Europrivacy.com
Privacy Audit and Certification

Europrivacy™® Main Criteria for Data Importer Certification under Art. 46 GDPR

Subject to copyrights

Identifier:	EP-C.ALL.DI.P
Version:	v2.0 / also referred to as v.82
Date:	20 January 2026
Publication status:	Restricted use, subject to IPR
Websites:	https://www.europrivacy.com www.eccpcenter.org
Contact:	contact@europrivacy.com

All rights reserved, European Centre for Certification and Privacy ©
Europrivacy is an international trademark registered in several jurisdictions.

Introduction

Intellectual Property Rights Notice

Like ISO standards, Europrivacy, **including its criteria and documentation, are subject to intellectual property rights, including trademarks and copyrights. This document is provided for reading purposes only** and is intended solely to inform interested parties about the Europrivacy criteria. Any copying, reproduction, extraction, distribution, or use (including for derivative work and for artificial intelligence purposes), without express prior written authorisation delivered by the European Centre for Certification and Privacy (ECCP) is prohibited. All rights, including Text and Data Mining (TDM) rights, are expressly reserved.

You can access a licensed version of the Europrivacy criteria with implementation guidelines, as well as all support documentation for the certification, including templates, handbooks, FAQ, and other online resources, on the Europrivacy Community and Resources website: https://community.europrivacy.com

Europrivacy European Data Protection Seal pursuant to Art. 42 GDPR

The Europrivacy Certification Scheme has been developed to assess the compliance of personal data processing operations of Data Controllers and Processors, including in products and services, with the obligations of the European General Data Protection Regulation (GDPR). The present document contains the Europrivacy Certification second version (also identified as v82) of criteria approved by the European Data Protection Board (EDPB) in April 2026 to serve as European Data Protection Seal pursuant to Article 42 of the GDPR. This new version enables to certify data processing activities of Data Controllers and Processors established inside and outside of the European Economic Area (EEA). The Europrivacy certification scheme has also been approved by European Accreditation (EA). In parallel, its international and geographically neutral version, Interprivacy, has been approved by the International Accreditation Forum (IAF) now renamed Global ACI. Europrivacy is maintained by the European Center for Certification and Privacy in Luxembourg and is supported by a global ecosystem of qualified partners.

What Can Be Certified

Europrivacy can be used to check, document, and certify GDPR compliance of all sorts of data processing activities, including in products and services. It can be applied to both data controllers and processors and has been designed to adequately assess data processing using innovative technologies such as artificial intelligence, blockchain, and Internet of things.

Why Certifying

Europrivacy enables to protect the rights and freedom of the data subjects, to reduce risks for the applicant and its partners, to support and facilitate international data transfers, to simplify and value compliance, to reduce the due diligence effort and costs. It also provides a structured and credible way to demonstrate accountability, transparency, and trustworthiness to clients, partners, supervisory authorities, and other stakeholders. Certification can also be used when selecting data processors to reduce the surface of risks, efforts, and costs for the data controllers.

Criteria Structure

The present document includes:

- the **preliminary checks and controls for Data Importers** (ADI) to ensure that the conditions are met to start the formal certification assessment;
- the **Europrivacy core criteria for Data Importers** (GI) used to assess compliance with the GDPR;
- the **Technical and Organizational Measures** (T) complementary criteria to assess the adequacy of information security in place.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

Each criterion includes information between parenthesis on:

To whom it applies: where C means the criterion is applicable only if the applicant is acting as a Data Controllers; P means it is applicable only to applicant acting as Data Processors; and CP means it is applicable to both Data Controllers and Data Processors.

The level of the criterion: where A means that the criterion is applicable by default to all data processing; while B means that it is applicable only if the target of evaluation is a high-risk data processing; and E means that it is applicable only where the Applicant claims an exemption specified in the GDPR.

The scope and potential for reusability of the criterion: where G refers to a criterion assessing a general obligation that is not data processing specific (i.e. the qualification of the DPO of the applicant), and S to a criterion that is assessing a data processing specific obligation (i.e. the lawfulness of a specific data processing).

Several criteria are subject to conditional clauses that are specified in the form "IF ….., THEN:". If the specified condition is not met, the related criterion or criteria are not applicable to the target of evaluation. To facilitate the reading, the conditional criteria are in grey colour.

Useful Resources

Europrivacy is also supported by comprehensive online resources, including:

- The Europrivacy public website with public information (europrivacy.com)
- The Europrivacy Community and Resources website that gathers all required documentation and resources to prepare and perform a certification, including criteria, implementation guidance, guidelines, FAQ, templates, etc. https://community.europrivacy.com
- The Europrivacy Academy website: that enables anyone to learn how to use and apply Europrivacy and get a formal qualification as implementer or auditor: https://academy.europrivacy.com

What is more, Europrivacy is supported by a large community of experts, as well as by a global ecosystem of qualified partners whose list is available on the Europrivacy public website to prevent any dependence or business lock in.

