Europrivacy.com
Privacy Audit and Certification

Europrivacy™® Guidelines for Applicants to Certification

Identifier:	EP-G.AP
Version:	7
Date:	12 March 2024
Publication status:	**Confidential**
Websites:	www.europrivacy.com
	www.eccpcentre.com
Contact:	admin@europrivacy.com

Europrivacy Guidelines for Applicants to Certification

Introduction

Europrivacy is a certification scheme and methodology to check, document, and certify compliance of data processing activities with the GDPR and other data protection regulations. It serves as official European Data Protection Seal under Art. 42 GDPR. These guidelines aim at facilitating the implementation of Europrivacy by Applicants. They provide recommendations and useful references.

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 shall be easily understandable by the data subjects.

General Principles

Europrivacy is a certification scheme and methodology developed for documenting, assessing, and certifying the compliance of data processing activities with the European General Data Protection Regulation (GDPR). Its criteria have been approved by the European Data Protection Board (EDPB) to serve as European Data Protection Seal under Art. 42 GDPR and are recognised by all EU and EEA jurisdictions. The Europrivacy certification scheme is maintained and updated by the European Centre for Certification and Privacy (ECCP) and its international board of experts.

Europrivacy can be extended to include complementary regulations and requirements, including non-EU regulations on data protection. Beyond the deliverance of a certificate itself, the Europrivacy criteria have been designed to reduce the legal and financial risks of the Applicant.

A GDPR certification performed under Art. 43 of the GDPR is quite distinct from usual ISO certifications. It aims at providing an impartial and fair indication of compliance of data processing activities with the European and applicable national data protection regulations. It is subject to strict requirements established by the EDPB, a European Union body established by the GDPR.

Smart Journey to Data Protection Certification

The Europrivacy certification is organized in three stages:

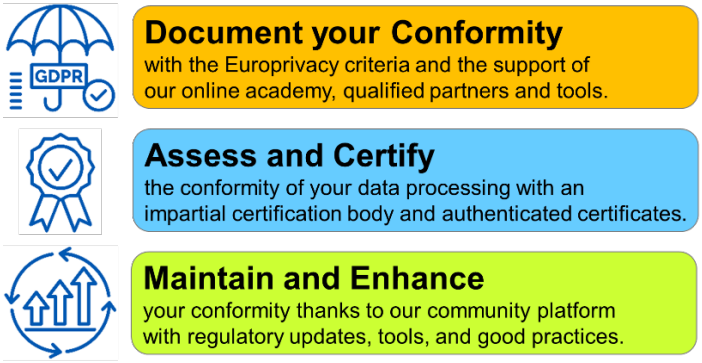

Figure 1 – Smart Journey to Europrivacy Certification

Europrivacy offers a virtuous process to build trust and confidence:

1. **Reducing legal and financial risks** through a systematic gap analysis to identify any remaining non-conformity and by documenting the compliance with the criteria;
2. **Demonstrating and valuing GDPR compliance** through the deliverance of certificates by impartial and qualified certification bodies;
3. **Providing continuous support** to maintain and enhance compliance with changing obligations.

Europrivacy Value Proposition

In summary, Europrivacy has been designed to deliver the following benefits:

1. **Identify and reduce legal and financial risks** through audit and systematic gap analysis.
2. **Demonstrate and value GDPR compliance** (Art. 42) through impartial third-party assessment.
3. **Improve reputation and access to market** through GDPR certification
4. **Ease cross-border data transfer** (Art. 46)
5. **Reduce risks when selecting data processors** (Art. 28)
6. **Provide competitive advantages**
7. **Build Trust and Confidence** (with B2B and B2C)

Europrivacy Resources and Tools

The Applicant can leverage several resources and tools to prepare and support their Europrivacy certification, 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
4. The **Privacy Pact** enables any company, including Data Processors, to commit to respecting the GDPR obligations regardless of their location, including the Data Processors-specific obligations listed in Art. 28 GDPR. https://www.privacypact.com
5. The Europrivacy **Welcome Pack** provides a whole set of resources and services to the Applicant, including the introductory course on the Europrivacy Online Academy, a Privacy Pact registration, the access to the Europrivacy Community Website, the two first certificates registration fees, Europrivacy Supporter Status and access to the community of experts, and a Europrivacy Flash Alert service that provides information on regulatory changes that may impact the GDPR compliance. https://www.europrivacy.com/en/ep/welcome-pack.

The Welcome Pack is usually included in the offer made by official partners such as qualified law firms and consulting firms, and can be purchased from the Community website.

Europrivacy Useful Documents

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

- EP-G.INTRO – Europrivacy Introduction and Overview
- EP-CS.1 – Europrivacy Certification Scheme
- EP-C.ALL – Europrivacy List of Criteria, Checks and Controls
- EP-G.CC – Europrivacy Guidelines on the use of Criteria, Checks and Controls
- EP-G.COM – Europrivacy Communication and Marketing Rules
- EP-G.STOA – Europrivacy Guidelines for Specifying the Target of Evaluation
- EP-P.TC – Europrivacy General Terms and Conditions

Preliminary Activities

Ensuring Compliance

For an Applicant to be certified, it must make its data processing activities comply with the data protection regulation. The GDPR requires several specific actions from the Applicant, whose implementation will be verified in the certification process.

