Europrivacy.com
Privacy Audit and Certification

Europrivacy™/®
FAQ for Official Partners

Identifier:	EP-G.FAQ.P
Version:	1
Date:	12 June 2022
Publication status:	**Confidential**
Websites:	www.europrivacy.com
	www.eccpcentre.com
Contact:	admin@europrivacy.com

Introduction

The aim of the following document is to provide clarifications on frequently asked questions by official Europrivacy partners (certification bodies, consulting and law firms, and software providers) in relation to their Europrivacy-related services in all stages of the process. The section "Customers' Questions" offers prepared responses to the most commonly asked questions by Europrivacy Applicants (partners' clients).

Table of Contents

Introduction

This document gathers and answers frequent questions related to the use and implementation of Europrivacy. It is specifically intended to official partners and professionals who are using and implementing Europrivacy certification scheme and methodology. It complements the general FAQ on Europrivacy that answers more general questions on its genesis and methodological approach.

This document is purely informative and provided as is on a best effort basis without contractual obligations for the Scheme Owner or other Parties.

Useful Definitions

Applicant: The Client of a Certification Body applying for a Europrivacy certification.

Data subject: Any *"identified or identifiable natural person to whom the data relates."*

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."*

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."*

Data Processor: *"A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller."*

European Data Protection Board: is the European body established *"to contribute to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities."*

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.

Minor Non-Conformity: A non-critical Non-conformity which does not qualify as a Major Non-conformity. A non-Conformity can be qualified of "minor" only if it has no impact on data subject's rights and would not cause a certification to be perceived as misleading by end-users and consumers.

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."* (GDPR Article 4)

Scheme Owner: The organisation responsible for developing and maintaining the Europrivacy Certification Scheme.

Supervisory Authority: The national authority, which has received the legal mandate to overview the certification of compliance with the applicable data protection regulations.

Target of Evaluation: The description and specification of the data processing activities to be assessed and certified through a certification process. The Target of Evaluation shall be clearly specified and easily understandable by the data subjects.

Europrivacy Resources and Tools

Europrivacy Online Resources

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. The experts in charge of supporting Applicants must have completed the "Course for Implementers" and successfully passed the test. https://academy.europrivacy.com
3. The **Europrivacy Community Website** provides a whole set of online resources, templates and documents to facilitate both the pre-certification and certification processes, as well as to support the continuous enhancement of data protection compliance once the certificate has been delivered. https://community.europrivacy.com
4. The **Privacy Pact** enables any company, regardless of its location, to commit to respecting the GDPR obligations, including the Data Processors-specific obligations listed in Art. 28 GDPR. https://www.privacypact.com

Europrivacy Useful Documents

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

- EP-G.FAQ.A – FAQ on Europrivacy Certification Scheme Model
- EP-I.INTRO – Europrivacy Introduction and Overview
- EP-CS.1 – Europrivacy Certification Scheme
- EP-C.ALL – Europrivacy List of Checks and Controls
- EP-G.CF – Europrivacy Guidelines for Consulting and Law Firms
- EP-G.CB – Europrivacy Guidelines for Certification Bodies
- EP-G.CC – Europrivacy Guidelines on the use of Criteria, Checks and Controls
- EP-G.COM – Europrivacy Communication and Marketing Rules
- EP-P.TC – Europrivacy General Terms and Conditions
- TBC – Europrivacy White Paper on GDPR Certification

Clients' Usual Questions

The following section provides suggestions on how to best respond to frequently asked questions by Applicants and Clients.

Q1 What can be certified?

Europrivacy methodology has been researched and developed to be applicable to a large set of scopes and data processing activities, including data processing, products, services and management systems. However, the European Data Protection Board has set strict limits to what can be certified under GDPR Article 42 and 43: **Only data processing activities can be certified.** The certification of a whole company or a management system with a single certificate is not accepted by the European Data Protection Board.

The positive aspect of this restrictions is that it forces to have more reliable certifications and it enables companies to start with the most mature data processing.

In order to determine the scope of a data processing, the Applicant can use its record of data processing.