For more information, feel free to contact us.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

ADI APPLICATION & TARGET OF EVALUATION - PRELIMINARY CHECKS AND CONTROLS FOR DATA IMPORTERS

ADI.1 Application Form

ADI.1.1 Application Documentation

ADI.1.1.1 Application Form Control

A) The Application Form shall satisfy the following:

a.1) AND) The Applicant has clarified that it is acting as a Data Importer located outside of the EEA and not directly subject to the GDPR (in the sense of Art. 3(2) GDPR);
a.2) (AND) The Applicant is the Data Controller or Processor of the Target of Evaluation;
a.3) (AND) The country outside the EEA where the Applicant is established and whether the country benefits from an adequacy decision, for the purposes of the international transfer(s) covered by the Certification;
a.4) (AND) The Target of Evaluation relates to the processing of personal data subject to transfers processing operations;
a.5) (AND) The person of contact is clearly identified;
a.6) (AND) Information on potential consulting services involved in the Target of Evaluation during the last two years has been requested;
a.7) (AND) Information on potential valid and refused certifications encompassing the Target of Evaluation has been requested;
a.8) (AND) There is no apparent impartiality issue or conflict of interest;
a.9) (AND) The application form is complete and signed.

ADI.1.2 Monitoring and Recertification

IF the application concerns a surveillance audit or a recertification, THEN:

ADI.1.2.1 Previous report

A) The Applicant shall have provided the previous certification report

ADI.1.2.2 Communication material

A) The Applicant shall commit to provide access to all publications and communication material in which the Europrivacy certificate is used, including printed material, electronic documents (such as pdf files), and web pages.

ADI.1.3 Special Requirements for Data Importers located outside of the EEA

IF the Applicant is a Data Importer located outside of the EEA, THEN:

ADI.1.3.1 Contractually binding instrument

A) The Applicant shall confirm the existence of a model of contractually binding and enforceable commitments to apply the appropriate safeguards, including as regards data subjects' rights.

ADI.1.3.2 Data in transit

A) The Target of Evaluation shall clarify whether the processing of data in transit that is under the control of the Data Importer is included in the Application.

ADI.1.3.3 Certification agreement for Data Importers

A) The Applicant shall provide the information on:

a.1) the rules for the recording and investigation of complaints relating to compliance with the certification criteria;
a.2) (AND) explicit statements on the structure and the procedure for complaint management.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

ADI.2 Scope and Target of Evaluation

ADI.2.1 Target of Evaluation Specification (ToE)

ADI.2.1.1 ToE Information

A) The Target of Evaluation shall be clearly described and satisfy the following:
Processing description

a.1) the description of the data processing;
a.2) (AND) the purpose of the data processing, including the purpose of the international transfer(s);
a.3) (AND) the categories of data (such as special categories of data, data related to criminal convictions, etc);
a.4) (AND) the categories of data subjects (i.e. minors of age, employees, patients, etc);
a.5) (AND) the recipients of data or categories of recipients;
a.6) (AND) IF the Data Importer performs onward transfers of data to other third countries and international organisations, THEN the list of such third countries and international organisations involved in the Target of Evaluation;
a.7) (AND) whether data in transit in included in the Target of Evaluation;
a.8) (AND) Any exclusion of interdependent data processing from the Target of Evaluation shall be justified.

ADI.2.1.2 ToE Formal Specification

A) The Target of Evaluation shall be illustrated on a drawing or diagramme where:

a.1) All relevant data processing operations and systems shall be identified and described;
a.2) (AND) The Target of Evaluation shall be clearly delimited;
a.3) (AND) There shall be a clear indication of where the data processing starts and ends;
a.4) (AND) Where applicable, the interfaces of the data processing with independent processing operation shall be clearly identified.

ADI.2.1.3 ToE Clarity for data subjects

A) The Target of Evaluation shall be clearly understandable by the data subjects involved in the data processing.

ADI.2.1.4 Expertise adequation

A) The Certification Body shall have access to adequate expertise to assess the compliance of the Target of Evaluation.

ADI.2.1.5 ToE Condition for Applicants located in non-EEA countries

A) The Certification Body shall check:

a.1) the existence of a report on potential conflict of laws as specified in GI.1.1.5;
a.2) (AND) that the report concludes that the national law and practice of the non-EEA country does not hinder compliance with the Certification requirements.

AND

B) IF the report concludes that supplementary measures are required, THEN the Certification body shall assess if it is possible to have effective supplementary measures applied to address the conflict of law.

ADI.3 Contractual and Administrative Documentation

ADI.3.1 Contractual Documentation

ADI.3.1.1. Contractual clauses

A) The contractual procedure for the certification shall be complete and the Applicant shall have formally accepted:

a.1) to comply with the Europrivacy General Terms and Conditions and rules on the Certification Scheme Extention for Certifying Data Importers under Art. 46 GDPR;
a.2) (AND) to inform the Certification Body without delay of any change that would expose the certified Target of Evaluation to the breach of the applicable Certification requirements.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI EUROPRIVACY GDPR CORE CRITERIA FOR DATA IMPORTERS

All rights reserved. The content of this document is subject to intellectual property rights, including registered copyright and cannot be re-used, altered, adapted, copied or replicated in any format without explicit authorisation by the European Centre for Certification and Privacy ('ECCP'). The following criteria are complemented by complementary criteria and resources which can be accessed through the Europrivacy Community and Resources website.

GI.1 Lawfulness of Data Processing

GI.1.1 Lawfulness of processing

GI.1.1.1 Potential conflict of law with Applicants based in non-EEA countries *(GDPR Art. 6.1; 10) (CP; S; A)*

A) There shall be a written assessment of the law and practices of the Applicant's country, performed on behalf of the Applicant, describing at least:

a.1) the Target of Evaluation;

a.2) (AND) the law and practice of the country with regards to government access to personal data, including safeguards limiting government access to the processed data, independent oversight of government access, and available redress mechanisms for Data Subjects;

a.3) (AND) the legal status regarding encryption and protection of online communications;

a.4) (AND) a risk and impact assessment of the law and practice of the country on the level of data protection and Data Subjects' rights and freedoms;

a.5) (AND) identification of potential issues for complying with the certification and Europrivacy criteria requirements;

a.6) (AND) where applicable, recommendations for supplementary measures to protect the processed data and the rights and freedoms of the Data Subjects.

