Europrivacy.com
Privacy Audit and Certification

Europrivacy™/® Guidelines on the Use of Criteria, Checks and Controls

Identifier:	EP-G.CC
Version:	21
Date:	15 February 2024
Publication status:	**Confidential**
Websites:	www.europrivacy.com www.eccpcenter.com
Contact:	admin@europrivacy.com

Europrivacy Guidelines on the Use of Criteria, Checks and Controls

Table of Contents

Introduction 4

Useful Definitions 4

Europrivacy Resources and Tools 5
- Europrivacy Useful Documents 5

Europrivacy Criteria, Checks and Controls Overview 6
- Homogeneous use of the Complementary Checks and Controls 6
- Europrivacy Innovative Hybrid Model of Certification Scheme 7

Preparation Phase 8
- Complying with the National Obligations 8
  - Applicants Based in the European Economic Area 8
  - Applicant Based outside the European Economic Area 8
  - National Criteria Extension 9
- Useful Resources for the Preparation 9
- Software Applications 9

Certification Process and Applicability of the Checks and Controls 10
- Preliminary Phase 10
- Assessment Phase - Certification Checks and Controls 10
- Regular Certification Process 11
- Certification Process Preparation 13

Europrivacy Criteria, Checks and Controls 14
- Criteria Focus on Legal Compliance 14
- Maintaining the criteria up-to-date 14
- Criteria Principles 14
- Available Sources 14

Criteria, Checks and Controls Applicability 15
- Applicants Differentiation 15
- Criteria Level 15
- Specific versus Generic Criteria 15
- Geographic Applicability 15

Criteria Format 16
- Example 16

Evaluation Methods 17
- Documentation and Files Review 17
- Interviews 17
- Examination 17
- Test 17

Use of Audit Results from Other Certification Bodies 18
Suggested Means of Evaluation and Verification 18
Recommended Order of Priority 19
Online Resources 19
Criteria, Checks and Controls Tables Structure 20
How to Fill the Table 22
Overall process 22
For each check and control 22
Indicative dashboard 22
Status Options 23
Regular Status cells 23
Sub-questions status cells 23

Introduction

These Guidelines provide advice on how to use and apply the Europrivacy Criteria, Checks and Controls. It provides recommendations, as well as a list of useful guidance and references for compliance assessment.

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."*

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

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.

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

Europrivacy Resources and Tools

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

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

Europrivacy Useful Documents

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

- EP-G.INTRO – Europrivacy Introduction and Overview
- EP-G.AP – Europrivacy Guidelines for Applicants to Certification
- EP-CS.1 – Europrivacy Certification Scheme General Specification and Requirements
- EP-C.ALL – Europrivacy List of Criteria, Checks and Controls
- EP-G.COM – Europrivacy Communication and Marketing Rules
- EP-G.STOA – Europrivacy Guidelines for Specifying the Target of Evaluation

Europrivacy Criteria, Checks and Controls Overview

Europrivacy has been designed to deliver homogeneous, consistent, and reliable certifications applicable to diverse categories of data processing activities. Beyond the core GDPR requirements, Targets of Evaluation may be subject to complementary national regulations. Particular application domains and technologies may also expose the data subjects to specific risks for their rights and freedoms. Consequently, Europrivacy is structured in a sequence of complementary criteria, checks and controls. Each set of criteria, checks and controls is identified with a distinct letter.

The most important list of criteria is:

- **G** **The Europrivacy GDPR Core Criteria**
  which gathers GDPR requirements applicable to all data processing.

It is complemented by three sets of complementary requirements:

- **C** **Complementary Contextual Checks and Controls**
  to assess compliance with the domain and technology specific requirements.
- **T** **Technical and Organisational Measures Checks and Controls**
  to assess the security measures set in place to protect the processed data.
- **N** **National Data Protection Obligations**
  with their complementary data protection requirements.

The following figure illustrates the complementarity between the Europrivacy GDPR Core Criteria and the complementary checks and controls.

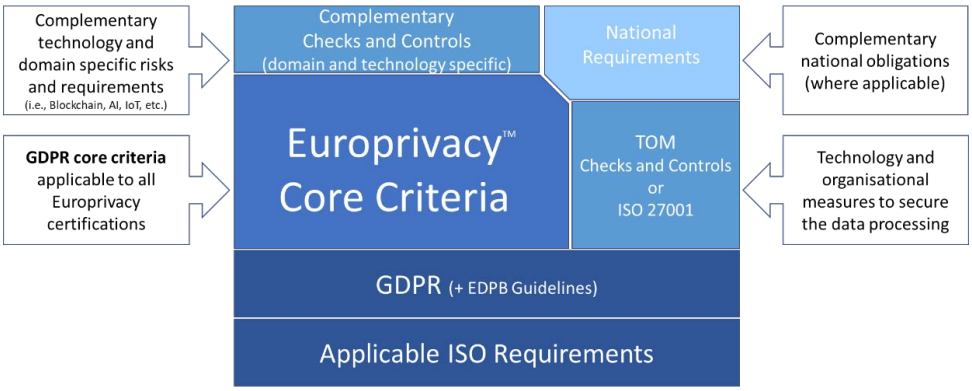


Figure 1 – Europrivacy Core Criteria and Complementary Requirements

Homogeneous use of the Complementary Checks and Controls

The applicability of the complementary checks and controls is determined by factual and objective factors, such as the nature and location of the data processing, as illustrated in Figure 2.

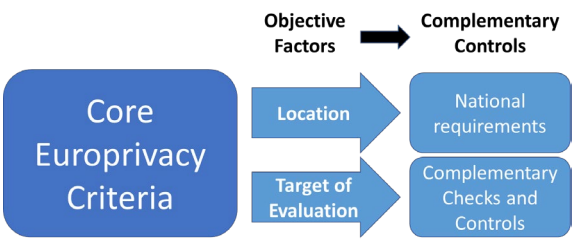


Figure 2 – Complementary controls determined by objective factors

Europrivacy Innovative Hybrid Model of Certification Scheme

Finding the adequate certification scheme that can adequately assess the compliance of diverse data processing and Targets of Evaluations may be a challenge. Universal certification schemes are cost-efficient for SMEs but do not assess technology-specific risks. On the other hand, specialised certification schemes may be optimal to assess specific categories of data processing, but they are inherently limited and cannot be extended to other categories of data processing. Moreover, they force companies to use diverse certification schemes and requirements with increased costs for SMEs.