Please note that two contextual requirements of the GDPR are mandatory for Europrivacy certification:

1. Designating a qualified Data Protection Officer (DPO). The DPO can be internal or provided as an external service, but in all cases, they must have adequate expertise in data protection regulation.
2. Having in place a record of the data processing activities, as well as records of data subject requests and data breaches as specified in the GDPR.

Documenting Compliance

It is important to document the above-mentioned actions to comply with the GDPR. For instance, where the GDPR requires to perform an assessment, the Applicant must have evidence that such assessment has been made. The Applicant is encouraged to prepare and systematically document its compliance with the GDPR and Europrivacy criteria in advance. A good and complete documentation is required to be certified and to reduce the legal risks of the Applicant. Documentation should be as much as possible provided in a single repository shared with the auditors. It can also be prepared with a conformity self-assessment software that includes the Europrivacy criteria. **The reference list of expected documents is provided in Annex 2**.

Internal Policies and Procedures

The GDPR implicitly requires having set in place a certain number of internal policies and procedures to comply with the law (i.e. for handling and complying with data subject requests). Usually, these policies and procedures will be the same for all ToE. **The reference list of key requirements to be present in the Applicant's policies and procedures is provided in the Annex 3**.

DPO Statement

In the Europrivacy certification process, the DPO of the Applicant is expected to confirm in written form a certain number of requirements. To simplify the certification process, **an example of DPO Statement that is expected for the certification of the ToE is provided in Annex 4**. As these statements are ToE-specific, there must be a distinct DPO Statement for each ToE. An editable template of DPO Statement is made available in the Europrivacy Community Website.

National Obligations Conformity Assessment Report (NOCAR)

Both the GDPR and the EDPB require that national obligations are taken into account when delivering a certification of compliance. In order to address these requirements, when assessing the compliance of a data processing activity in the European Economic Area, Europrivacy requires that the Applicant requests its DPO or a qualified legal expert to assess the conformity of the Target of Evaluation with the applicable national-specific obligations.

To facilitate this process, ECCP has established national profiles including the list of the most important national-specific obligations. These national obligations profiles, a NOCAR template and complementary resources are available through the Europrivacy Community Website.

In addition, Europrivacy is easily extensible to complementary national data protection regulations outside of the European Economic Area. Where applicable, such geographic extension of the certification requires to assess and comply with complementary requirements published by the Scheme Owner for selected non-EU countries.

Application and Certification Process

The Applicant requests an offer from a qualified certification body[1] by filling a formal application form in which it describes the Target of Evaluation (ToE) of the data processing activities to be certified.

Specifying the Target of Evaluation

The European Data Protection Board has set strict requirements with regards to the way the Target of Evaluation (ToE) must be specified. It must be clearly understandable by third-parties and prevent risks of misinterpretation by third parties. The official Europrivacy partners can help the Applicant specifying their ToE. Europrivacy also provides dedicated guidelines[2] and a checklist[3] to help specifying and validating the adequacy of the ToE description before starting the assessment.

Gathering the Documentation

The Certification Body provides a form with reference list of documentation[4] to be prepared and made available by the Applicant. Where needed for security reasons, documents can be prepared and consulted on-site. The Applicant shall complete and return the form with the list of available documents in order for the Certification Body to perform a preliminary documentation review.

Initial Certification Assessment

The Initial certification assessment will assess the compliance of the Target of Evaluation with all the applicable criteria, checks and controls. The number of criteria may vary according to several factors:

1. Role of the Applicant: whether it serves as Data Controller or as Data Processor.
2. Data processing of Special Categories of Data or data of minors of age.
3. Presence of special technologies and/or application domains.

If the Applicant has a valid ISO/IEC 27001 or 27701 certification that covers the ToE, some criteria can be skipped. Likewise, if a similar ToE has already been assessed and certified, the evidences of generic criteria can be reused, saving time for subsequent certifications (i.e. assessing the DPO qualifications).

The Audit team may identify non-conformities. The Applicant will be given a delay to address these non-conformities. All Major Non-Conformities must be resolved in order to be certified. Up to 5 Minor Non-Conformities can be tolerated if the Applicant provides a clear plan to address them.

Initial Certification Decision

In line with ISO rules and principles, the decision to deliver the certification must be made by a person who has not been directly involved in the assessment. The decision is made on the basis of the report and findings of the audit team. If the decision is positive, the Certification Body delivers a certificate of conformity to the Applicant. The Certificate must be registered and published online in the official registry of Europrivacy certificates to become valid.

Surveillance and Recertification

In conformity with the EDPB requirements, Europrivacy certificates are valid for a period of three years, and are monitored through yearly Surveillance Audits: one audit within 12 months after the issuance of the certificate and a second within 24 months after the issuance of the certificate. It can be followed by a recertification at the end of the period of validity to deliver a new certificate for three years.