AND

B) The report shall:

b.1) have been prepared by a legal expert with demonstrated knowledge of the respective national law and practices;

b.2) (AND) include the level of independence of the expert performing it.

AND

C) The report shall conclude that the law and practice in the country of the Applicant:

c.1) do not prevent the Applicant from complying with the Europrivacy criteria;

c.2) (AND) respect the essence of the fundamental rights and freedoms of the Data Subjects;

c.3) (AND) do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23.1 GDPR;

c.4) (AND) provide for appropriate safeguards for the rights and freedoms of Data Subjects.

AND

D) The Applicant shall have;

d.1) documented the supplementary measures they have decided to implement among those recommended in the report, including the justification for their choice;

d.2) (AND) where applicable, implemented the supplementary measures they have decided to apply;

d.3) (AND) where applicable, documented the justification for not applying any other recommended measures included in the report.

AND

E) There shall be rules, policies, or procedures in place:

e.1) to review the report whenever regulatory or organisational changes may hinder the compliance with the Europrivacy criteria or affect the Target of Evaluation or the Data Subjects' rights;

e.2) (AND) to inform the Certification Body of such change.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.1.1.2 Purpose Limitation and Lawfulness *(GDPR Art. 5.1b; 6.4) (CP; G; A)*

A) The Applicant shall have:

a.1) assessed and documented the purposes for which imported data is processed;

a.2) (AND) concluded in the assessment that the imported data is processed only for the specific purposes of the transfer, unless:

- GI.1.1.3 applies for Applicants acting as Data Controllers;
- OR the Data Exporter has provided further instructions to Applicants acting as Data Processors.

AND

B) The Applicant shall:

b.1) collect and document the legal basis of the Data Exporter for the imported data;

b.2) (AND) have rules, procedures or mechanisms in place to ensure that the data processing of imported data is consistent with the legal basis of the Data Exporter.

GI.1.1.3 Exceptions for Processing of Personal Data *(GDPR Art. 6.1; 46) (C; G; A)*

IF the Applicant processes the received personal data for other purposes than the one for which the data have been received, THEN the Applicant shall further process the data only where one of the following cases applies:

A) The data processing shall be based on the prior informed consent of the data subjects where:

a.1) consent shall be collected and documented before processing their personal data;

a.2) (AND) consent shall be expressly given by the data subjects for the processing of their personal data for one or more specific purposes;

a.3) (AND) the Applicant shall have a policy, procedure, rules or mechanism in place to assess the adequacy of the age and verification of the data subject for delivering consent.

OR

B) The data processing shall be performed on the basis of a legal obligation that is based on:

b.1) EU law or EEA Member State law;

b.2) (OR) the Applicable Law to the Applicant when acting as Data Importer.

OR

C) The data processing shall be necessary in order to protect vital interests of data subjects (i.e. essential for the life of the data subject, health).

OR

D) The processing is necessary for the establishment, exercise, or defence of legal claims, or whenever courts are acting in their judicial capacity.

Subject to copyrights

GI.1.2 Complementary requirements for consent to be valid (if applicable)

IF the lawfulness of the data processing is based on consent, THEN:

GI.1.2.1 Formal requirements for consent *(GDPR Art. 7.2) (C; S; A)*

A) The consent of the data subjects shall be prior and informed by ensuring that:

a.1) information on the purpose of the data processing and the identity of the Controller shall be communicated to the data subjects before or when consenting;

a.2) (AND) the consent shall be requested for a specific purpose;

a.3) (AND) the request for consent shall be worded in an easily understandable manner;

a.4) (AND) if made in a written form, the request for consent shall be presented in a separate paragraph and in a manner that renders it distinguishable from other matters;

a.5) (AND) consent shall be collected and documented prior to the processing of personal data by the Applicant;

a.6) (AND) consent shall be given by the data subjects in a clear and express manner (with a clear affirmative action);

a.7) (AND) consent shall cover each and every purpose for which the processing is carried out.

AND

B) The consents of the data subjects shall be freely given, including by ensuring that:

b.1) data subjects can limit or renounce to give their consent without detrimental effect on them;

b.2) (AND) where the Target of Evaluation encompasses several purposes for data processing, the Applicant shall provide a granular consent mechanism enabling the data subject to freely select which purpose to consent with;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

b.3) (AND) where the Applicant is a public authority or an employer of the data subject, the consent shall not be subject to an imbalance of power.

GI.1.2.2 Right to withdraw consent *(GDPR Art. 7.3) (C; S; A)*

A) The Applicant shall demonstrate that the procedure or mechanism in place to comply with the right of a data subject to withdraw consent enables to effectively implement the request.
AND
B) The procedure to withdraw consent shall be:

b.1) as simple as the one used for collecting consent;
b.2) (AND) accessible through the user interface(s) used to collect consent;
b.3) (AND) without detriment for the Data Subject.

GI.2 Special Data Processing

GI.2.1 Compliance of processing special categories of data

IF the Target of Evaluation processes any Special Categories of personal data, THEN:

GI.2.1.1 Special categories of data - DPO involvement *(GDPR Art. 9) (C; S; A)*

A) The Applicant shall 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
B) The Applicant shall have:

b.1) assessed and documented: the purposes for which imported data is processed;
b.2) (AND) concluded in the assessment that the imported data is processed only for the specific purposes of the transfer (unless GI.2.1.2 applies).