In non-EU jurisdictions (i.e., Switzerland), there is the possibility to certify beyond data processing also products, services, and information management systems.

Q2 Who can apply for certification?

The Europrivacy certification is applicable to almost any data processing activity, whether it is processed by a data controller or a data processor. It is applicable to private and public entities. It is also applicable to data processing distributed across several jurisdictions.

The main restriction may come from the location of the data processing activities. It is possible to certify data processing activities in Europe and in non-European countries, as long as it can be demonstrated that the rights of the data subjects are effectively protected. They must comply with the European Data Protection Board requirements with regards to the right of freedom of data subjects. Such conditions are not satisfied in all countries, in particular in non-democratic countries that do not respect individual civil and political rights. To assess if a country is eligible, you may consider using the criteria G.10 and in particular criterion G.10.1.5.

Q3 Why should a company certify its data processing activities? Is it a legal obligation?

Although not a legal obligation, the GDPR makes over 70 references to certification as a powerful mechanism to reduce the risks of non-conformity, to assess the compliance of data processors and the adequacy of data transfers, including towards non-EU jurisdictions.

Here are a set of benefits in performing a Europrivacy certification:

1. **Identify and reduce legal and financial risks**
2. **Assess, validate and demonstrate GDPR compliance**
3. **Build Trust and Confidence**
4. **Develop competitive advantages**
5. **Improve reputation and market access**
6. **Support cross-border and processor data transfer**
7. **Reduce risks with certified data processors, at no cost**

8. **Turn data protection into an asset and source of revenues**
9. **Benefit from continuous compliance updates**
10. **Extend compliance to non-EU jurisdictions**

In B2C relations, demonstrating compliance through a recognised certification scheme helps building trust within data subjects and supports data controllers in complying with their legal obligation of accountability.

In B2B relations, data controllers working with data processors have a strong incentive to get their data processors certified. Otherwise, they have to carry themselves the assessment of the technical and organisational measures set in place by their processors: high cost and liability. Reciprocally, data processors will directly benefit from a certification that will be a strong competitive advantage, not only to build trust, but also to reduce effort and cost on the data controller side.

Q4 How to pitch Europrivacy Value Proposition?

We invite you to leverage the numerous available resources, including the value proposition in the previous FAQ, the Benefits and Advantages of Europrivacy, as well as the Europrivacy White Paper.

Additionally, we propose the following considerations:

1. Europrivacy enables to identify and reduce legal and financial risks of the company by systematically assessing the compliance of the data processing activities.
2. The cost of non-compliance is far higher than the cost of compliance. To assess the cost of non-compliance, you can use the Europrivacy online GDPR Certification Cost Saving Estimator: https://www.europrivacy.com/en/resource/gdpr-estimator
3. Complying with the European General Data Protection Regulation (GDPR) is not an option. With over 70 references in the GDPR, Europrivacy certification is a powerful mechanism to identify and reduce the risks of non-conformity. It can be used to reduce uncertainty on the level of compliance, including for the DPO and top management of the company.
4. A certification relies on an independent and impartial assessment made by qualified auditors and certification bodies whose accreditation is supervised by a national authority. As such, it brings an additional layer of trust with third parties, including data subjects, B2B partners and the public.
5. As stated in art 42 and 46 GDPR, certification can be used to assess and demonstrate that appropriate safeguards are in place when data are processed in third countries, including in non-EU jurisdictions
6. So far controllers had no other choice than to monitor and assessing by themselves the compliance of their data processors and sub-processors. Each controller had to repeat the same exercise from scratch with each one of their processors. Certification is recognized by article 28 as *"an element by which to demonstrate sufficient guarantees".* Using certified services of data processors will simplify the life and burden of data controllers.
7. A European Seal for certifying the compliance of data processing activities under the GDPR is recognized across all EU and European Economic Area jurisdictions.
8. Finally, Europrivacy certifications will enable to recognize and communicate the efforts made by data controllers and processors in complying with the regulation and protecting data subject rights and freedoms. It will enable to value these efforts and offers a fair recognition for those who are proactively working on compliance and privacy.

