About the Handbook.....	3
Introduction	4
Introduction to Europrivacy	6
Europrivacy value proposition.....	6
Europrivacy characteristics.....	7
The Europrivacy Certification Scheme.....	8
Key definitions.....	8
The Europrivacy certification process	10
Europrivacy certification process	10
Evaluation criteria	11
Specifying the Target of Evaluation.....	11
Non-Conformities.....	11
Europrivacy resources and tools.....	13
Useful websites.....	13
Other useful documents	13
Exam preparation	14
Example.....	14
Mock exam	16
Answers.....	18

Introduction to Europrivacy

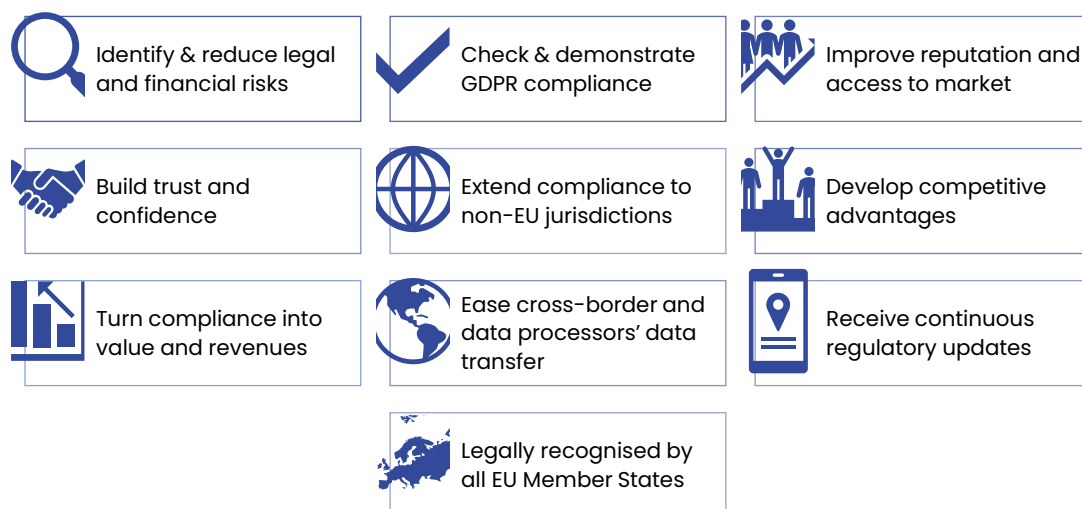
Personal data protection is considered a fundamental right in Europe. With the adoption of the European General Data Protection Regulation, data subjects' rights can no longer be ignored. Companies collecting personal data in the European Union without complying with these rules are exposed to substantial fines regardless of their location. However, beyond the legal, financial, and reputational risks, the GDPR also presents an opportunity for companies to become certified and demonstrate their respect for data subject rights.

Europrivacy has been developed to deliver highly reliable and efficient GDPR compliance certification. It enhances end-user trust through independent third-party evaluations of compliance, leveraging the expertise of impartial and qualified auditors to assure the protection of data subject rights. Additionally, certification promotes trust in the European digital single market, where the protection of personal data is a priority.

In October 2022, **the Europrivacy Certification Scheme and its criteria received a formal recognition by the EDPB as the first EU-wide GDPR certification.** As an **official European Data Protection Seal**, Europrivacy is **formally recognised by all EU jurisdictions.** This means that certificates delivered under Article 42 of the GDPR by Certification Bodies authorised under Article 46 of the GDPR will be recognised in all EU jurisdictions as well.

Europrivacy encompasses the European General Data Protection Regulation and can easily be extended to include complementary national and domain-specific obligations. It has been designed to be comprehensive and capable of assessing a wide range of data processing activities by complementing its list of core criteria with complementary checks and controls according to the Target of Evaluation. Europrivacy can be used to evaluate the conformity of data processing activities carried out in diverse contexts, such as online services, hospitality industries, the health sector, and smart cities. Furthermore, it benefits from the expertise of top European experts in information and communication technologies to address risks related to disruptive technologies, such as Internet of Things, Artificial Intelligence, and Big Data.