AND
C) The Applicant shall:

c.1) collect and document the exception applicable to the Data Exporter for the imported special categories of data;
c.2) (AND) have rules, procedures and mechanisms in place to ensure that the data processing of imported special categories of data is compatible with the exception applicable to the Data Exporter;
c.3) (AND) have rules, procedures or mechanisms in place to process the data for the same purposes and to the same extent as the law of the Data Exporter (in line with GI.2.1.2).

AND
D) The Applicant shall have consulted the DPO or a legal expert and included their findings in the assessment.

GI.2.1.2 Exceptions for processing special categories of data *(GDPR Art. 9) (C; S; A)*

The processing of Special Categories of Personal Data in the Target of Evaluation for other purposes than those for which the data are transferred shall be performed according to at least one of the following exceptions applicable to the Data Exporter:
A) The processing of the special categories of data shall be based on the explicit consent of the data subjects, unless forbidden by EU or EEA Member State law.
OR
B) The processing of special categories of data shall be:

b.1) based on employment and social necessity;
b.2) (AND) required by EU or EEA Member State Law, or a collective agreement pursuant to EEA Member State Law that provides for safeguards for the data subjects.

OR
C) The processing of special categories of data shall be necessary for the establishment, exercise, or defence of legal claims, or for court actions in their judiciary capacity.
OR
D) The data processing shall be necessary in order to protect vital interests of data subjects (i.e. essential for the life of the data subject, health).

GI.2.1.3 Additional Safeguards for processing special categories of data *(GDPR Art. 9) (C; S; A)*

A) The Applicant shall have additional restrictions and safeguards in place to protect the special categories of data, adapted to the specific nature of the data and the corresponding risks.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

I.2.2 Processing of data relating to criminal convictions and offences (if applicable)

IF the Target of Evaluation aims at processing data relating to criminal convictions and/or offences, THEN:

GI.2.2.1 Restrictions on Data Importers processing data related to criminal convictions and offences *(GDPR Art. 10) (C; S; A)*

A) IF the Applicant is processing data related to criminal convictions and offenses for other purposes than those of the transfer, THEN the processing shall be:

a.1) authorised by EU or EEA Member State law;

a.2) (OR) based on a legal obligation prescribed by the Third-Country Law applicable to Applicant.

AND

B) The Applicant shall:

b.1) collect and document the legal basis of the Data Exporter for the imported data related to criminal convictions and offences;

b.2) (AND) have rules, procedures and mechanisms in place to ensure that the data processing of imported special categories of data is compatible with the legal basis of the Data Exporter.

GI.3 Rights of the Data Subjects

GI.3.1 Transparent information, communication and modalities for exercising the rights of the data subjects

GI.3.1.1 Duty to inform in clear language *(GDPR Art. 12.1) (S; C; A)*

A) The information on the data processing provided by the Applicant to the data subjects and interested parties shall be:

a.1) concise and transparent;

a.2) (AND) intelligible and easily accessible form;

a.3) (AND) in a clear and plain language;

a.4) (AND) provided in writing or by other means (e.g. electronically);

a.5) (AND) available in the official national language(s) of the Applicant;

a.6) (AND) available in the language of the targeted data subjects.

AND

B) IF the Target of Evaluation includes the processing of personal data of a child, THEN the information shall have been assessed and deemed as appropriate and understandable to a child.

Subject to copyrights

GI.3.1.2 Duty to facilitate data subject rights exercise *(GDPR Art. 12.2) (G; A; C)*

A) The Applicant shall demonstrate that they have:

a.1) informed the data subjects on how they can exercise their rights via the Applicant's publicly accessible means e.g. via their website;

a.2 (AND) have personnel trained on how to handle data subject requests.

GI.3.1.3 Ensuring proper data subject rights management and recording *(GDPR Art. 12.2) (C; G; A)*

A) The Applicant shall have a procedure or a mechanism in place to:

a.1) receive and record all the requests of the data subjects;

a.2) (AND) confirm the reception of the request to the data subject;

a.3) (AND) identify or authenticate the data subjects' identity;

a.4) (AND) assess and verify that all conditions are satisfied to proceed with the request;

a.5) (AND) comply with the request or reject it;

a.6) (AND) control the delay between the reception of the data subject request and the reply and/or action by the Applicant.

AND

B) The Applicant shall keep records of:

b.1) the identification or authentication of the data subject;

b.2) the data subject requests with the date of reception;

b.3) (AND) the communications with data subjects with their dates;

b.4) (AND) the follow-up actions with their dates.

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

b.5) (AND) where applicable, the reasons for not complying with received request.

GI.3.1.4 Information without undue delay *(GDPR Art. 12.3) (C; G; A)*

A) The Applicant shall demonstrate that the procedure or mechanism in place is effective and appropriate to:

a.1) record the requests received from the data subjects;

a.2) (AND) address and reply to the received requests in no more than one month and without undue delay.

GI.3.1.5 Electronic response *(GDPR Art. 12.3) (C; G; A)*

A) The Applicant shall have rules, procedures, or a mechanism in place to ensure that where the data subject makes the request by electronic means, the information is provided by default through electronic means too.

GI.3.1.6 Duty to inform and justify non action *(GDPR Art. 12.4; 12.6) (C; G; A)*

A) The Applicant shall have rules, procedures or a mechanism in place to inform and justify non-action on the request of the data subjects.