A Certification Process Overview is provided in Annex 1.

[1] A list of qualified certification bodies is maintained on the Europrivacy website.
[2] The *Europrivacy Guidelines for Specifying the Target of Evaluation*
[3] The checklist "*A – Application & ToE Checks and Controls.*"
[4] The checklist "*D – Documentation Checklist.*"

Criteria and Complementary Checks and Controls

Preliminary Phase

In the preliminary phase, Europrivacy uses two preliminary checklists that are mandatory:

- ***A - Application and Target of Evaluation – Preliminary Checks and Controls;***
- ***D - Documentation checklist for Europrivacy certification*** *(see Annex 2);*

It provides complementary informative documents and templates to facilitate the process, including:

- ***P - Checklist of Key Policies and Procedures Requirements*** *(see Annex 3);*
- ***N - National Data Protection Obligations*** compiling the main data protection obligations per country, to support the preparation of the National Obligation Compliance Assessment Report;
- ***I - Inventories of Datasets, Data Processors and Data Storage Locations;***

As well as templates (i.e. NOCAR, DPO statement, etc.) and hundreds of reference documents.

Assessment Phase

Beyond the core GDPR requirements, Targets of Evaluation may be subject to complementary national regulations or domain specific risks for the data subjects. In order to deliver reliable certifications applicable to a large variety of data processing activities, the compliance assessment combines the following criteria, checks and controls:

- ***"G - GDPR Core Criteria"*** to assess compliance with the core data protection requirements;
- ***"C - Complementary Contextual Checks and Controls"*** to assess compliance with the domain and technology-specific requirements;
- ***"T - Technical and Organizational Measures Checks and Controls"*** to assess the security measures set in place to protect the processed data (can be replaced by ISO/IEC 27001);

Surveillance Phase

Once a certificate has been delivered, the Certification Body will have to perform surveillance assessments to verify the continuous compliance of the Target of Evaluation. The surveillance audits are also subject to a series of specific checks and controls listed in:

- ***"S – Complementary Surveillance Checks and Controls"*** used in surveillance audits.

Overview of the Criteria Application During the Certification Process

The certification process is organised in a logical sequence of criteria, checks and controls to be applied by the Certification Body, as illustrated in Figure 1 below:

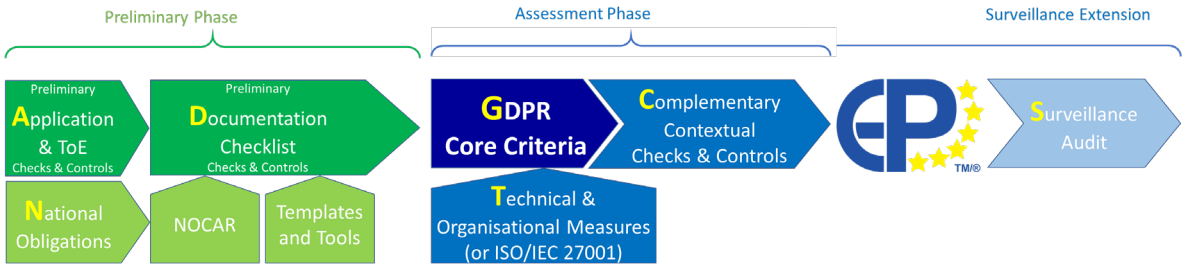

Figure 1 – Structure of Europrivacy Criteria and Complementary Checks and Controls

The reference list of criteria and checks and controls is maintained by the Europrivacy International Board of Experts of ECCP to take into account the evolution of the jurisprudence, national legislations and technology, as well as EDPB publications. A detailed description of the different sets of criteria is included in Annex 5, and the high-level requirements of the Europrivacy compliance assessment are listed in Annex 6.

Annex 1 – Certification Process Overview

The following table provides a detailed overview of the certification process.