Europrivacy value proposition



Europrivacy characteristics



The Official **European Data Protection Seal** under GDPR (Art. 42)



Continuously updated to align with evolution of regulations, jurisprudence



Extensible to complementary national obligations



Applicable to **emerging technologies**



Highly reliable with systematic assessments



Time- and cost-efficient thanks to its innovative methodology



ISO compliant and easily combinable with ISO 27001 and 27701



Comprehensive and applicable to almost any data processing activities



Independent and managed by the International Board of Experts



Online **resources, tools, and support**



Global ecosystem of qualified partners and experts



Research and Innovation empowered

The Europrivacy Certification Scheme

Europrivacy has been designed to provide a clear and comprehensive certification scheme on compliance of data processing with personal data protection regulations. It provides an independent, impartial, and reasonable assurance level of data processing compliance with the GDPR and the corresponding data subjects' fundamental rights, as well as with complementary requirements.

The Europrivacy Certification Scheme is applicable to diverse data processing activities performed by data controllers and/or data processors. Its architecture enables to easily extend its core criteria to complementary national and domain-specific requirements.

As data protection regulations are evolving, the Certification Scheme is regularly updated to consider the evolution of the legal environment and jurisprudence related to data protection. It is also intended to enable continuous improvement. The Scheme Owner, supported by the International Board of Experts, is in charge of reviewing and updating the Certification Scheme.

A certification process is based on the findings identified by an auditor after following a clearly specified and systematic methodology. A certificate is an official 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** that must continuously ensure that its certified Target of Evaluation complies fully with the requirements of the Certification Scheme and the applicable data protection regulations. **To be certified, a data processing activity must comply with the latest version of the Europrivacy Certification Scheme requirements and criteria, as well as with the applicable data protection regulations.**

Key definitions

Applicant refers to the client of a Certification Body applying for certification or taking part in a certification process.

A **certificate** is a statement of conformity.

Certification is the assessment and impartial third-party attestation that the certification criteria has been fulfilled.

The **Certification Body** is a third-party conformity assessment body operating a certification mechanism. Certification Bodies are authorised to use Europrivacy to deliver a certificate of compliance.

A **Check and Control** is a formal requirement against which the Target of Evaluation is assessed.

Criteria or **Certification Criteria** are the criteria against which certification is performed.



A **Data Controller** is the natural or legal person, public authority, or other body that determines the purposes and means of processing personal data.

A **Data Processor** is an entity processing data on behalf of a data controller or another data processor.

A **Data Subject** is any identified or identifiable natural person whose data are processed.

Data protection regulations refer to both European and complementary applicable national regulations.

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

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

Non-Conformity refers to the failure to comply with one or several applicable data protection requirements.

Target of Evaluation (ToE) refers to the data processing to be assessed and certified.

The Europrivacy certification process

Europrivacy certification process

The Applicant must document the compliance of its selected data processing activities before applying for certification at the selected Certification Body. The documentation process can be done by the Applicant in a do-it-yourself way, or they can commission a qualified Consulting or Law Firm to support through the process. Implementers can support Applicants in remediating potential gaps and shortening the certification process, reducing associated costs.

The following table summarises the key steps of the Europrivacy certification process:

	STAGE	LEAD	OBJECTIVES	RESOURCES
1	Documentation of compliance	Applicant	Document compliance with the applicable data protection regulations	Guidelines for Applicant; Templates, checklists, criteria
2	Application	Applicant	Specify the Target of Evaluation and fill in the Application Form	Europrivacy Application Form template
3	Application review	Certification Body	Verify the application and the ToE	A – Application & ToE Checklist
4	Offer and agreement	Certification Body	Prepare an offer, sign agreement and terms & conditions	Europrivacy General Terms and Conditions
5	Assessment Plan	Certification Body	Prepare Certification Plan	Europrivacy Certification Plan template
6	Documentation Preparation	Applicant	Gather and complete documentation	Guidelines for Applicant D – Documentation checklist
7	Documentation review	Auditor	Verify documentation	D – Documentation checklist
8	Compliance assessment	Auditor	Assess the compliance of ToE	Europrivacy criteria
9	Initial reporting	Auditor	Write an initial assessment report with the list of Non-Conformities	Europrivacy Assessment Report template
10	Remediation	Applicant	Address and resolve identified Non-Conformities	List of non-conformities
11	Final report	Auditor	Validate the resolution of Non-Conformities, update the assessment report	Europrivacy template of assessment report
12	Review	Certification Body	Review the assessment report, make recommendation for certification	NA
13	Certification decision	Certification Body	Make certification decision	Z – Europrivacy checklist for certificate publication
14	Certificate publication	Certification Body	Communicate the decision and publish the certificate	Europrivacy Registry of Certificates
15	Compliance maintenance	Applicant	Maintain and enhance compliance	Europrivacy Community website
16	Surveillance/recertification	Auditor	Assess compliance of the ToE	Europrivacy criteria