AND

B) When the Applicant decides not to take action on a request for information from a data subject, it shall inform the data subject within no more than one month after receipt of the request about:

b.1) the reasons for not taking action;

b.2) (AND) the right to lodge a complaint with a Competent Data Protection Authority;

b.3) (AND) the possibility of seeking a judicial remedy.

GI.3.1.7 Free of charge (GDPR Art. 12.5) (C; G; A)

A) By default, the Applicant shall not charge any cost to the data subjects in the context of a request to exercise their rights.

AND

B) The Applicant shall have a written procedure in place to:

b.1) assess on factual criteria if the requests is manifestly unfounded or excessive;

b.2) (AND) document with factual justifications any decision not to provide free information;

b.3) (AND) assess the administrative costs of the related request if qualified as manifestly unfounded or excessive;

b.4) (AND) propose to charge the data subject with a reasonable fee in order to comply with manifestly unfounded or excessive data subject requests;

b.5) (AND) provide a justified decision to not comply with the request for free.

Subject to copyrights

GI.3.1.8 Machine-readability of icons *(GDPR Art. 12.7) (C; G; A)*

IF the Applicant uses icons to inform data subjects on its data protection policy by electronic means, THEN:

A) The Applicant shall demonstrate that its icons used to inform data subjects on its data protection policy are machine readable.

GI.3.2 Information to be provided where personal data have not been obtained from the data subject

IF the Target of Evaluation processes data that have not been obtained from the data subjects, THEN: [Except if an exemption can be demonstrated in conformity with GI.3.3.4]

GI.3.2.1 Duty to inform (GDPR Art. 14) (C; S; A)

The information provided to the data subject shall contain the following information:

A) The Controller's and DPO's details, namely:

a.1) the identity of the Controller and, where applicable, of its representative;

a.2) (AND) the contact details of the Controller and, where applicable, of its authorised representative;

a.3) (AND) the contact details of the data protection officer (or contact mechanism to contact the DPO).

AND

B) Information regarding the data processing, namely:

b.1) the purposes of processing;

b.2) (AND) the legal basis for the processing;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

b.3) (AND) if applicable, the legitimate interests pursued by the Controller or by a third-party;
b.4) (AND) the categories of personal data concerned;
b.5) (AND) the retention period or, if that is not possible, then the criteria for determining the retention period;
b.6) (AND) the source from which personal data originate;
b.7) (AND) if applicable, whether information came from publicly accessible sources;
b.8) (AND) the recipients or categories of recipients of the personal data.

AND

C) The data subjects' rights, namely:
c.1) information on data subject's right to access to personal data;
c.2) (AND) information on data subject's right to rectification of personal data;
c.3) (AND) information on data subject's right to erasure of personal data;
c.4) (AND) information on data subject's right to restriction of data processing;
c.5) (AND) information on data subject's right to objection to data processing;
c.6) (AND) information on data subject's right to data portability;
c.7) (AND) if processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of the processing before its withdrawal;
c.8) (AND) the right to lodge a complaint with a Competent Data Protection Authority in the EEA.

AND

D) IF personal data are intended to be transferred outside the EEA, or to an international organisation, THEN:
d.1) the list of non-European countries where the data will be transferred;
d.2) (AND) whether a valid adequacy decision applies for the data transfer;
d.3) (AND) information on the safeguards adopted by the Controller to ensure that the level of protection as provided to the data within the EEA will not be undermined;
d.4) (AND) where data subjects can obtain a copy of the safeguards or where they have been made available.

AND

E) IF automated processing decision-making and/or profiling is performed, THEN:
e.1) meaningful information about the logic involved in the processing activities;
e.2) (AND) the significance of the processing activities;
e.3) (AND) the envisaged consequences of the processing activities for the data subject.

GI.3.2.2 Duty to inform (GDPR Art. 14.3) (C; S; A)

A) The Applicant shall have a procedure in place to inform the data subjects: about the indirect collection of their data.

AND

B) The Applicant shall keep records of:
b.1) the date when personal data have been indirectly obtained;
b.2) (AND) the communication with the data subjects with the dates;
b.3) (AND) the information provided to the data subjects.

AND

C) Records shall demonstrate that information was provided by the Controller to the data subjects:
c.1) within no more than one month after obtaining the personal data;
c.2) (AND) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication with data subjects;
c.3) (AND) if disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

GI.3.2.3 Duty to inform on purpose extension *(GDPR Art. 14.4) (C; S; A)*

A) The Applicant shall have a procedure in place 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.

AND

B) The Applicant shall demonstrate the effectiveness of the procedure.

GI.3.2.4 Tolerated Exemption *(GDPR Art. 14.5) (C; S; E)*

IF one of the following cases apply, THEN GI.3.2.1 can be skipped:

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

Case 1 - Data subjects are already informed:
A) The Applicant shall demonstrate that the data subjects are already in possession of the information listed in GI.3.2.1.
OR Case 2 - Impossible or disproportionate:
A) The Applicant shall demonstrate that the provision of such information:
a.1) proves impossible;
a.2) (OR) would involve a disproportionate effort;
a.3) (OR) is likely to render impossible or seriously impair the achievement of the objectives of that processing.
AND
B) The Controller shall have taken appropriate measures to protect data subject's rights, freedoms and interests, including by making the information publicly available.
OR Case 3 - Legal obligation:
A) The Applicant shall be bound by a specific legal obligation which expressly requires the obtention or disclosure of personal data that shall be:
a.1) based on EU law or EEA Member State law;
a.2) (OR) based on Third Country Law that has been assessed in a written report to be essentially equivalent to EU law or EEA Member State law.
OR Case 4 - Regulated professional secrecy:
A) The Applicant shall be subject to an obligation of secrecy regulated by law, including a statutory obligation of secrecy that is:
a.1) based on EU law or EEA Member State law;
a.2) (OR) based on Third Country Applicable Law that has been assessed in a written report to be essentially equivalent to EU law or EEA Member State law.