Specialized certification schemes are often inadequate to certify data processing that tend to be increasingly complex by nature. Considering the example of a data processing collecting data through a smart watch (that is an Internet of Things devices), this kind of processing collects biometric data and send them through cellular network to a server in the cloud. There the data are usually analyzed by artificial intelligence algorithms in order to extract relevant information to be displayed on the smart phone application of the data subject. Using a specialized certification scheme for the Internet of Things would be adequate for the smart watch part, but would not cover the risks and requirements related to the use of Artificial intelligence, health data, or mobile phone applications. Similarly, a specialized certification scheme for processing in the cloud or based on Artificial Intelligence would face the same limitations by delivering only a partial, incomplete and potentially misleading assessment of compliance.

Europrivacy provides an **innovative hybrid model of certification** that combines the advantages of a universal certification scheme (with its comprehensive list of core criteria) together with complementary domain and technology specific criteria whose application is determined by the Target of Evaluation.

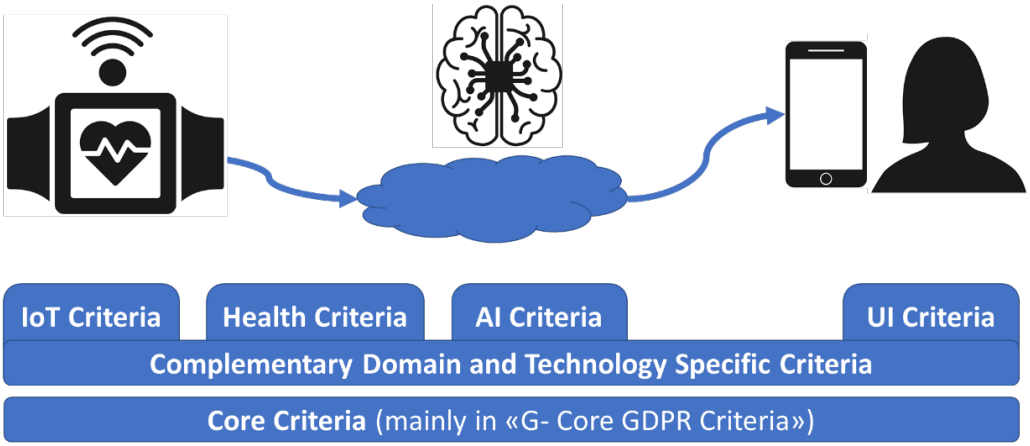


Figure 3 – Example of Europrivacy Hybrid Model applicability to a biometric data processing

Preparation Phase

A successful certification depends on the ability of the Applicant to document the compliance of its data processing activities to be certified with the applicable data protection regulations. The Journey to a successful Europrivacy Certification is quite simple:

Figure 4 – Smart Journey to Certification

Complying with the National Obligations

Each country has several specific national laws and regulations that may impact and extend the requirements for data protection. The GDPR requires that 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.

Applicants Based in the European Economic Area

Applicant requesting certification from the European Economic Area 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 complementary national data protection regulations of their country. This assessment is delivered as a written report named "**National Obligation Compliance Assessment Report**" (NOCAR).

By default, the NOCAR is expected to assess the compliance of the Target of Evaluation with the regulations of the EU country where the Applicant is headquartered or from which it effectively manages the data processing to be certified. Of course, nothing prevents the Applicant to extend the NOCAR to additional jurisdictions.

The NOCAR can be prepared by internal or external experts with adequate knowledge of the applicable regulations. The DPOs of the Applicant can produce the NOCAR to the condition that they preserve their independence and do not take the responsibility of the Applicant.

Europrivacy provides **National Data Protection Obligations Profiles** for each European country, with a list of particularly important national requirements to be addressed when assessing the conformity of the Target of Evaluation with national obligations. These lists are subject to changes according to the evolution of the national legislations and to comments received from the National Supervisory Authorities. The identified obligations must be taken into account by the legal expert in charge of preparing the NOCAR. It aims at ensuring that these requirements are not forgotten by the legal expert when assessing the conformity, but the assessment shall not be limited to this list and it shall consider all applicable national regulations.

Applicant Based outside the European Economic Area

Applicant requesting certification from outside the European Economic Area do not need to prepare a NOCAR.

National Criteria Extension

The Applicant can opt to extend the normative scope of its certification by using, where available, a Europrivacy national criteria Extension. The Extensions are made available in the Europrivacy Community and Resources website. Each Extension provides a set of additional criteria that the Auditor will assess when performing its audit to check compliance with these complementary requirements. It enables to deliver certifications that address not only compliance with the GDPR obligations but also with complementary national obligations. Some of these extensions may be also formally recognised in the corresponding jurisdiction.

Useful Resources for the Preparation

In order to support the preparation phase, ECCP provides a series of Europrivacy templates, reference documents, and tools that can be used to prepare and facilitate the certification process. All these resources are made available through the Welcome Pack and the Europrivacy Community website: https://community.europrivacy.com

- **Europrivacy Guidelines for Applicants**
- **Europrivacy Certification Application Form**
  This form enables to formally specify the Target of Evaluation to be certified.
- **A - Application and Target of Evaluation – Preliminary Checks and Controls**
  This checklist enables to assess the adequacy of the Target of Evaluation specification with the guidelines established by the EDPB.
- **D - Documentation Checklist**
  This checklist aims at facilitating the collection of documentation and at ensuring that the Audit team will have access to the required documentation.
- **P - Policy and Procedures Checklist**
  This checklist enables to check if the policies and procedures in place are sufficiently comprehensive to satisfy the Europrivacy requirements.
- **National Obligations Conformity Assessment Report (NOCAR) template**
- **N - National Data Protection Obligations Profiles**
  These profiles include references to the most important national obligations that complement the GDPR. These obligations must be respected by the Applicants based in the EEA. These lists are informative, but they must be taken into account by the legal expert preparing the NOCAR.
- **DPO Statement template**

The Applicants are encouraged to documenting the compliance of their Target of Evaluation with the applicable Europrivacy criteria, checks and controls used for the assessment (see next pages) in order to internally validate their compliance and readiness. Once the Applicant is ready to be certified, it shall apply to a qualified certification body with a clearly specified Target of Evaluation.