Evaluation criteria

The evaluation criteria are applied in compliance with the latest version of the Europrivacy Certification Scheme requirements. The list of criteria, checks and controls is used by the Certification Bodies to systematically assess the compliance of the data processing in the Target of Evaluation. Each applicable criteria, check and control must be sufficiently completed and documented with adequate evidence to assess the conformity to the requirement.

Beyond the core GDPR obligations, Targets of Evaluation may be subject to complementary national or domain-specific regulations. Consequently, the Europrivacy core requirements are complemented by contextual requirements to consider the applicable national regulations and the specificities of the data processing.

Specifying the Target of Evaluation

A reliable and meaningful assessment of conformity can only take place when the Target of Evaluation is described precisely. The Target of Evaluation is described clearly including the processing operations. Examples of Target of Evaluation include but are not limited to public websites, smart phone applications, human resources, newsletters, customer database.

The description of the Target of Evaluation:

1. Be named with a clear title.
2. Describes the data processing.
3. Illustrates the data flows in a diagram or drawing, including the identification of data flows with external data processing.
4. Identifies the data types processed.
5. Identifies and describes all data processing operations and systems pertaining to the Target of Evaluation.
6. Indicates where the data processing starts and ends.
7. Where applicable, identifies and describes the interfaces of the data processing with independent processing operation.
8. Specifies the protocols used and other relevant assurance measures.

Non-Conformities

If one or more Non-Conformities have arisen during the certification audit, the Certification Body must require the Applicant to analyse the cause and describe the specific correction and corrective actions to eliminate these Non-Conformities. Each Non-Conformity must be qualified as either minor or major non-conformity.

A **Major Non-Conformity** is a Non-Conformity that 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. Any Non-Conformity where the Applicant breaches its legal obligations as specified in the GDPR constitutes a Major Non-Conformity.



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

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 status is qualified as “**Observation**”.

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

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

Europrivacy resources and tools

To complete the Europrivacy Introductory Course, there is no need for additional resources apart from the four Modules. Nevertheless, additionally to the present Handbook, there are other useful resources available through the different platforms.

Useful websites

- Europrivacy website: <https://europrivacy.com/>
- Europrivacy Community: <https://community.europrivacy.com/>
- Europrivacy Registry of Certificates:
<https://www.europrivacy.com/en/resource/registry>
- Privacy Pact: <https://privacypact.com/>

Other useful documents

The following documents are used by both consulting firms and Certification Bodies. While some of these documents are already made available through the Europrivacy Implementation Course and the Europrivacy Assessment Course, others can be downloaded through the Europrivacy Community website after subscription.

- Europrivacy Certification Scheme General Specification and Requirements
- Europrivacy Certification Introduction and Overview
- Europrivacy Certification Process Overview
- Europrivacy General Terms and Conditions
- Europrivacy Guidelines for Applicant
- Europrivacy Certification Application Form
- Europrivacy Guidelines on Specifying the Target of Evaluation
- Data Protection Officer Statement Template
- Europrivacy detailed list of criteria, checks and controls
 - A – Application & ToE Checklist
 - D – Documentation Checklist
 - G – GDPR Core Criteria
 - C – Complementary Contextual checks and controls
 - T – Technical & Organisational checks and controls
 - P – Policy and Procedure Checklist
 - DPO's statement template
 - NOCAR template

Exam preparation

To obtain an official certificate and become an expert who understands the fundamentals of how Europrivacy Certification Scheme works, participants of the Europrivacy Academy must successfully pass a final exam. This section of the Handbook is intended to prepare and familiarise you with the type of exam.