GI.3.3 Right of access by the data subject

GI.3.3.1 Right of access by the data subject *(GDPR Art. 15.1; 15.2) (C; S; A)*

The Applicant shall have an effective mechanism or procedure in place enabling the data subjects to request and access the following information:
A) Information on the data processing, namely:
a.1) whether their personal data is processed and the purposes of the processing;
a.2) (AND) the categories of processed personal data;
a.3) (AND) the recipients or categories of recipients of their personal data, including recipients in third countries or international organisations;
a.4) (AND) the retention period or, if this is not possible, the criteria for determining the retention period;
a.5) (AND) the source from which the personal data has been obtained and, if applicable, whether the personal data came from a publicly accessible source.
AND
B) Information on their rights, namely:
b.1) information on the data subject's rights to access his/her data;
b.2) (AND) information on the data subject's rights to rectification;
b.3) (AND) information on the data subject's rights to erasure of personal data;
b.4) (AND) information on the data subject's rights to restriction of processing;
b.5) (AND) information on the data subject's rights to object to their personal data processing;
b.6) (AND) information on the data subject's rights to data portability;
b.7) (AND) the right to lodge a complaint with a Competent Data Protection Authority in the EEA.
AND
C) Information regarding the implementation of automated decision making, including profiling, namely:
c.1) whether the Controller implemented automated decision-making, including profiling;
c.2) (AND) meaningful information about the logic involved in the processing activities;
c.3) (AND) the significance of the processing activities;
c.4) (AND) the envisaged consequences of the processing activities for the data subject.
Transfer outside the EEA
AND
D) Information on data transfers outside the EEA, namely:

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

d.1) whether personal data are transferred to any third country or to an international organisation;
d.2) (AND) a list of third countries or international organisation(s) to which the data are transferred;
d.3) (AND) whether a valid adequacy decision applies to the data transfer;
d.4) (AND) information on the safeguards relating to the transfer that is used and, if needed, the supplementary measures to ensure the level of protection to the personal data.

GI.3.3.2 Duty to provide a copy *(GDPR Art. 15.3) (C; S; A)*

A) The Applicant shall have rules, policies or procedures in place to:
a.1) extract a copy of Data Subjects' personal data processed;
a.2) (AND) provide Data Subjects with a copy of their personal data processed upon their request.

AND

B) IF the Data Subject has requested to receive the information by electronic means, THEN the copy shall be provided in a commonly used electronic format.

GI.3.3.3 Duty to respect the rights of others *(GDPR Art. 15.4) (C; S; A)*

A) The Applicant shall have a procedure or a mechanism in place to prevent adverse effects on rights and freedoms of other data subjects when complying with a data subject request to receive a copy of their personal data.

GI.3.4 Right to rectification

GI.3.4.1 Right to rectification *(GDPR Art. 16) (C; S; A)*

A) The Applicant shall demonstrate that the procedure or mechanism in place to comply with the right of a data subject to rectify or complete his personal data enables to effectively handle the request.

GI.3.5 Right to erasure ('right to be forgotten')

GI.3.5.1 Right to erasure *(GDPR Art. 17.1) (C; S; A)*

A) The Applicant shall have rules, a procedure, or a mechanism in place to effectively erase the personal data transferred upon the data subjects' request, unless one of the conditions of GI.3.5.3 applies.

GI.3.5.2 Duty to relay the request to other data Controllers *(GDPR Art. 17.2) (C; S; A)*

IF the Applicant has made personal data of the Target of Evaluation publicly available, THEN:
A) The Applicant shall have rules, a procedure, or a mechanism in place to inform other Controllers about the request for erasure by the data subjects, except if the Applicant has evaluated the potential measures to inform the other data Controllers and has demonstrated that the identified measures would have been disproportionate.

Subject to copyrights

GI.3.5.3 Tolerated Exemption *(GDPR Art. 17.3) (C; S; E)*

The right to erasure is subject to restrictions in the following cases:
A) The Applicant shall demonstrate that the personal data is used for exercising the right of freedom of expression and information.
OR
B) The Applicant shall demonstrate that there is an obligation to comply with a legal obligation that is:
b.1) based on EU law or EEA Member State law;
b.2) (OR) based on the Third Country Law that has been assessed in a written report to be essentially equivalent to EU law or EEA Member State law.
OR
C) There shall be a public interest in the area of public health that is:
c.1) based on EU law or EEA Member State law;
c.2) (OR) based on a legal obligation of the Applicant acting as Data Importer.
OR
D) The Applicant shall demonstrate that:
d.1) the processing is necessary for archiving purposes in the public interest;
d.2) (OR) the processing is necessary for scientific purposes;
d.3) (OR) the processing is necessary for historical research purposes;
d.4) (OR) the processing is necessary for statistical purposes;
d.5) (AND) the erasure is likely to render impossible or seriously impair the achievement of the objectives of the processing;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

d.6) (AND) appropriate safeguards for the data subjects are in place.