Software Applications

In addition to the resources available in the Europrivacy Community and resources website, several Europrivacy official partners provide software application that have integrated the Europrivacy list of checks and controls. The list of official partners providing solutions is available on the Europrivacy website in the section “Technology Provider”: https://europrivacy.com/en/partners/list

Certification Process and Applicability of the Checks and Controls

The Europrivacy conformity assessment is organised in a well-structured sequence of criteria, checks and controls, as illustrated in Figure 4 below.

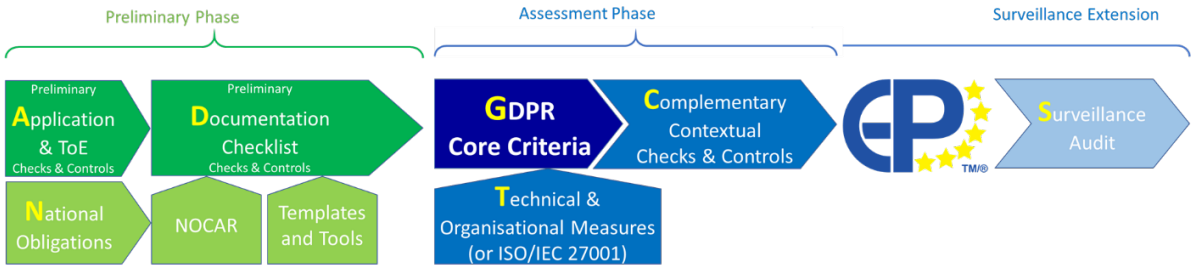


Figure 5 – Sequence of Europrivacy Criteria and Complementary Checks and Controls

Preliminary Phase

The preliminary phase aims at ensuring that the Target of Evaluation is ready to be assessed:

- **A** **Application and Target of Evaluation – Preliminary Checks and Controls**
  The 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 can be prepared by the Applicant but must be validated by the Certification Body before starting the assessment process.

- **D** **Documentation Validation**
  The Documentation checklist aims at facilitating the collection of documentation and at ensuring that the Audit team will have access to the required documentation. It is made available as a Word form that should be completed by the Applicant. Once completed, it must be validated by the Lead Auditor before starting the assessment.

The adequacy of the Target of Evaluation and available documentation should be validated by the Lead Auditor before starting the assessment process itself.

Assessment Phase - Certification Checks and Controls

The following checks and controls are used for assessing the conformity of the Target of Evaluation with Europrivacy. The Applicant can prepare evidence to satisfy the various criteria, but the formal validation is under the exclusive responsibility of the Certification Body:

- **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 obligations contained in the GDPR. They ensure that all Europrivacy certifications guarantee a high level of conformity with the GDPR. This list is mandatory for all certifications.

- **C** **Complementary Contextual Checks and Controls**
  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. This list is mandatory for each and every certification.

  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 and must assess and verify all the subsets 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.

- **T** **Technical and Organisational Measures (TOM)**
  Europrivacy certification requires that adequate technical and organisational measures are in place to protect the processed data. The Technical and Organisational Measures (TOM) Checks and Controls aim at assessing the conformity of the measures set in place by the Applicant to secure and protect the processed data.

  If the Target of Evaluation does not include any High-Risk Data Processing (as defined in the scheme), the TOM checks and controls can be replaced by a valid ISO/IEC 27001 certification covering the Target of Evaluation.

- **S** **Surveillance Audit Complementary Checks and Controls**
  Europrivacy has specified a few complementary checks and controls to be applied when performing Surveillance or Recertification audits in order to assess obligations specific to already certified data processing, such as the obligation to provide information on the certified data processing in the languages of the member States.

Additional resources:

- **NC** **List of Non-conformities**
  This template is to be used by the Certification Body for reporting and listing the identified non-conformities that the Applicant must address to be certified. Alternatively, the Certification Body can use its own templates to report non-conformities.

- **Z** **Checklist for certificate publication**
  This informative checklist is made available to the Certification Body to ensure that all administrative requirements are met before delivering a Europrivacy certificate.

The following table summarises the applicability of the various lists of checks and controls.

ID	List of Checks and Controls	Status	Lead	Alternative
A	**Application and Target of Evaluation**	**Mandatory**	**CB**	**No**
D	**Documentation Validation**	**Informative**	**App. & CB**	CB Management System
G	**GDPR core criteria**	**Mandatory**	**CB**	**No**
C	**Complementary and Contextual Checks and Controls**	**Mandatory**	**CB**	**No**
T	**Technical and Organizational Measures (TOM)**	**Mandatory**	**CB**	ISO 27001/27701
N	**National Data Protection Obligations Profiles**	**Informative**	**CB**	Legal assessment
S	**Surveillance Audits**	**Mandatory**	**CB**	**No**
Z	**Certificate Publication checklist**	**Informative**	**CB**	CB Management System
NC	**List of Non-conformities**	**Mandatory**	**CB Only**	CB Management System
Complementary Checklists and Resources				
I	Data Processing Inventories templates	Informative	App. & CB	Data processing registry
E	Evaluation of Datasets	Informative	Applicant	Compliance Solution
P	Policy and Procedures Checklist	Informative	Applicant	Compliance Solution
M	Matrix of Applicability	Informative	App. & CB	Compliance Solution
	Other templates	Informative	Applicant	Any

Table 1 – Applicability of the Europrivacy Lists of Checks and Controls

Regular Certification Process

The following drawing illustrates a regular certification process with the use of the corresponding lists of Criteria, Checks and Controls available in the Europrivacy Community and Resources website.