The exam consists of multiple-choice questions (20 for the Introductory Course) that must be finished within the given time (30 minutes). Each question has 4 possible answers. Sometimes only one answer is correct while for some questions there are multiple correct answers. During the exam, you will be given a hint whether you need to concentrate on finding a single or multiple answers. For more information, you can refer to the [Final Exam Disclaimer](#) on the Course's page.

The mock-exam in this Handbook consists of 10 questions and it is advised to be completed within 15 minutes. Just as in the real exam, each question has 4 possible answers. Answering a question correctly will give you a point. Some questions have multiple correct answers. The scoring is the following:

- 1 point when answering a question correctly;
- 0 point for missing a correct answer from a multiple correct answer question;
- 0 point for making an incorrect answer, regardless of whether the right answer(s) were marked.

To pass the mock-exam, you need to score 6 points out of 10. The answer-sheet is available at the end of the section.

Example

QUESTION		A	B	C	D
15	Which of the following is NOT a key principle of Europrivacy certifications?	Independence	Fair presentation	Favouritism	Confidentiality
16	Which of the following are considered a Europrivacy Complementary Normative Documents?	Europrivacy Guidelines for NOCAR completion	Europrivacy Communication and Marketing Rules	Guidelines on Accountability and Openness	Europrivacy Guidelines on the Use Criteria, Checks and Controls
17	Which of the following provides definitions for the Europrivacy Certification Scheme?	GDPR and EDPB Guidelines	Oxford Dictionary	Other relevant normative sources, such as ISO	Wikipedia

In this scenario, the student picked the following answers (indicated in orange):

- Question 15: C
- Question 16: D
- Question 17: A, B and C

The answer sheet indicates the following correct answers:

Question number	Correct answer
15	C
16	B D
17	A C



This means the following:

- The answer to Question 15 is correct, the student receives a point.
- The answer to Question 16 is partial, it misses Answer B. The student does not receive a point.
- In Question 17, answers A and C are correct. However, the student also chose answer B that is incorrect, meaning they will not receive a point for the whole question.

Explanation

With the correct answers, it is indicated which part of the modules the question refers to. In case of uncertainty, please study these points carefully.

Mock exam

QUESTION		A	B	C	D
1	Which of the following statements apply to the geographic scope of the certification?	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	Certification is only valid in countries that have a tropical climate	The geographic scope of certification depends on the availability of fast-food chains in the region	The recognition of certificates is subject to complementary requirements where the Target of Evaluation processes personal data outside the EEA
2	When is a Major Non-Conformity considered resolved and closed?	The Applicant's top management accepted the existence of the Major Non-Conformity in writing	The Certification Body must have reviewed, accepted and verified the correction and corrective actions	The Scheme Owner accepted the Applicant's plan for correction and corrective actions to be validated	The Consulting firm must have reviewed, accepted and verified the Certification Body's conclusion
3	What are the characteristics of Europrivacy?	That Data Protection Authorities certify the Applicants on the behalf of the Scheme Owner	That all audit processes are performed on-site	That it is an independent certification scheme managed by an international board of experts	That it is extensible to complementary national obligations
4	What is the benefit of the Europrivacy Community website?	It gathers a set of resources and tools to support Applicants and other Europrivacy partners in preparing and delivering certifications	It enables the Scheme Owner to authenticate all Europrivacy certifications	It enables companies to express their commitment to respect and abide by the GDPR	It provides training opportunities for Data Protection Authorities
5	Which of the following is NOT a feature of certification?	Limiting the validity of a certificate to a period of three years	Providing a transparent certification process	Allowing the certified parties to impose new taxes on data subjects	Allowing for the certification renewal if relevant conditions and requirements are met
6	What is the main objective of the preliminary certification phase?	To identify potential gaps and residual Non-Conformities	To certify data protection compliance	To validate the continuous compliance of the certified Applicant	To enhance communication between the Scheme Owner and the Applicant
7	Through which of the following websites can companies commit to respect and abide by the GDPR rules and principles?	The Europrivacy Community website	The Data Processing ID website	The Privacy Pact website	The Europrivacy Registry of Certificates
8	Which of the following are considered main external normative references?	ISO/IEC 17021-1, Conformity assessment – Requirements for bodies providing audit	Management of Competencies of Personnel Involved in Europrivacy Certifications	Europrivacy Communication and Marketing Rules	Europrivacy Certification Scope Limitations