OR

E) The Applicant shall demonstrate that the processing of personal data is related to the establishment, exercise or defence of legal claims.

GI.3.6 Right to restriction of processing

GI.3.6.1 Right to restriction of processing *(GDPR Art. 18) (C; S; A)*

A) The Applicant shall have rules, a procedure, or a mechanism in place:

a.1) to effectively comply with the requests of data subjects to restrict the processing of their personal data, in case:

- the accuracy of the personal data is contested by the data subject;
- (OR) personal data have been unlawfully processed or processing violates the requirements contained in the Certification issued, and the data subject opposes the erasure of the personal data and requests restriction instead.
- (OR) the processing is no longer necessary for the purpose for which it was collected;
- (OR) the data subject has objected to the processing, including profiling, based on legitimate interest of the Controller or public interest vested in the Controller;

a.2) (AND) to ensure that the processing can only continue to take place:

- if the data subject consents;
- (OR) for the establishment, exercise or defence of legal claims;
- (OR) for reasons of important public interest to which the Data Exporter is subject;

a.3) (AND) to document the decisions to lift data processing restrictions;

a.4) (AND) to ensure that the data subject is informed before lifting the restriction on the processing of his personal data.

GI.3.7 Notification obligation regarding rectification or erasure of personal data or restriction of processing

GI.3.7.1 Duty to inform recipients *(GDPR Art. 19) (C; S; A)*

A) The Applicant shall have a procedure or mechanism in place 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.

OR

B) The Applicant shall demonstrate that the duty to inform the recipient is impossible or involves disproportionate effort.

GI.3.7.2 Duty to inform data subjects (on lifting the restriction on processing and on recipients if requested) *(GDPR Art. 19; 18.3) (C; S; A)*

A) The Applicant shall have rules, a procedure, or a mechanism in place to effectively comply with the requests of data subjects to be informed on the recipients of their personal data.

AND

B) IF the Data Subject had obtained the restriction of processing, THEN the Applicant shall inform the Data Subject prior to lifting the restriction of processing.

GI.3.8 Right to object

GI.3.8.1 Effectiveness of the right to object *(GDPR Art. 21) (C; S; A)*

A)The Applicant shall have rules, a procedure, or a mechanism in place to effectively comply with the requests of data subjects to object to the processing of their personal data on grounds relating to their particular situation.

AND

B) IF the data are processed for direct marketing, including profiling related to direct marketing, THEN: the rules, procedure, or mechanism in place shall ensure that:

b.1) the Data Subject can object at any time;

b.2) (AND) the personal data of the objecting Data Subject are no longer processed for a marketing purpose.

AND

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

C) IF the data are processed for scientific or historical research purposes or statistical purposes, THEN: the rules, procedure or mechanism in place shall ensure that the Data Subject can object to the processing of their personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest as recognised in the EEA or Member State law.

GI.3.8.2 Clear information on the right to object *(GDPR Art. 21.4) (C; S; A)*

A) The Applicant shall inform the data subjects about their right to object to the processing of their personal data:

a.1) before processing their data;

a.2) (AND) in a distinct paragraph or separately from any other information.

AND

B) The Applicant shall have verified that the information is clear and understandable by the Data Subject.

GI.3.9 Right not to be subject to automated individual decision-making, including profiling

GI.3.9.1 Automated individual decision-making, including profiling *(GDPR Art. 22.1) (C; S; A)*

A) The data processing in the Target of Evaluation shall be exempt of any decisions based solely on automated decisions that may have an effect on the data subjects, except where the automated decision process shall be:

a.1) necessary for entering into, or performing, a contract between the data subject and the data Controller according to a written analysis that has concluded that there is no alternative less intrusive measures that can reach an equivalent result;

a.2) (OR) authorised by EU or EEA Member State law providing suitable measures to safeguard the rights and legitimate interests of the Data Subjects;

a.3) (OR) authorised by the Third-Country Law of the Data Importer, whose law has been assessed as providing suitable measures to safeguard the rights and legitimate interests of the Data Subjects;

a.4) (OR) based on the Data Subject's explicit consent.

AND

B) The Applicant shall have dedicated measures in place to safeguard the data subject's rights and freedoms and legitimate interests.

GI.3.9.2 Rights to obtain human intervention and to contest *(GDPR Art. 22.3) (C; S; A)*

IF automated decision, including profiling, are based on the processing of personal data, THEN:

A) The Applicant shall provide specific information to the data subject pertaining to the automated decision making, including profiling, in relation to their personal data;

AND

B) The Applicant shall have procedure or mechanism in place that enables the data subjects:

b.1) to obtain human intervention on the part of the Controller;

b.2) (AND) to express their points of view and to contest the decision.

Subject to copyrights

GI.4 Data Controller Responsibility

GI.4.1 Responsibility of the Controller

IF the Applicant is a data Controller, THEN:

GI.4.1.1 Documentation on technical and organization measures *(GDPR Art. 24.1) (C; S; A)*

A) The Applicant shall have written documentation of its technical and organizational measures implemented for protecting the processed data.

GI.4.1.2 Duty to review and update *(GDPR Art. 24.1) (C; S; A)*

A) The Applicant shall have a procedure in place to review on a regular basis (at least yearly) the appropriateness of the:

a.1) technical and organizational measures in place to protect personal data;

a.2) (AND) policies, procedures and mechanisms in place to protect personal data.