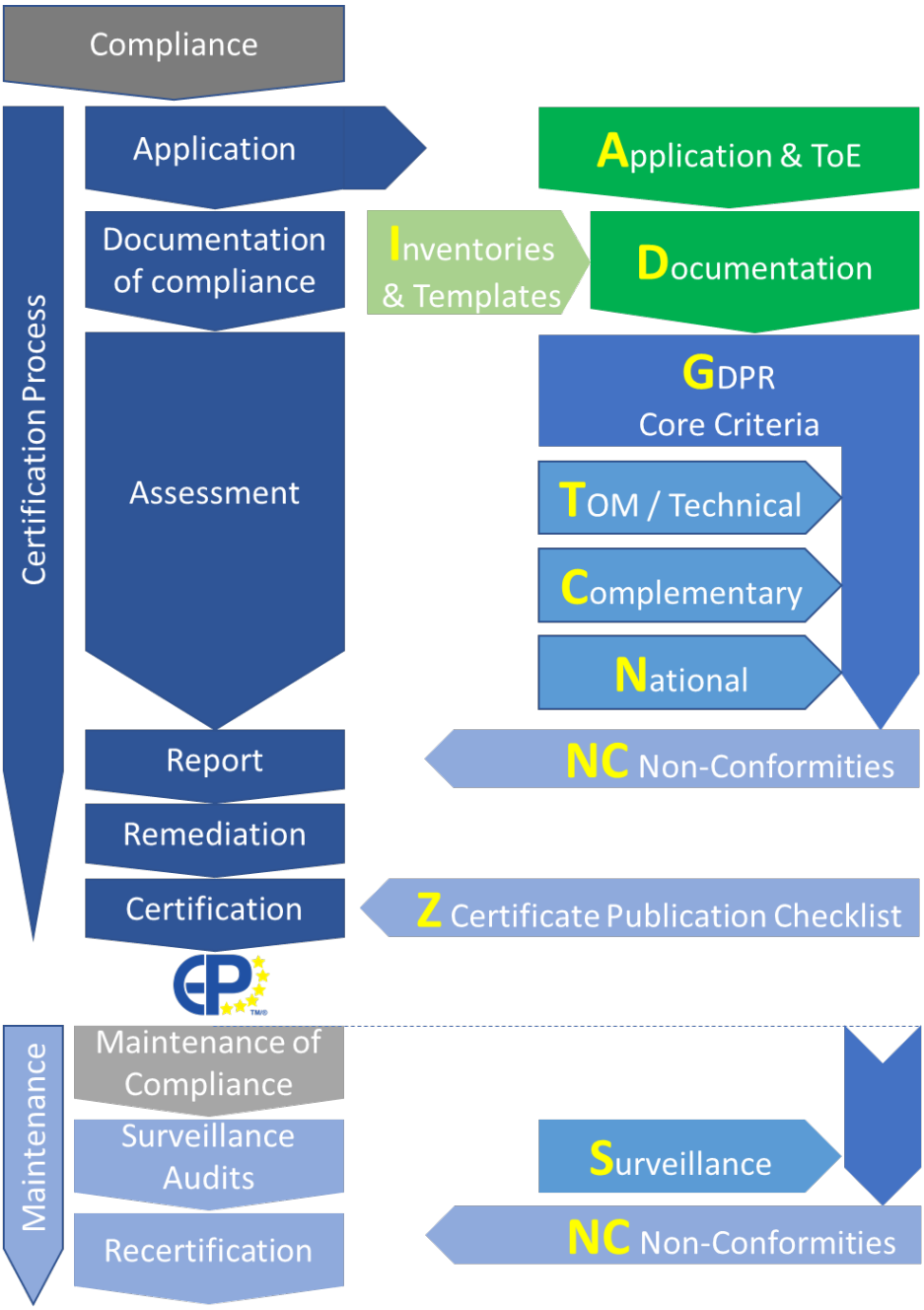


Figure 6 – Europrivacy Regular Certification Process

Certification Process Preparation

The Applicant and/or its Consulting Firm can also prepare and document in advance the conformity of its data processing with Europrivacy criteria. In such cases, the process can be adapted as follow where the green blocks (I, D, A) can be prepared in advance by the Applicant (or its consulting firm) and validated by the Certification Body. The preparation can extend to pre-documenting the evidence of conformity with the core criteria (G) as well as with the complementary checks and control (T, C, N, and S if applicable).

A good preparation will substantially accelerate the certification, reduce the uncertainty with regards to the result of the certification, and may reduce its cost. The preparation can be made manually or with conformity assessment tools.