Q5 Why should an applicant choose Europrivacy?

There are several characteristics that make Europrivacy distinct from other certification schemes:

European and GDPR by design
funded by the European Commission.

Continuously updated to align with the evolution of regulations and jurisprudences

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

Comprehensive and applicable to almost any data processing activities

Independent and managed by an international board of experts

Online resources, tools, and support

Global ecosystem of qualified partners and experts

Research and Innovation empowered

Moreover, Europrivacy is the first hybrid certification scheme that combines the advantage of a single certification scheme for all sorts of data processing, while taking into account technology and domain specific requirements (*see Q6 in FAQ on Europrivacy Certification Model*).

Q6 How much does a Europrivacy certification cost?

The cost of a certification is composed of the following items:

1. **The cost of the consulting or law firm** that will support the Applicant to prepare and document the criteria for the certification. This cost varies from case to case and is optional in case the Data Protection Officers of the Applicants decide to document the criteria by themselves.
2. **The Europrivacy Welcome Pack** that provides a comprehensive set of resources and online services to the Applicant for a period of three years. It includes also the two first certificates publication fees. The Welcome Pack reference price is 6'000.- Euros, but it may be charged at a lower price to official partners according to their category of partnership. An Applicant purchases only one welcome pack, regardless of the number of data processing to be certified.
3. **The certification body fees** to perform the assessment of the data processing to be certified. The cost my vary among certification bodies and according to the country. The initial certification will be followed by shorter yearly surveillance audits. To estimate the audit time, see the next FAQ.
4. **If applicable, the additional certificates publication fees** on the Europrivacy official registry. **The two first publications fees are already included in the Welcome Pack; only the additional ones need to be purchased** (when certifying more than two data processing activities). They can be purchased individually or at a lower price when purchased in batches. The price list is available in the community website.

   The publication of the certificates on the official Europrivacy registry is mandatory and it enables to authenticate and prevent falsification of the certificates. It also addresses the obligations set be the European data Protection Board with regards to public information on delivered certifications.

Q7 How to determine the number of criteria and to estimate the Audit time?

The number of criteria to be prepared and assessed during the certification my vary according to the complexity of the data processing and the role of the Applicant (controller versus processor). Moreover, the first data processing to be certified is longer than the subsequent ones.

You can estimate the precise number of criteria to be prepared and certified with the following documents:

a. **Europrivacy Guidelines on Assessment Time Estimation** provides detailed guidelines on how to assess the time required for the assessment.

b. **EP Certification Process – Time Estimate and Roles** provides a summary of time required for a regular data processing certification.

c. **EP-F.CCN - Calculator of Europrivacy Criteria Number** enables to calculate the assessment time according to the characteristics of the data processing.

Q8 How long does it take to get certified?

The length of the certification process will depend on the Applicant's readiness, i.e., document preparation, identification of data processing activities to be certified, existing previous certifications, including ISO, etc. It the data processing of the Applicant is fully compliant with the GDPR, the documentation of the criteria can be done quite swiftly. The use of software can facilitate and accelerate the documentation process.

It is to be noticed that once a first data processing has been documented, the subsequent ones are faster to document as part of the criteria (criteria labelled as generic) are documented only one time with the first data processing and can be reused for the following data processing.

The assessment is usually performed in less than a week. See the previous FAQ for more details on the audit time.

Q9 Can an ISO/IEC 27701 certification, or ISO/IEC 27001, provide all or part of the evidence of compliance to comply with the Europrivacy criteria?

Criteria T gathers part of the criteria related to the security of the data processing activity to be certified. In order to avoid duplicating the effort and cost, in particular for SMEs, Europrivacy recognizes that a certification of the information management systems that covers the data processing to be certified can be considered as a substitute to the subset of T criteria, but only if the data processing is not a high-risk data processing.

If an Applicant has a valid ISO/IEC 27001 or 27701 certification that covers the scope of a data processing to be certified, and if the data processing activity to be certified is not a high-risk data processing, then the ISO certification can be recognized as an equivalent and substitute to the subset of Technical and Organizational Criteria (T criteria). Of course, all the other criteria must still be assessed and certified.