STAGE	LEAD	OBJECTIVES	RESOURCES
DOCUMENTATION OF COMPLIANCE	Applicant	Document compliance with the applicable data protection regulations.	Guidelines for Applicant Europrivacy templates, checklists, and criteria
APPLICATION	Applicant	Specify the Target of Evaluation and fill the application form to request offer from Certification Body.	Europrivacy Application Form
APPLICATION REVIEW	Certification Body	Verify that the application and the Target of Evaluation conform with the EDPB requirements.	A – Application & ToE Checklist
OFFER AND AGREEMENT	Certification Body	Prepare an offer and sign the agreement, and terms and conditions.	Europrivacy General Terms and Conditions
CERTIFICATION PLAN	Certification Body	Prepare the Certification Plan, including methodology, assessment team, and planning.	Europrivacy template of Certification Plan
DOCUMENTATION PREPARATION	Applicant	Gather and complete the documentation.	Guidelines for Applicant D – Documentation checklist
DOCUMENTATION REVIEW	Auditor	Verify the qualification of the DPO and the availability of the required documentation.	D – Documentation checklist
CONFORMITY ASSESSMENT	Auditor	Assess the compliance of Target of Evaluation with the Europrivacy Criteria, Checks and Controls.	G, C, T criteria, checks and controls Guidelines for Auditors
INITIAL REPORTING	Auditor	Write the assessment report with the list of identified non-conformities.	Europrivacy template of assessment report
REMEDIATION	Applicant	Address and resolve the identified non-conformities.	List of non-conformities
FINAL REPORT	Auditor	Verify and validate the resolution of the non-conformities and update the assessment report.	Europrivacy template of assessment report
REVIEW	Certification Body	Review the assessment report and the required documentation. Make recommendation for certification.	Regular review process of the Certification Body
CERTIFICATION DECISION	Certification Body	Decide to certify or not the Target of Evaluation. Validate the decision with the Supervisory Authority.	Z – Europrivacy checklist for certificate publication
CERTIFICATE PUBLICATION	Certification Body	Communicate the decision and publish the certificate in the registry.	Europrivacy registry of certificates
COMPLIANCE MAINTENANCE	Applicant	Maintain and enhance compliance with data protection regulations.	Europrivacy community website
SURVEILLANCE / RECERTIFICATION	Auditor	Assess compliance of the Target of Evaluation with the Europrivacy Criteria, Checks and Controls.	S, G, C, T criteria, checks and controls

Annex 2 – List of Documents for Certification

The following documents and resources are to be assessed by the Audit Team. They should be gathered and made available to the audit team in due time. Documents that cannot be consulted remotely shall be made accessible to the auditors onsite.

Core Documentation

Data Protection Officer

1. Resume of the DPO
2. Certificates of the DPO qualifications in personal data protection and/or in law
3. Organization Chart, including the DPO function position in the organization
4. Access to the work contract between the Applicant and the DPO

Data Processing description

5. Presentation and description of the purpose of the data processing for the Data Subjects
6. Technical description of the solution, service or deployment
7. Drawing or UML description of the personal data flows
8. Website and webpage of the user interface with the data subjects
9. Copy of the information provided to the Data Subjects before/when collecting their data
10. The inventory (templates are available) of:
    - the datasets processed in the Target of Evaluation;
    - the data processors involved in the Target of Evaluation;
    - the data storage locations involved in the Target of Evaluation.

Compliance Assessment Reports and Documentation

11. Documentation that justifies the lawfulness of the data processing, including:
    - Evaluation of the data processing lawfulness;
    - Evaluation of the "data protection by design and by default" obligations (Art. 25 GDPR);
    - Any documentation that justifies the lawfulness (i.e. contract, legal basis).
12. DPO Statement of compliance (template made available).
13. National Obligations Conformity Assessment Report (NOCAR) for the Target of Evaluation, made by the DPO or by a qualified expert (template made available).
14. Where available, the Top Management Review report of the data protection policy.

Rules, policies and procedures

15. Public Data Protection Policy (made available to the data subjects).
16. Internal Data Protection and cybersecurity policies encompassing:
    - the data subject rights;
    - the data retention policy;
    - the access restriction to the processed data;
    - the cybersecurity.
17. Policies and procedures related to:
    - management of data subject rights and requests;
    - data protection by design and by default;
    - data protection breaches;
    - data processors;
    - data protection officer.
18. Where applicable, cookies policy.

Technical and Organisational Measures Related Reports

19. Risk Analysis Report(s) with recommended actions and plan to mitigate the identified risks.
20. Description of the Technical and Organisational Measures adopted by the Applicant for protecting the data in the Target of Evaluation.
21. Documentation of the assessment and review of the Technical and Organisational Measures.
22. Where available, valid certificates of cybersecurity certification such as ISO/IEC 27001 or 27701.
23. Where available, penetration test reports (PEN Test).

Complementary Documents to Be Provided Where Applicable

If a Data Protection Impact Assessment (DPIA) is required, then:

24. The Data Protection Impact Assessment (DPIA) Report (in line with Art. 35).

If the Target of Evaluation involves Data Processor(s), then:

25. Contractual clauses with the Data Processors (in line with Art. 28 GDPR).
26. Report or documentation presenting the Technical and Organisational Measures adopted by the Data Processors and the evaluation of the adequacy of such measures by the Applicant.
27. Where available, the GDPR certifications of the processors involved in the Target of Evaluation.

If the Applicant transfers data to third-countries (without adequacy decision), then:

28. Report or documentation justifying the adequacy of the cross-border transfer (in line with Art. 44-50 GDPR).

If the data processing is intended to data of minors of age, then:

29. Report or documentation demonstrating that the Applicant has adapted and assessed the wording of the information provided to be easily understood by minors of age.

If the Target of Evaluation does include automated decision making with impact on data subjects, then:

30. Report or documentation demonstrating that the Applicant has assessed the impact of the automated decision-making process and validated its compliance with the GDPR.