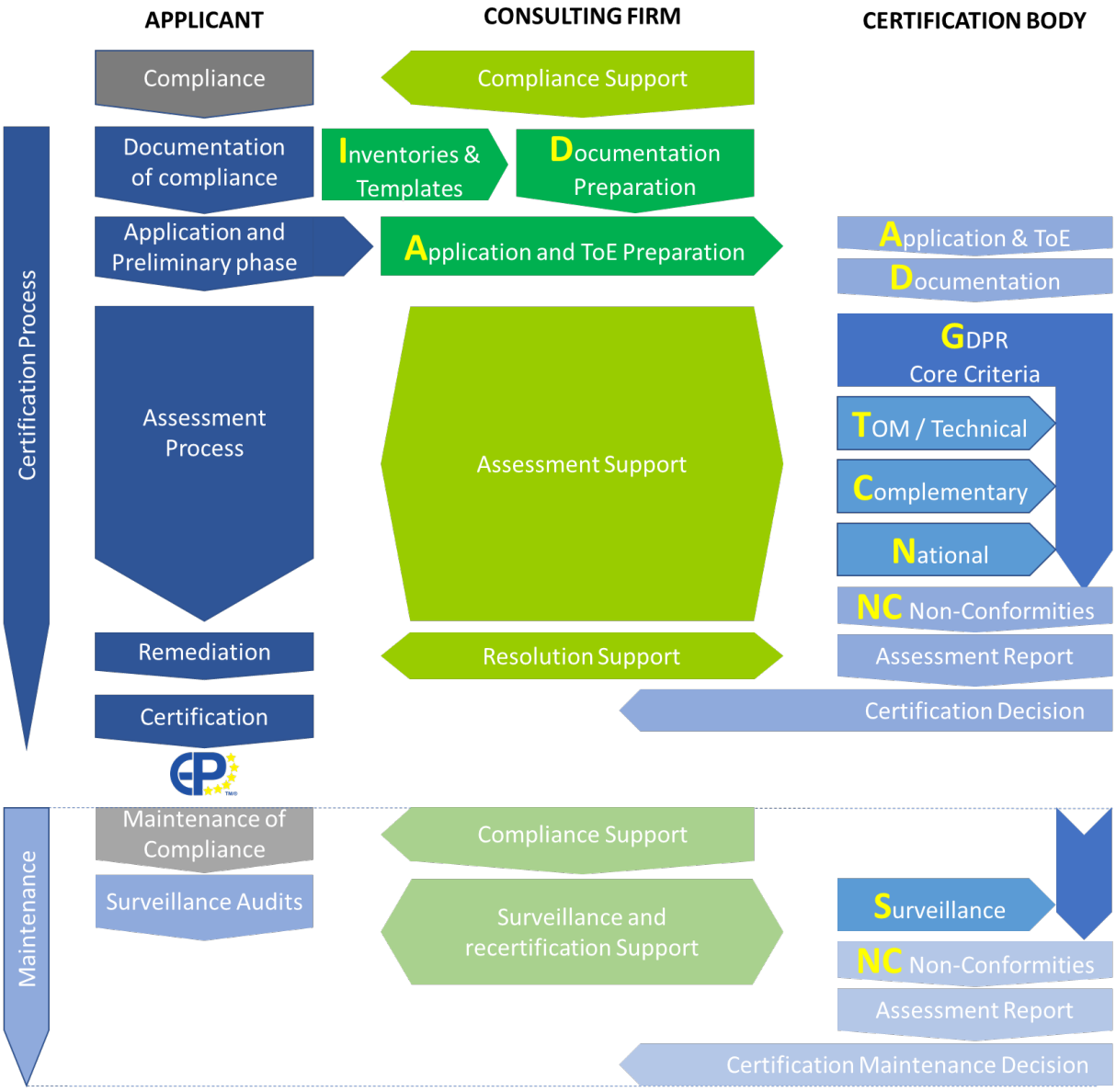


Figure 7 – Europrivacy Prepared Certification Process

Europrivacy Criteria, Checks and Controls

Criteria Focus on Legal Compliance

In line with Art. 42 of the GDPR, Europrivacy criteria are specified *"to provide an independent, impartial, and reasonable assurance level of data processing compliance with the European General Data Protection Regulation and, where applicable, with complementary data protection requirements, such as national regulations or domain specific requirements."*

The criteria aim at assessing the compliance and at preventing the certification of any data processing that would not be compliant with the GDPR. That is why the criteria tend to cover all the GDPR obligations, and many requirements are assessed by clusters of complementary criteria.

Europrivacy focuses on the core legal obligations of the GDPR and intends to avoid adding unnecessary constraints that would exclude GDPR compliant data processing from certification. For instance, adding additional requirements for how *"data protection by design"* shall be implemented by the Applicant, would imply that an SME which already complies with the GDPR requirements will have to redo the process according to our own specific views, with additional and dissuasive costs for SMEs.

Maintaining the criteria up-to-date

The Europrivacy criteria, checks and controls are maintained by the Europrivacy International Board of Experts of ECCP to take into account the evolution of the jurisprudence, national legislations, the EDPB publications, and the evolution of the technology.

Criteria Principles

Criteria must avoid the risk of subjectivity. Each criterion shall be worded in a manner that limits the room for interpretation. Each criterion, check and control has been specified to be:

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

Available Sources

The Europrivacy criteria, checks and controls are made available through the Welcome Pack and the Europrivacy community website in various forms, including pdf files and Word templates to facilitate compliance assessment.

The Europrivacy criteria can also be used through conformity assessment software and solutions developed by official partners (more information on Europrivacy website). The specific format of Europrivacy criteria, checks and controls has been optimized to facilitate their parsing and automated integration into software and applications.

Criteria, Checks and Controls Applicability

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

Applicants Differentiation

Some criteria are applicable to all Applicants, while others are applicable only to Data Controllers or to Data Processors. Europrivacy uses the following codes to differentiate the Criteria applicability according to the role of the Applicant in the Target of Evaluation:

C Criteria applicable to Data Controllers only.

P Criteria applicable to Data Processors only.

CP Criteria applicable to both Data Controllers and Data Processors.

Criteria Level

Each Europrivacy criteria is categorised in one of the following three main categories:

A **Mandatory by default for all certification processes**. Level A criteria must always be assessed whatever the Target of Evaluation is.

B Not required for certifying simple data processing, **but mandatory for certifying any High-Risk Data Processing, defined as data processing that:**

- processes **special categories of personal data** or data relating to criminal convictions, or;
- specifically **targets personal data of minors of age**, or;
- is likely to result in a **high risk for the rights and freedom of natural persons**[1].

E **Exemptions**: for determining if an exemption to a criterion can be justified. The application of level E criteria is reserved to check if a claimed exemption is justified.

Specific versus Generic Criteria

Criteria are differentiated between "Specific" and "Generic" criteria. Specific Criteria are distinct for each and every Target of Evaluation. Generic Criteria can be common to several Targets of Evaluation. For instance:

- Assessing the lawfulness of a data processing (i.e. G.1.1.1) is specific and different for each and every Target of Evaluation. As a consequence, it will be categorised as "Specific".
- Assessing the designation of a DPO (i.e. G.9.1.1) is common to several Targets of Evaluation. As a consequence, it will be categorised as "Generic".

The interest of this categorisation is to enable the Applicants and their Implementers to enhance the preparation process by reusing the documentation of G Criteria for several Targets of Evaluations.

Geographic Applicability

In view of the extension of applicability of Europrivacy Criteria to non-EEA jurisdictions, the Core Criteria also distinguish criteria required to certify Data Importers based outside of the European Economic Area (EEA) that are not directly subject to the GDPR but are willing to use certification as a mechanism for international data transfer[2], where:

R indicates that the criterion **is required** for Data Importers based outside of the EEA;

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

[1] The Certification Body shall consider the related guidelines of the EDPB in that matter.

[2] Non-EEA Applicants are subject to the GDPR when directly collecting personal data in the EEA (Art. 3 GDPR). The applicability of Europrivacy Criteria to non-EU Applicants is under review and subject to EDPB approbation.

Criteria Format

Criteria are formulated as "shall" clauses which are articulated with clear logical relations by using the words "AND", "OR", and "IF…THEN:" in upper cap letters. It enables a very clear wording and structuration of the requirements. It also eases the integration of the Europrivacy criteria in self-assessment software and applications, enabling Applicants to prepare their certification and to save costs by reducing the audit time.