Preparing an Offer

Q10 Where should a partner start delivering Europrivacy services?

We recommend starting with clients located in the European Union. You can then progressively extend it internationally, first with countries with adequacy decision. We recommend to avoid data processing performed in countries that are considered at high risk for the rights of data subjects as it may be an obstacle to satisfy the EDPB requirements and Europrivacy criteria for cross-border data transfer.

Q11 What is the scope of a data processing?

The scope of a data processing must be clearly outlined and specified. It can comprise any operation or set of operations which is performed on personal data or on sets of personal data. It encompasses a set of personal data that are collected and processed for a specific purpose. For instance:

- Personal data of visitors collected and processed by a website;
- Personal data of customers collected and processed by the customer support service;
- Personal data of employees processed by the human resource service;
- etc.

The scope of the data processing is focused on the part of the data processing that is under the effective control of the Applicant. When data are transferred to other data controllers or processors, the scope will include the measures in place to ensure that these third parties comply with the data protection requirements.

While there is a certain flexibility when specifying the perimeter of a data processing, you must ensure that:

1. the data processing must be given a clear name;
2. the name must be understandable by third parties without risk of misinterpretation;
3. all personal data involved in the data processing can be identified and mapped.

Q12 How to specify the Target of Evaluation?

In practice, we recommend to use the Record of Data Processing mentioned under art. 30 of the GDPR. It should provide a good segmentation of the data processing activities of a company into distinct data processing.

In order to clarify and formalize the Target of Evaluation, we invite you to use the document “Application Form for Europrivacy Certification” that enables to specify and formalize the Target of Evaluation. It includes a simplified model for mapping the data processing to be certified, including the source of personal data and if applicable the data processors involved. The advantage of using this form is that you can directly use it to request offers from qualified Certification Bodies.

Once the Target of Evaluation has been specified, you should use the “Europrivacy Checklist A on Application and Target of Evaluation” (EP-C.A, version 56) to ensure that your Target of Evaluation complies with the European Data Protection Board requirements.

Q13 What is the Europrivacy Welcome Pack?

The Europrivacy Welcome Pack is a package of resources and services which facilitate the certification process and includes:

- **2 first Europrivacy certificates publication fees**
- **Europrivacy Introductory Course for the DPO of the Applicant**
- **DPO Access to Europrivacy Platform of Online Resources** for Europrivacy certification and GDPR compliance, including national and domain specific requirements, useful links and updated reference documents.
- **Europrivacy Flash Alerts on regulatory changes** to be kept informed and updated on requirements changes due to regulatory changes, jurisprudence, EDPB publications, etc.
- **1 Privacy Pact** for communicating commitment to respect data protection and the GDPR.
- **Europrivacy Advocate Status** and access to an ecosystem of companies engaged in promoting data protection compliance.

Q14 What is usually included in a Europrivacy Welcome Offer by a consulting or law firm?

The consulting or law firm acting as official Europrivacy partner will invite the Applicant to select two priority data processing activities and will usually propose the following services in its initial welcome offer:

- Provides a Europrivacy Welcome Pack.
- Prepares the documentation for the certification
- Assesses the compliance with the criteria and reports remaining non-conformities if any
- Supports for remediating identified non-conformities if any
- Validates the readiness
- Prepares the Application and Target of Evaluation specification
- Handovers to the Certification Body
- Delivers a Certification Plan for remaining data processing

The Welcome offer may also include discounts on complementary services such as self-assessment solutions (i.e. Smart Global Governance discount for their solution).

Q15 Is the Europrivacy Welcome Pack mandatory?

The Europrivacy Welcome Pack is a set of resources and services made available to the Applicant (client) to support the certification process with online resources, to cover the two first certificates publication fees and to get regular updates on the certification requirements for three years. It is highly recommended that the Applicant purchases a Welcome Pack, and we recommend including it in the Welcome Offer of the consulting of law firm.