		and certification of management systems			
9	Which of the following statements apply to the Welcome Pack?	It is a starter pack for Applicants interested in certifying their data processing activities with Europrivacy	It enables the authentication of Europrivacy certificates	It provides Europrivacy Flash Alerts of regulatory changes	None of the answers is correct
10	What does the principle of evidence-based approach mean?	Audit findings and conclusions must be based on facts and evidence, in line with the Europrivacy Certification Scheme evaluation criteria	Certification Bodies must provide public access to information about their certification process on their website and about the delivered certifications on the Europrivacy registry of certificates	Auditors must always bear in mind that the Europrivacy Certification Scheme has been designed to build trust and confidence	The Certification Body and the Scheme Owner must adopt procedures and implement an effective policy for protecting the confidentiality of the information acquired in relation to the certification process

Answers

Question number	Correct answer	Explanation
1	A D	Module 2 – Purpose and scope of Europrivacy certifications (slide 5) The geographic scope of the Certification Scheme is not formally limited but there are certain restrictions (Answers A and D). Answers B and C are incorrect and are not factored in certifications.
2	B	Module 3 – Non-Conformities (slide 12) The <i>Certification Body</i> is responsible for reviewing, accepting, and verifying correction and corrective actions. The Applicant, the Scheme Owner, or the Consulting or Law Firm do not participate in the evaluation of Non-Conformities. Consulting and law firms, however, can support their Applicants in defining the correction and corrective actions to be implemented.
3	C D	Module 1 – Europrivacy characteristics (slide 12) There are several benefits to Europrivacy certification. Regarding Answer A, Data Protection Authorities are <i>not responsible</i> for certifying compliance on behalf of the Scheme Owner, this is the task of the Certification Body. Similarly, contrary to Answer B, audit processes <i>can</i> be performed <i>off-site</i> as well.
4	A	Module 4 – Europrivacy Community & resources (slide 5) The purpose of the Europrivacy Community site is to provide a set of references for DPOs, Implementers, and Auditors to be used throughout the certification process and beyond.
5	C	Module 2 – Alignment with European data protection regulations (slide 6) Article 42 of the GDPR provides a series of features that certification must entail to be GDPR compliant, including limited validity (3 years), transparency of the certification process, and renewal. Taxation is not part of the list.
6	A	Module 1 – From risk mitigation to data protection excellence (slide 18) Identification of potential gaps and residual non-conformities should happen before the certification process starts. <i>Answer B</i> is part of the core certification process, while <i>Answer C</i> happens during the maintenance step.
7	C	Module 4 – Privacy Pact (slide 8) Companies can commit to respect and abide by the GDPR rules and principles through the Privacy Pact website. <i>Answer A</i> is a resource repository for various stakeholders, <i>Answer B</i> is a global registry of public information on data processing activities, while

		<i>Answer D</i> is for registering and authenticating Europrivacy certificates.
8	A	Module 2 – Normative and perspective references (slide 10) In the list, only ISO/IEC 17065 is considered an external reference. The rest of the answers are part of the Europrivacy Complementary Normative Documents list.
9	A C	Module 1 – Welcome Pack (slide 20) The Welcome Pack is an introductory starter pack for Applicants interested in certifying their data processing activities with Europrivacy. <i>Answer B</i> is not included as part of the Welcome Pack as it is readily available to everyone through the Europrivacy Registry of Certificates.
10	B	Module 2 – Key principles (slide 16) While <i>Answer A</i> refers to the principle of <i>openness</i> , <i>Answer C</i> refers to the principle of <i>building trust and confidence</i> , and <i>Answer D</i> refers to the principle of <i>confidentiality</i> .