If the Applicant claims the use of Binding Corporate Rules (Art. 47 GDPR), then:

31. Copy of the Binding Corporate Rules.
32. Report or documentation demonstrating that the Applicant has assessed and validated the adequacy of these Binding Corporate Rules with the GDPR obligations.

If the Applicant claims the use of an Approved Code of Conduct (Art. 40 GDPR), then:

33. Copy of the Approved Code of Conduct based on Art. 40 GDPR.

If there is a joint-controller, then:

34. A document describing the respective roles of each controller

If there are Internet of Things deployment involved in the Target of Evaluation, then:

35. Deployment plan/map of the Internet of Things
36. List of deployed devices (preferably ordered per category)

If, there are Automated Decision-making Process, then:

37. Automated Decision-making Process description
38. Test report and/or analysis of the Automated Decision-making process and algorithm

If a newsletter is sent on the basis of the personal data processed in the Target of Evaluation, then:

39. Sample of newsletter(s)

Registries and Records to be made accessible during the audit

40. Record of data processing activities (in line with Art. 30 GDPR).
41. Registry of access rights to the personal data.
42. Record of access logs to the personal data.
43. Where available, record/log of consents given by the data subjects.
44. Records of communication/correspondence with:
    - the data subjects;
    - the data processors;
    - the national authority.
45. Record of data breaches and subsequent actions taken by the Applicant.
46. Access to the database storing the processed data for sample control and analysis.

Annex 3 – Indicative List of Key Requirements with Regards to the Applicants' Policies and Procedures

The Applicant should have adequate policies and procedures in place to comply with the GDPR. These policies and procedures should be clearly documented, complete and effectively applied.

Different Applicants may choose different ways to implement their policies and procedures. Policies and procedures can be distributed across various documents or centralised in a single document. It is however expected that all Applicants will have at least a reference Data Protection and Security Policy.

The following section lists **key requirements that should be part of the policies and procedures of the Applicant**. It is recommended to check and verify that the policies and procedures in place effectively cover each requirement of the list before the start of the audit. If any requirement is missing, it is recommended to adapt the Applicant's policy to comply with all the requirements.

Data Subject Rights

Information

1. To provide clear and transparent information to the data subjects on the processing of their personal data.
2. To inform in due time the data subjects about the indirect collection of their data.
3. To inform the data subjects on any further processing of their personal data envisaged for another purpose than the declared purpose for which the data were initially collected.

Minors of Age

4. To request the age of data subjects that are minors of age;
5. To request the consent of the holder of the parental responsibility for minor below the age of consent.

Data Subject Requests

6. To receive and record all the requests of the data subjects.
7. To identify and authenticate the data subjects in case of uncertainty on their real identity.
8. To assess and verify that all conditions are satisfied to proceed with the request.
9. To comply with the request without undue delay (except if there is a legitimate reason not to do so).
10. To monitor the delay between the reception of the data subject request and the reply and/or action by the Applicant.
11. In case of objection to the request, to inform and justify the non-action to the data subject, with:
    - the reasons for not taking action;
    - information on the possibility of lodging a complaint with a Supervisory Authority and the possibility of seeking a judicial remedy;
12. To prevent adverse effect on other data subjects' rights and freedoms when complying with a data subject request to transfer a copy of its personal data.
13. To enable data portability, enabling data subjects to obtain a copy of their personal data in electronic format, while requesting to:
    - filter out personal data pertaining to other data subjects if this may adversely affect the rights and freedom of the latter;
    - enable the transmission of personal data to other data Controllers where technically feasible.
14. To comply with the requests of data subjects to object to the processing of their personal data

15. In case of automated decision making, to comply with the requests of data subjects:
    - to obtain human intervention on the part of the Controller;
    - to express their points of view and to contest the decision.
16. To communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed.
17. Where applicable, to inform other Controllers about the request for erasure by the data subjects.
18. Where data are processed on the basis of consent, to prevent that personal data are disclosed to third-parties without data subject consent.

Data Protection by Design and by Default

19. To adopt data protection by design and by default policy for its data processing by:
    - analysing the risks for the freedom and rights of the data subjects in terms of likelihood and severity;
    - assessing if the collection of personal data is limited to what is needed;
    - assessing if the processing of personal data is limited to what is needed;
    - assessing if the retention period of personal data is limited to what is needed;
    - assessing if the access to the processed personal data is limited to who needs it;
    - using of encryption, pseudonymisation and anonymisation techniques where applicable.
20. To review on a regular basis (at least yearly) the technical and organisational measures in place and to keep documented records of the review of the technical and organisational measures.
21. To review the DPIA whenever the scope or purpose of the data processing of the Target of Evaluation is substantially modified or exposed to new risks.

Data Processors

22. To request and record information from potential data Processors about their technical and organisational measures to protect personal data and/or GDPR-related certification;
23. To assess the adequacy of the technical and organisational measures set in place to protect personal data;
24. To document and record the decision to accept the services of the Data Processor.
25. To keep documented records of:
    - the information and guarantees provided by the Processor on its Technical and Organisational Measures;
    - the evaluation and decision process to accept the data Processors involved in the data processing of the Target of Evaluation.