Nevertheless, there is also the possibility for the Applicant to purchase the Welcome Pack separately or to include it in the offer made by the certification body. Alternatively, the client can choose to renounce to the Welcome Pack but then he will have then to pay the certificates publication fees instead.

Q16 How to calculate the budget for an offer?

For Implementers

1. Clarify the number of data processing activities to be certified (number of Targets of Evaluation).
2. Determine the cost for delivering your services as an implementer, including:
    a. to gather the required documentation;
    b. to check and document the compliance of the selected data processing with the criteria. The exact number of criteria can be calculated with the Excel file "Calculator of Europrivacy Criteria Number" and/or with the document "Europrivacy Guidelines on Assessment Time Estimation". You can estimate:
        i. about 5 days for a controller and 3 days for a processor for the first Target of Evaluation;
        ii. about 4 days for a controller and 2,5 days for a processor for each subsequent Target of Evaluation.
    c. to support the Applicant in addressing the identified gaps and non-conformities;
    d. to prepare the application with the Target of Evaluation for the certification body;
    e. to prepare a certification plan for the remaining data processing.
3. If the Applicant does not have a Welcome Pack yet, add the cost of a Welcome Pack.
4. If the Applicant wants to have an offer that is all-inclusive, you can also request an offer from a qualified certification body. You can also consider including an offer from a software solution provider.
5. if required, add the additional certificates publication fees required (the two first publication fees are included in the Welcome Pack).

For Certification Bodies

1. Clarify the number of data processing activities to be certified (number of Targets of Evaluation).
2. Assess the costs for your certification service. to check and document the compliance of the selected data processing with the criteria. The exact number of criteria can be calculated with the Excel file "Calculator of Europrivacy Criteria Number" and/or with the document "Europrivacy Guidelines on Assessment Time Estimation". You can estimate:
        i. about 5 days for a controller and 3 days for a processor for the first Target of Evaluation;
        ii. about 4 days for a controller and 2,5 days for a processor for each subsequent Target of Evaluation.
3. Add the following costs:
    a. If the Applicant does not have a Welcome Pack yet, include the budget of a Welcome Pack (valid for three years);
    b. If you intend to certify more than two data processing (whose publication fees are included in the Welcome Pack), calculate the additional certificate publication fees.

We invite you to consult the Europrivacy Example for Certification Bodies' Costs and Revenues (EP-G.EX) as well as Europrivacy Examples for Consulting and Law Firms' Revenues and Costs (EP-G.EXCF) for details on the costs for on-site support.

Preparatory Phase

Q17 How much time would the documentation and assessment require?

The required time for the assessment depends on multiple variables, including:

- The readiness of the client – Do they have all needed documents in place?
- How many data processing activities does a client wish to certify?
- Does the client possess previous certifications, i.e., ISO 27701, etc. that may be relevant and considered during the certification process?
- Is this the client's first Europrivacy certification or have their already undergone Europrivacy assessment?

Furthermore, the readiness of the Implementer/ Auditor is also to be considered. In general, for the first certification, the implementer/ certification body may have additional questions during the process for which they may require the help of the Scheme Owner. Such consultations may slow down the process; however, this would only be the case for the first certification.

For Certification Bodies, we have prepared a high-level estimate of the time to complete the certification process. The document "Europrivacy Certification – Time Estimate and Roles" can be consulted on the Europrivacy Community website.

Q18 How can I get support for conducting the Europrivacy assessments?

First of all, the Europrivacy Community website provides a comprehensive set of resources, templates and guidelines to make your journey with Europrivacy as efficient and enjoyable as possible.

In addition to the regular resources, where needed our official partners can request online or on-site support delivered by qualified Europrivacy experts. Such support is not free but you can request an estimate for such services.

The use of an adequate software solution to document the compliance can also support and facilitate the process.

Q19 How to make a certification plan for the Applicant?

We recommend using the Record of Data Processing Activities mentioned under art. 30 of the GDPR. It should provide a good segmentation of the data processing activities of a company into distinct data processing.