Conditional Clauses: Conditional clauses enable to restrict the applicability of a criteria to certain conditions. They start with the word "**IF**" upper cases and ends with "**THEN:**" in upper cases. If the conditions are applicable to the data processing, then the related subsequent criteria shall be evaluated. If the condition does not apply, then the related subsequent criteria can be skipped.

Requirement Clause: The criteria are specified in one or several clauses specifying formal requirements, named "Requirement Clause". A criterion can contain several Requirement Clauses. Each major Requirement Clause starts with a letter in upper case and a parenthesis, starting with letter A: **A)**, **B)**, etc.

Boolean Relations: When criteria include several Requirement Clauses, a Boolean Relation term in upper cap ("**AND**" or "**OR**") shall be specified between each Requirement Clause.

Sub-requirements Clauses: Each major clause may optionally contain a set of Sub-requirements. The list of Sub-requirements shall be preceded by à column ("**:**"). Each Sub-requirement shall:

- start with the letter of the corresponding major Requirement clause in lower cap, followed by a dot and a number (starting with 1) (i.e., "**a.1)**";
- include a Boolean relation term in upper caps between parenthesis "**(AND)**" or "**(OR)**" except for the first Sub-requirement of the list;
- end with a semi-column ("**;**") if the Sub-requirement is followed by another Sub-requirement, or by a dot if it is the last Sub-requirement of the list.

Example

Here is an example of a regular standard Criteria structure:

> **IF** ……., **THEN:**
>
> **A)** [Requirement Clause A]**.**
>
> **AND**
>
> **B)** [Requirement Clause B] where**:**
>
> **b.1)** [Sub-requirement b.1]**;**
> **b.2) (OR)** [Sub-requirement b.2]**;**
> **b.1) (OR)** [Sub-requirement b.3]**.**

Here is an example of a formal criteria (G.1.3.1) from the Europrivacy GDPR Core Criteria:

> *"IF the Target of Evaluation includes Information Society Services offered directly to children below 16 years old THEN:*
>
> *A) The applicable limits of age for consent shall be clearly communicated to potential new data subjects involved in the data processing;*
> *AND*
> *B) there shall be a procedure and/or a mechanism:*
> *b.1) to request the age of data subjects that are minor of age;*
> *b.2) (AND) to request the consent of the holder of the parental responsibility for minor below the age of consent."*

Evaluation Methods

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

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

The assessment of conformity can include activities such as documentation and files review, sampling, testing, Examination, interviews, and audits, as appropriate. In accordance with ISO/IEC 17007, *"it should be left to the users of the normative document to decide what conformity assessment activity (if any) will be utilized, who will carry out the conformity assessment and under what conditions."*

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

For each Criterion, the Auditor shall use one or more means of evaluation, until sufficient evidence is collected to determine if the requirements are met.

Documentation and Files Review

Documentation review refers to the review by the Auditor of documentation, files, and records that are relevant to assess the compliance of the Target of Evaluation with Criteria, Checks and Controls.

Section 8.2 of the Europrivacy Certification Scheme General Specification and Requirement (EP-CS.1) provides more details on how to perform a documentation review.

Interviews

Interview consist in meeting relevant stakeholders, such as the DPO, to ask questions and request clarifications. The interview can be performed through face-to-face meeting, online and remote meetings, or other relevant communication means such as phone calls or written questions.

Examination

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

Section 8.4 of the Europrivacy Certification Scheme General Specification and Requirement (EP-CS.1) provides more details on how to perform Examinations and on-site assessments.

Test

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

Section 8.3 of the Europrivacy Certification Scheme General Specification and Requirement (EP-CS.1) provides more details on how to perform tests, including sample analysis.

Use of Audit Results from Other Certification Bodies

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

Suggested Means of Evaluation and Verification

Criteria are followed by suggested means of verification that aim at guiding the assessment work of the auditor. For instance, criterion G.5.3.3 criterion requires that:

> *"A) There shall be a registry and/or documentation of instructions communicated by the Controller to the Processors (or where applicable by the Processor to the Subprocessors)"*

It provides the following suggested means of verification:

- *"Examination,*
- *Data Processing instructions records,*
- *Interview of CISO or DPO."*

The suggested means of verification are intended to guide and homogenize auditing practices. However, as specified in ISO/IEC 17007, *"it should be left to the users of the normative document to decide what conformity assessment activity (if any) will be utilized, who will carry out the conformity assessment and under what conditions."* In conformity with ISO/IEC 17007 (referred to by ISO/IEC 17067) and in order to address a vast diversity of data processing activities and implementation as illustrated in Annex I, the auditor can still decide and select the best means of evaluation.

Regardless of the means of evaluation chosen, the auditor must, for each applicable criterion, determine with sufficient evidences that all the specified requirements are met. Europrivacy requires that: ***"Each applicable criterion, check and control shall be sufficiently completed and documented with adequate evidence to assess the conformity with the requirements."*** (Section 6.2) and that ***"The Auditor shall use the most efficient means of evaluation and collect sufficient evidences to determine with a high level of confidence the conformity or non-conformity of each applicable Criterion."*** (Section 6.8.1). **For each Criterion, the Auditor shall use one or more means of evaluation, until sufficient evidence is collected to determine if all the requirements are met**. The Auditor shall be able to demonstrate that its findings are based on clear evidence.

Auditors shall select and use the means of evaluation that are the most efficient and reliable. When applying a means of evaluation, three cases may occur:

A. It delivers sufficient evidence that the requirements of the criterion are satisfied to determine conformity;
B. It delivers sufficient evidence that the requirements of the criterion are satisfied to determine a non-conformity;
C. It does not deliver sufficient evidence to determine whether the criterion is satisfied or not satisfied, then the Auditor must continue its assessment with another means of evaluation until it gathers sufficient evidences to determine if the target of evaluation complies or not with the requirements specified in the criterion.

If despite the use of several means of evaluation, the assessment process ends without sufficient evidence of conformity, the criterion shall be qualified with a non-conformity.