Security Policy

26. To have written security rules and/or policies to protect and secure the data processing, that covers at least:
    - the data confidentiality policy;
    - the data minimisation policy;
    - the data access policy;
    - the data processing restrictions (on instruction);
    - the data storage and retention period policy;
    - the data continuity and backup policy;
    - the data breach policy;
    - the restrictions on copying data and "bringing your own device".
27. To ensure that any natural person acting under its authority does not process personal data except if instructed by the Controller (unless he or she is required to do so by Union or Member State law).
28. To regularly test, assess and evaluate the effectiveness of the Technical and Organisational Measures at least on a yearly basis.

29. To document its tests and assessments of the Technical and Organisational Measures, including the identified vulnerabilities and actions taken to address these vulnerabilities.
30. To ensure that all the natural persons who come in contact with personal data shall be bound by confidentiality obligations which extend beyond the end of their activities.
31. To have an access control policy defined around roles and responsibilities.
32. To keep an updated registry of access rights of its employees and agents who can access the personal data.
33. To have an access right policy that is enforced and verifiable for both:
    - physical access to the place where the data are stored;
    - electronic access to personal datasets.
34. To have a monitoring system, a mechanism or a process in place to record and keep a log of:
    - access to personal data by employees and agents of the Applicant;
    - transfer of personal data to third parties, including processors and cross-border transfers.
35. To ensure the continuity of the processing and associated services in case of physical or technical incidents, including:
    - for ensuring the ongoing confidentiality and integrity of the personal data;
    - for ensuring availability and resilience of the access of the data subjects to their personal data.

Data Breach Policy

36. To record data breaches and follow-up actions with the date and time.
37. To determine and take appropriate actions to minimise the risks and potential impact on data subjects.
38. To assess if the data breach is likely to result in a risk to the rights and freedoms of natural persons.
39. If the risk is likely to result in a risk to the rights and freedoms of natural persons, to inform the Supervisory Authority without undue delay and no more than 72 hours after having been aware of it.
40. If the risk is likely to result in a risk to the rights and freedoms of natural persons, to inform the data subject without undue delay (except if a GDPR Art. 34.2 exception applies).
41. To include at least the following information in the notification procedure:
    - the nature of the personal data breach;
    - the categories and approximate number of data subjects and personal data concerned (where possible);
    - the name and contact details of the data protection officer or another contact point where more information can be obtained;
    - the likely consequences of the personal data breach;
    - the measures taken or proposed to be taken by the Controller to address the personal data breach, including where appropriate measures to mitigate its possible adverse effects.
42. To include at least the following information in the procedure for communicating a data breach to the data subjects:
    - the nature of the personal data breach;
    - the categories of personal data records concerned;
    - the name and contact details of the data protection officer or another contact point where more information can be obtained;
    - the likely consequences of the personal data breach;
    - the measures taken or proposed to be taken by the Controller (and/or recommended to the data subjects) to address the personal data breach, including where appropriate the measures to mitigate its possible adverse effects (where appropriate).

Data Protection Officer related Policies

43. To request employees to inform and involve the DPO in a timely manner in all data protection issues.
44. To give authority and effective access to the DPO for controlling personal data processing operations.
45. To protect the autonomy and independence of decision of the DPO.
46. To protect the DPO against any form of undue pressure related to the performance of his task.
47. To enable the DPO to directly report to the highest management level of the Applicant.
48. To periodically train personnel having permanent or regular access to personal data.
49. If specified in a policy, to assign at least the following tasks to the DPO:
    - to inform and advise the Applicant and its employees involved in data processing of their obligations regarding data protection;
    - to monitor the risks and compliance of data processing with the applicable data protection regulations and policies;
    - to provide advice on the performance of the data protection impact assessment and monitor its performance (in accordance with Art. 35 GDPR);
    - to cooperate and act as the contact point with the Supervisory Authority;
    - to handle or overview the requests of the data subjects when exercising their rights.

If the Applicant acts as Processor:

50. To prevent data processing without instructions from the Controller.
51. To receive and record instructions from the Controller.
52. To record its processing activities.

If Binding Corporate Rules are Used

53. To report, document, and record any breach of the binding corporate rules.
54. To assess the effectiveness of the binding corporate rules.

Annex 4 – Example of DPO Statement

The certification requires that the DPO confirms that it has assessed and validated the adequacy of the data processing activities covered by the Target of Evaluation. The following section presents an example of DPO Statement that is expected by the Auditors.

Certification Details

Company Name:

Target of Evaluation:

Data Protection Officer Details

First Name:

Family Name:

Email address:

Phone number:

Short description of the education/qualification in personal data protection regulations:

Statement

I hereby confirm that in my capacity of Data Protection Officer I have performed the tasks hereafter mentioned on the Target of Evaluation, with all due diligence and professionalism. I confirm that this statement has been made in full independence and impartiality, without any pressure from my hierarchy.