We invite you to use the template Excel file document "Europrivacy Certification Plan Table" *(TBC)* to map all recorded data processing activities or to use ad hoc software solutions

Then, for each data processing, you should assess and determine for each data processing:

1. the level of risk for the Applicant and/or for the data subjects;
2. the likeliness of the risk to occur;
3. the resulting priority levels.

Once the table is complete, you can reorder the data processing according to their priority level, from the highest to the lowest priority level.

You can then prepare the Certification Plan report with the template "Europrivacy Certification Plan Report" *(TBC)*.

Finally, you are encouraged to budget and prepare an offer to cover the first slice of high priority level data processing you have identified.

Q20 How to pass the token from an implementer to a Certification Body once the Target of Evaluation is ready for certification?

Once an implementer has supported an Applicant with the documentation of the Europrivacy criteria, it can either request offers from qualified Certification Bodies or let the Applicant contact and select a certification body.

The list of authorized certification bodies is available on the main Europrivacy website, in the official partner's section: https://www.europrivacy.com/en/partners/list. It is also possible to request offer directly through the dedicated form of the Europrivacy website at: https://www.europrivacy.com/en/contact/apply-certification

Assessing Compliance

Q21 What is required from a Certification Body to be authorized to deliver formal Europrivacy certification?

The certification body must satisfy three conditions:

1. To be an official Europrivacy partner (can be checked on Europrivacy public website);
2. To obtain a formal accreditation under article 43 GDPR to be delivered by a national authority in one of the EU members states;
3. To use qualified auditors who:
    a. have adequate expertise in data protection regulation; and
    b. have successfully passed the exam of auditor on the Europrivacy online academy.

Q22 Can a certification body deliver certificates in other countries?

Once a certification body has obtained an accreditation in one EU member state, it can deliver certifications to applicants in all European countries. However, the review of the audit report and the decision to deliver the certificate shall be taken in the country where the certification body has its accreditation. The certification body shall also inform the data protection authority of the country where it is delivering its services.

Q23 What are the required competencies of the personnel of the Certification Body?

As requested by the EDPB, the audit team of the certification body must gather expertise in:

- audit and certification, including Europrivacy certification scheme;

- data protection regulations, including GDPR requirements;
- technical and organizational measures to secure the data (Cybersecurity).

The auditors must have completed and passed the exam of auditor on the Europrivacy online academy.

The auditor must also comply with the requirements specified by the European Data Protection Board and where applicable the complementary requirements specified by the national authorities.

More details on the required qualification of personnel are available in:

- EP-P.3 Management of Competencies of Personnel Involved in Europrivacy Certification
- EP-P.4 Management of Competencies of Personnel - Complementary Guidelines

Q24 What are the differences between (1) Criteria, (2) Checks and Controls, and (3) Checklists?

Criteria refers to the core Europrivacy requirements. They are formal mandatory requirements that must be used by the auditor when assessing the compliance of the Target of Evaluation.

Checks and Controls refers to complementary mandatory requirements that must be assessed by the auditor too.

Checklists refers to list of informative requirements that made available to facilitate the implementation of Europrivacy and to support the certification process.

Q25 What is the difference between Major and Minor Non-Conformities?

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 as stated in this document. Any non-conformity where the Applicant breaches its 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. In case of remaining Minor Non-Conformities, the Applicant must present a remediation plan and commit to address the identified non-conformities before the subsequent surveillance audit or recertification.

Q26 Can a certificate be delivered in the presence of non-conformities? When is it prohibited to deliver a certificate?

Europrivacy authorises to deliver certificate when there is up to five minor non-conformities if:

1. there is a plan to address these non-conformities; and
2. there is no major non-conformity.

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

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

Closing, Reporting and Follow-Up

Q27 Is there a surveillance audit required during the validity period of the certificate?

Yes, on a yearly basis, as indicated in the scheme. After the initial certification, a first surveillance audit must be performed by month 12 and a second surveillance audit by month 24, like for ISO/IEC 27001. The surveillance audits are usually substantially lighter and shorter than the original certifications.

Miscellaneous

Q28 What are the fundamental rules to follow when applying Europrivacy?