Recommended Order of Priority

By default, the following order of priority is recommended:

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

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

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

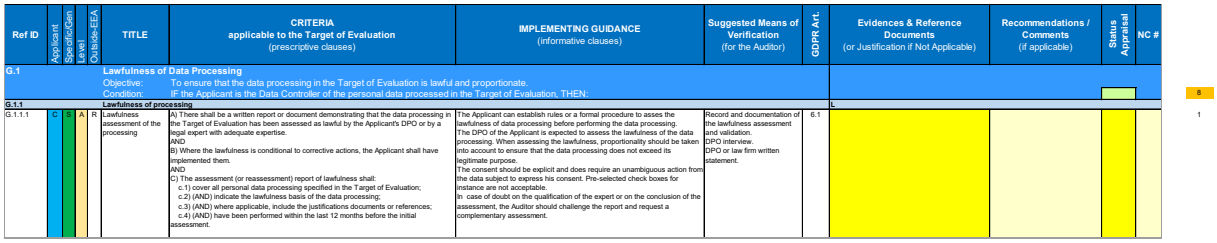
Online Resources

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

Criteria, Checks and Controls Tables Structure

The Europrivacy Criteria, Checks and Controls may be available in different forms, such as pdf documents, pdf forms, Word documents, Excel files, software solutions or Software as a Service. They are usually structured and presented in the form of lists or tables.

We will use the Excel version of the Europrivacy Criteria, Checks and Controls as an example. The lists of Criteria, Checks and Controls are organised in several tabs. The tab labelled "Core GDPR" gathers the core criteria, checks and controls that shall be addressed in each and every audit.



Ref ID	Applicant	Specific/Gen	Level	Outside-EEA	TITLE	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	IMPLEMENTING GUIDANCE (informative clauses)	Suggested Means of Verification (for the Auditor)	GDPR Art.	Evidences & Reference Documents (or Justification if Not Applicable)	Recommendations / Comments (if applicable)	Status Appraisal	NC #
G.1					Lawfulness of Data Processing	Objective: To ensure that the data processing in the Target of Evaluation is lawful and proportionate. Condition: IF the Applicant is the Data Controller of the personal data processed in the Target of Evaluation, THEN:							
G.1.1					Lawfulness of processing					L			
G.1.1.1	C	S	A	R	Lawfulness assessment of the processing	A) There shall be a written report or document demonstrating that the data processing in the Target of Evaluation has been assessed as lawful by the Applicant's DPO or by a legal expert with adequate expertise. AND B) Where the lawfulness is conditional to corrective actions, the Applicant shall have implemented them. AND C) The assessment (or reassessment) report of lawfulness shall: c.1) cover all personal data processing specified in the Target of Evaluation; c.2) (AND) indicate the lawfulness basis of the data processing; c.3) (AND) where applicable, include the justifications documents or references; c.4) (AND) have been performed within the last 12 months before the initial assessment.	The Applicant can establish rules or a formal procedure to asses the lawfulness of data processing before performing the data processing. The DPO of the Applicant is expected to assess the lawfulness of the data processing. When assessing the lawfulness, proportionality should be taken into account to ensure that the data processing does not exceed its legitimate purpose. The consent should be explicit and does require an unambiguous action from the data subject to express his consent. Pre-selected check boxes for instance are not acceptable. In case of doubt on the qualification of the expert or on the conclusion of the assessment, the Auditor should challenge the report and request a complementary assessment.	Record and documentation of the lawfulness assessment and validation. DPO interview. DPO or law firm written statement.	6.1				

8
1

Figure 8 – Table structure overview

The Criteria tables are usually comprised of the following columns:

A. **Ref ID**: provides a unique and distinct identifier for each and every Criterion, Check and Control.
B. **Applicant**: defines to whom the Criterion, Check or Control is applicable to:
   - C = applicable to Data Controllers only.
   - P = applicable to Data Processors only.
   - CP = applicable to both Data Controllers and Data Processors.
C. **Specific**: clarifies whether the check and controls are specific or generic:
   - S = Specific and distinct for each and every Target of Evaluation.
   - G = Generic and common to several Targets of Evaluation.
D. **Level**: specifies whether the check and control are:
   - A = mandatory by default.
   - B = not required for simple data processing, but mandatory for high-risk data processing.
   - E = required to justify an exemption to criteria.
E. **Outside-EEA**: specifies whether the Criterion, Check and Control is required for Data Importers based outside of the EEA:
   - R = indicates that the criterion is required for Data Importers based outside of the EEA;
   - NR = indicates that the criterion is not required for Data Importers based outside of the EEA.
F. **Title**: indicates the title of the check and control.
G. **Criteria**: describes the formal requirement to be implemented by the Applicant and assessed by the auditor. Criteria are prescriptive clauses to be respected by the Applicant.
H. **Implementing Guidance**: provides complementary information and guidance to Applicants on the good practices to be implemented for complying with the criteria. The implementing Guidance are informative clauses.
I. **Suggested Means of Verification:** provides guidance to the auditor on the usual sources where the information is located. It is indicative and the auditors can choose any alternative relevant source of information.
J. **GDPR Art.**: provides an indication of the main GDPR article related to the check and control.
K. **Evidence & Reference Documents (or Justification where the criteria is considered as Not Applicable)**: has to be filled by the Auditor with a clear indication of the evidence that were

considered for determining the conformity or non-conformity of the Object to be certified with the check and control. Except for checks and controls that are determined as being non-applicable to the certification, this field is compulsory and shall be systematically completed with care, as it serves as the foundation for the assessment of the conformity.

L. **Recommendations / Comments (if applicable)**: enables the Audit Team to identify some issues or elements to be addressed by the Applicant.
M. **Status**: is used by the Auditor to qualify the status of the finding on the check and control.
N. **NC #**: serves to indicate the identifying number of an identified non-conformity.

The checks and controls are clustered in different criteria in line with the GDPR structure.

Vertically, the table is structured as follow:

1. **Header (in dark blue)**: provides the title and function of each column.
2. **Top Sections (in blue)**: indicates the start of a main section.
3. **Subsections (in light blue)**: indicates the start of a subsection inside a main section.
4. **Checks and controls**: are identified by the white background of their cells in the Mandatory requirement column.
5. **Preliminary Checks**: are identified by the light green background of their cells in the Mandatory requirement column.