I hereby confirm the following:

Adequacy of the position

I have adequate expertise in data protection regulation to perform my task as a Data Protection Officer.

I have sufficient time to perform my work as Data Protection Officer and to overview the data processing included in the Target of Evaluation.

The work time of my position as DPO has been assessed by taking into account the types of data processing and the risks for the rights and freedom of data subjects.

Lawfulness assessment

I have assessed the lawfulness of the data processing in the Target of Evaluation and I confirm that it is lawful and based on (check the corresponding box(es)):

- ❑ Consent (Art. 6.1.a GDPR);
- ❑ Contractual necessity (Art. 6.1.b GDPR);
- ❑ Legal obligation (Art. 6.1.c GDPR);
- ❑ Vital interests (Art. 6.1.d GDPR);
- ❑ Public interest or official authority (Art. 6.1.e. and 6.3GDPR);
- ❑ Legitimate interests (Art. 6.1.f GDPR).

Where the data processing is based on legitimate interests, I have assessed the impact of the data processing on the rights and freedoms of the data subjects and I concluded that the legitimate interest is not overridden by the rights and freedoms of the data subjects.

National Regulations Compliance Assessment

I have assessed and I confirm the compliance of the data processing activities in the Target of Evaluation with the applicable national regulations of the Applicant, including with sector-specific data protection law. In my assessment, I also checked where applicable the compliance of the data processing activities in the Target of Evaluation with the indicative Complementary National Requirements provided by the European Centre for Certification and Privacy.

Special Categories of Data assessment

I have analysed the data processed in the Target of Evaluation in order to identify if it contains any Special categories of data such as:

- data that reveal racial or ethnic origin;
- data that reveal political opinions, religious or philosophical beliefs, or trade union membership;
- genetic or biometric data for the purpose of uniquely identifying a natural person;
- data on health, sex life and sexual orientation.

I have assessed the risks and impact of processing the special categories of data on the rights, freedoms and legitimate interests of the data subjects, and I confirm the lawfulness of the processing of the special categories of data.

Archiving purpose (if applicable)

Where the data are necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, I have assessed and I confirm that the processed data are useful and proportionate for the declared purpose.

Data Protection by Design and by Default assessment

I have assessed the data processing from data protection by design and by default perspective, including by:

- analysing the risks for the freedom and rights of the data subjects in terms of likelihood and severity;
- assessing if the collection of personal data is limited to what is needed, and if not making recommendations;
- assessing if the processing of personal data is limited to what is needed, and if not making recommendations;
- assessing if the retention period of personal data is limited to what is needed, and if not making recommendations;
- assessing if the access to the processed personal data is limited to who needs it, and if not making recommendations;
- recommending the use of encryption, pseudonymisation and anonymisation techniques where applicable;

and I confirm that:

- the analysis and recommendations are adequate;
- I did not identify less privacy intrusive solution in terms of personal data collection for achieving the same results and delivering the same services;
- the applicable recommendations have been implemented.

Technical and Organisational Measures assessment

I have assessed the results of the assessment of the Technical and Organisational Measures (TOM) and I concluded that they are sufficient and adequate to protect the rights and freedoms of the data subjects.

Transfer to Third Countries assessment (if applicable)

Where data are transferred to third-countries, I have assessed and validated the transfer as lawful and based on (check the corresponding lawfulness basis):

- ❑ Adequacy decision by the European Commission (Art. 45 GDPR);
- ❑ Appropriate safeguards (Art. 46 GDPR);
- ❑ Binding corporate rules (Art. 47 GDPR);
- ❑ Express consent of the Data subject (Art. 49.1.a GDPR);
- ❑ Contractual necessity (Art. 49.1.b GDPR);
- ❑ Interest of the data subjects (Art. 49.1.c GDPR);
- ❑ Public interest (Art. 49.1.d and 49.4 GDPR);
- ❑ Legal claims or procedures (Art. 49.1.e GDPR);
- ❑ Vital interests (Art. 49.1.f GDPR);
- ❑ Public registry (Art. 49.1.g and 49.2 GDPR).

Complementary Contextual Statements (where applicable)

In case of video camera deployment included in the Target of Evaluation

I have assessed and I confirm the compliance of the video camera deployment with the applicable laws and regulations.

In case of Internet of Things Deployments included in the Target of Evaluation

I have assessed and I confirm that:

- the deployment is lawful with regards to the GDPR;
- the benefits of using the IoT deployment are higher than the risks for the data subjects.

In case of Blockchain or Ledger Technology included in the Target of Evaluation

I have assessed and I confirm that the benefits of the use of Blockchain/ledger technology are higher than the risks associated with the technology.

In case of Artificial Intelligence and Data Analytic included in the Target of Evaluation

I have assessed and I confirm the lawfulness and adequacy of using artificial intelligence in the context of the Target of Evaluation, and I confirm that the intended data processing is:

- lawful;
- conform to the principle of purpose limitation;
- proportionate and conform to the data minimisation principle;
- does not generate any Special Categories of data which would not be part of the express consent given by the data subjects.