1. **Trust and reliability**: Europrivacy aims at building trust and confidence. There shall be no complacency in the assessment of the compliance and only compliant data processing shall be certified.
4. **Impartiality**: Europrivacy official partners, implementers and auditors must preserve impartiality when delivering their Europrivacy-related services. For instance, certification bodies and auditors cannot deliver certifications to clients to which they have provided consulting services. They can explain the identified non-conformities, but they cannot provide advice on how to resolve the non-conformities. Similarly, it is not possible for a certification body and a consulting firm to do joint marketing.
5. **Quality of service**: Europrivacy Implementation and audits shall be conducted by skillful professional, who, beyond their legal and/or technical training, have successfully completed their Europrivacy Academy courses.
6. **Precaution principle**: In case you have doubt on a criterion, you should not validate its compliance until you can demonstrate that the target of evaluation is complying with satisfactory evidence.
7. **Evidence-based assessment**: You must be able to justify your decision on the basis of evidences for each one of the criteria.
8. **Efficiency**: Europrivacy methodology has been designed to be efficient, including with a large number of data processing activities to be assessed and certified.
9. **Courtesy and customer satisfaction**: All Europrivacy partners are required to behave professionally and to always remain courteous with their Europrivacy-related clients. They shall do their best effort to deliver high quality service and the best customer experience possible.
10. **Anti-corruption and anti-bribery policy**: Europrivacy certification activities aim at building trust and confidence. All certifications shall be delivered in a professional, reliable and ethical manner, compliant with the law, and impartially. Partners must refuse any attempt of corruption, bribery or other forms of influence that could compromise their impartiality.
11. **Prohibition of anti-competition practices**: Partners of the Europrivacy ecosystem are required to respect free competition and related market regulations. Anti-competition practices, such as price setting, are strictly prohibited.
12. **Continuous improvement**: Europrivacy follows a continuous improvement policy. The Europrivacy ecosystem partners are required to report issues and potential for

improvement to the scheme owner (ECCP). Your views are important and will be taken into account.

For more details, please consult the following documents:

- Europrivacy Anti-corruption and Anti-bribery Charter, available online at: https://community.europrivacy.com/wp-content/uploads/2021/04/EP-P.AC-Europrivacy-Anti-corruption-Charter-v2.pdf.
- Golden Rules for the Auditors, available online at: https://community.europrivacy.com/wp-content/uploads/2021/04/EP-P.GR-Europrivacy-Golden-Rules-for-Auditors.pdf

Q29 What is the role of Implementers?

The implementers deliver consulting and support service to applicants. Their qualified experts will help the applicants preparing and documenting the compliance of their data processing activities with the Europrivacy criteria for certification. They contribute to reduce the legal and financial risks of the applicant.

Q30 How is the maintenance and development of the certification scheme funded?

The maintenance and further development of the scheme relies mainly on the welcome pack revenue and certificates publication fees. These revenues enable to further develop and expend the certification scheme.

Q31 Does an official Partner have to pay for using the Europrivacy Certification scheme? Does it have to purchase the Welcome Pack?

Europrivacy functions on a model of free licensing to selected official partners. These partners have free access to the regular Europrivacy services and do not need to purchase the Welcome Pack for themselves.

The Welcome Pack is aimed to and paid by the clients of the partners. It shall be included in the offer made by the partner to its client. Similarly, the certification body shall check if the applicant has a welcome pack when preparing its offer. If the applicant does not have a welcome pack yet, the certification body shall include it in its offer. If the applicant wants to certify more than two data processing, the certification body shall also add the certificates publication fees for the additional certifications.

All these resources can be purchased on online through the community website. It is to be noticed that official partner may benefit from discounts.

Q32 How is the certification scheme funded?

Europrivacy aims at developing a virtuous ecosystem of complementary partners. Official partners have access to most services for free. In order to maintain and further develop the scheme, the European Centre for Certification and Privacy gets revenues from Europrivacy-related online services, such as the academy, the community website and the publication fees of delivered certifiates on the official Europrivacy registry. Most services are included in the Europrivacy Welcome Pack.