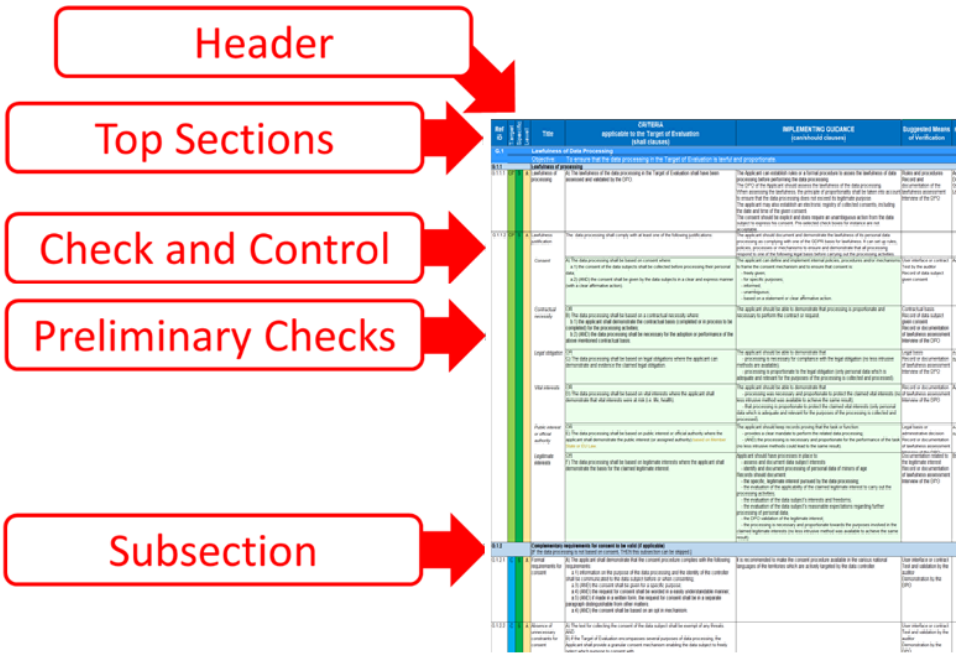


Figure 9 – Vertical structure

How to Fill the Table

When assessing the checks and controls of a Section, the process is as follow:

Overall process

1. The Auditor shall perform the requested checks and controls in each one of the Top Category.
2. When performing the assessment of a Top Category, the Auditor shall start g through the list of checks and controls.
3. If the check and control is linked to subsequent preliminary checks, the Auditor shall start by completing the preliminary checks first in order to determine the status of the related check and control.

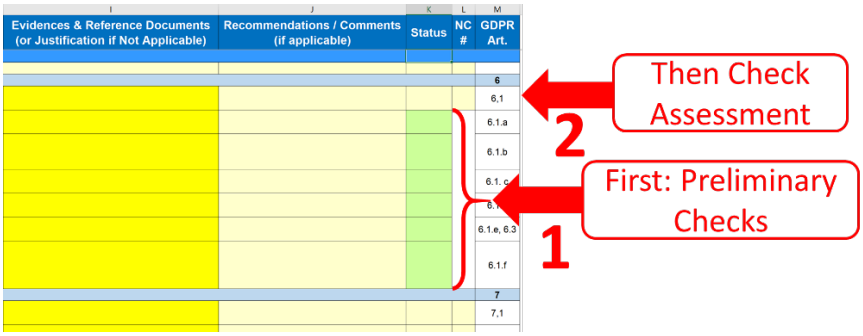


Figure 10 – Preliminary checks process

For each check and control

4. **At each check and control, the Auditor shall look for and provide clear evidence(s) in the corresponding cell**.
5. Where applicable, the Auditor can complement the found evidence with comments and suggestions regarding issues to be addressed by the Applicant to be included in the corresponding cell ("Recommendations / Comments" column). The Auditor can identify issues and clarify requirements, but it shall not provide guidance on how to resolve the issue that could be perceived as a consulting service and would create an impartiality issue for subsequent assessments.
6. **According to the found evidence(s), the Auditor shall determine the status of the check and control** (more details provided below).
7. **If a non-conformity has been identified, it shall be added to the list of non-conformities with a clear identifier** (number or letter) to be indicated in the "NC#" column.

Indicative dashboard

8. In the Excel file, a Dashboard is provided at the bottom of the table, providing a summary of the status of the checks and controls results.

Status Code		Meaning / Explanation	Tot	%
OK		Conformity: Requirement has been **controlled** and appears to be respected and no non-conformities have been identified.	2	22%
OK+		Good practice moving beyond simple conformity	2	22%
Obs		Observation	1	11%
			5	56%
Min NC		A **Minor Non-Conformity** (non-critical) has been identified.	1	11%
Maj NC		A **Major Non-Conformity** (critical) has been identified.	1	11%
?		**Missing Information / Don't know**	0	0%
NA		Control is **Not Applicable** for the targeted certification	2	22%
			9	

Figure 11 – Dashboard

Status Options

Regular Status cells

The Status field in the yellow cells offers a list of several options, corresponding to different statuses:

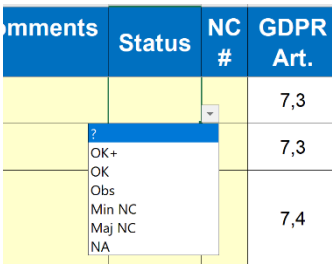


Figure 12 – Default status list

The meaning of each option is detailed in the following table:

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

Table 2 – Regular Status option

Sub-questions status cells

Some cells correspond to complementary questions used to assess the status of a check and control. These background colour of the corresponding cells for the Status is green instead of yellow. The Status field in the green cells offers a simplified list of options, corresponding to different statuses:

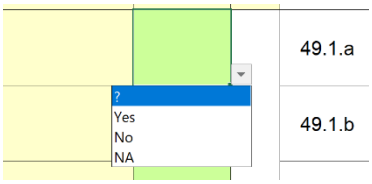


Figure 13 – Sub-question status list

The meaning of each option is detailed in the following table:

Status Code	Meaning / Explanation
?	**Missing Information / Don't know**
Yes	The answer is Yes
No	The answer is No
NA	Control is **Not Applicable** for the targeted certification

Table 3 – Sub-question status