In case the Target of Evaluation related to Work Environment and/or Relationship

I have assessed and I confirm that:

- the Bring Your Own Device Policy adequately protect the rights and freedoms of the data subjects;
- the processing of the employees' data is lawful, proportionate and adequate.

Signature

Name:

Place:

Date:

Signature :

Annex 5 – Europrivacy Lists of Criteria, Checks and Controls

A – Preliminary Application and Target of Evaluation Checks and Controls

These preliminary Application and Target of Evaluation checks and controls are used by the Certification Body to assess the adequacy of the Target of Evaluation specification with the guidelines established by the EDPB. These checks and controls must be validated by the Certification Body before starting the assessment process.

D – Documentation Checklist for Europrivacy Certification

This document lists the required documentation to perform the assessment process. It is made available as a form that the Applicant can complete and return to the Certification Body, in order for the latter to perform a preliminary documentation review before the confirming the start of the formal assessment.

G – GDPR Core Criteria

The GDPR Core Criteria constitutes the backbone of all Europrivacy certification processes and shall be applied by the auditors of the Certification Body to each and every Target of Evaluation, regardless of its application domain and location. The Core GDPR Criteria enable a systematic assessment of the conformity with the key obligations contained in the GDPR. They ensure that all Europrivacy certifications guarantee a high level of conformity with the GDPR.

C – Complementary Contextual Checks and Controls

Particular application domains and technologies may expose the data subjects to specific risks for their rights and freedoms. The Complementary Contextual Checks and Controls are specified to assess domain and technology-specific data protection requirements. They take into account the publications and guidelines of the EDPB and national data protection authorities, as well as expertise from the research community.

The Complementary Contextual Checks and Controls are clustered in various subsets of checks and controls applicable to specific technologies and application domains. The Certification Body must go through the list of Complementary Checks and Controls and must assess and verify all the subsets of checks and controls that are applicable to the Target of Evaluation. For instance, if the Target of Evaluation includes a web interface and blockchain technology, the Auditor will have to apply the corresponding Complementary Checks and Controls to the Target of Evaluation.

N – National Obligations

Each country has several specific national laws and regulations that may impact and extend the requirements for data protection. Certified data processing **shall comply with the national data protection regulations, including domain-specific regulations, that are applicable to the Target of Evaluation.** It shall also comply with revisions of the applicable national regulations.

The Applicant shall have requested a legal expert with the adequate expertise to control that the data processing activities in the Target of Evaluation comply with the applicable national regulations, to the extent required by the National Supervisory Authority and the EDPB guidelines for certification.

Legal assessments can be performed by internal or external experts with adequate knowledge of the applicable regulations. DPOs can perform such assessment to the condition that they preserve their independence and do not take the responsibility of the Applicant.

Europrivacy provides a list of particularly important national requirements to be addressed when assessing the conformity of the Target of Evaluation with national obligations. These requirements must be taken into account by the legal expert mandated by the Applicant to perform the conformity

assessment with the national obligations. It aims at ensuring that these requirements are not forgotten by the legal expert performing the conformity assessment, but the assessment shall not be limited to this list and it shall consider all applicable national regulations.

This list is subject to changes according to the evolution of the national legislations and to comments received from the National Supervisory Authorities.

T – Technical and Organisational Measures Checks and Controls

Europrivacy certification requires that adequate Technical and Organisational Measures (TOM) are in place to protect the processed data. A set of key TOM requirements are included in the list of Europrivacy GDPR Core Criteria. They are complemented by a list of "Complementary Technical and Organisational Measures" checks and controls.

These checks and controls are mandatory, but if the Target of Evaluation does not include any High Risk Data Processing (as defined in the scheme), they can be replaced by an active ISO/IEC 27001 (or 27701) certification covering the Target of Evaluation. This approach makes the certification process more efficient and cost-effective for SMEs if they already have an ISO 27001 certification of their management system.

S – Surveillance Audit

Europrivacy has specified a few complementary checks and controls to be applied at the time of the Surveillance or Recertification audits to assess obligations which are specific to certified data processing, such as the obligation to provide information on the certified data processing in the languages of the member States. These criteria are not applicable to the initial compliance assessment.

Z – Checklist for Certificate Publication

This informative checklist is made available to the Certification Body to ensure that all conditions are met to deliver a Europrivacy certificate of conformity.

Annex 6 – High-level View on the Evaluation Criteria

Europrivacy detailed criteria are specified to evaluate the following aspects:

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 subject' rights, including the right 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, 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 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 established in third countries;

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 user to withdraw his/her 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 subject's 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:
   - 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 (ability);
     - 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 breach 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**;
   - where applicable, for Controllers established in third countries, the obligation to designate in writing a local or regional representative as required by the regulation;

n) if **Data Processors** are being used, the procedures and agreement 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 any natural person acting under their authority does not process data except on 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 or where it has acted outside or contrary to lawful instructions of the Controller;

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