AND

B) The Applicant shall keep documented records of:

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

b.1) the review of the technical and organizational measures, and policies, procedures and mechanisms;
b.2) the identified vulnerabilities and measures taken to address these vulnerabilities.

GI.4.1.3 Data Protection Policies *(GDPR Art. 24.2) (C; S; A)*

A) Applicant shall have written data protection rules and/or policies encompassing at least:
a.1) security and access control;
a.2) (AND) personal data breach management;
a.3) (AND) risk assessment and where applicable data protections impact assessment (DPIA);
a.4) (AND) requirements and compliance assessment of data Processors;
a.5) (AND) procedure for informing and cooperating with the competent Data Protection Authorities;
a.6) (AND) policy regarding data protection by design and by default, such as data minimisation and data pseudonymisation;
a.7) (AND) management of data transfer to third countries.

GI.5 Data Processors (or sub Processors)

IF data Processors or Sub-Processors are involved in the Target of Evaluation, THEN:

GI.5.1 Responsibility of the Controller

GI.5.1.1 Engaging Processors *(GDPR Art. 28.1) (CP; S; A)*

IF the Applicant is acting as a Data Controller engaging Processors, THEN:
A) There shall be rules, a procedure, or a mechanism in place to only engage Processors and Sub-Processors that provide sufficient guarantees:
a.1) by requesting and recording information from its Data Processors and any Sub-Processors about their technical and organizational measures to protect personal data;
a.2) (AND) assessing the appropriateness of the technical and organizational measures taken by the Processor and any Sub-Processor for protecting personal data;
a.3) (AND) documenting the assessment and record the decision to accept the services of the Data Processor.

AND

B) The Applicant shall keep documented records of:
b.1) the information and guarantees provided by the Processor, and any Sub-Processor, in its Technical and Organizational Measures;
b.2) (AND) the evaluation and decision process to engage data Processors and any Sub-Processors involved in the data processing of the Target of Evaluation.

AND

C) The Applicant shall have rules or a procedure in place to perform regular review of the agreements with and guarantees provided by its Processors and any Sub-Processors.

GI.5.1.2 Engaging Sub-Processors (GDPR Art. 28.2; 28.4) (P; S; A)

IF the Applicant is acting as a Data Processor using Sub-Processors for the Target of Evaluation, THEN:
A) There shall be rules, procedure, or a mechanism in place to only use Sub-Processors that provide sufficient guarantees:
a.1) by requesting and recording information from its Sub-Processors about their technical and organizational measures to protect personal data;
a.2) (AND) assessing the appropriateness of the technical and organizational measures taken by any Sub-Processor for protecting personal data;
a.3) (AND) obtaining and documenting the Controller's prior authorization to engage the Sub-Processors;
a.4) (AND) ensuring that the Sub-Processors are contractually bound by obligations equivalent to those imposed to the Processors regarding the data processing in the Target of Evaluation;

AND

B) The Applicant shall keep documented records of:
b.1) the information and guarantees provided by the Sub-Processor, including its Technical and Organizational Measures;

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

b.2) (AND) the evaluation and decision process to engage Data Processors and the prior authorization for any Sub-Processors involved in the data processing of the Target of Evaluation.

AND

C) IF the prior authorization is general, THEN the Applicant's documentation shall include:

c.1) the list of criteria approved by the Controller to select and appoint Sub-Processors;

c.2) (AND) how the selected Sub-Processors meet the criteria set by the Controller;

c.3) (AND) the procedure, mechanism, or policy in place to inform the Controller of any intended changes of Sub-Processors, providing the Controller with a reasonable opportunity to object prior to engagement.

AND

D) IF the prior authorization is specific, THEN the Applicant's documentation shall include:

d.1) the prior authorisation request to the Controller for each Sub-Processor before their use;

d.2) (AND) the specific prior authorisation for each Sub-Processor.

AND

E) The Applicant shall have rules, policy, or a procedure in place to regularly review the agreements with and guarantees provided by the Sub-Processors.

GI.5.1.3 Contractual requirements for Applicant acting as a Data Controller and contracting Processors *(GDPR Art. 28.3) (C; S; A)*

IF the Applicant acts as Controller and uses Processors, THEN:

A) The Applicant shall have a written agreement with each and every Data Processor in relation to the processing of personal data in the Target of Evaluation, that shall:

a.1) be eligible to a European Union Member State court;

a.2) (AND) specify the subject matter and duration of the processing;

a.3) (AND) specify the nature and purpose of processing;

a.4) (AND) specify the type of personal data;

a.5) (AND) specify the categories of data subjects;

a.6) (AND) specify the rights and obligations of the Controller;

a.7) (AND) specify the requirements for transfers to third countries or international organisations;

a.8) (AND) require that any transfer of personal data by the Data Processors and Sub-Processors are performed upon the Controller's written instructions;

a.9) (AND) require that any use of data processor is conditioned to technical and organisational measures to protect data.

Subject to copyrights

GI.5.1.4 Contractual Requirements for Processors *(GDPR Art. 28.3) (P; S; A)*

IF the Applicant acts as Processor, THEN:

A) The Applicant shall have a written agreement with each and every Data Controller and Data Sub-Processor in charge of processing data in the Target of Evaluation.

AND

B) Each contractual relationship of the Processor with the Data Controllers and Data Sub-Processors involved in the Target of Evaluation shall:

b.1) be eligible to a European Union Member State court;

b.2) (AND) specify the subject matter and duration of the processing;

b.3) (AND) specify the nature and purpose of processing;

b.4) (AND) specify the type of personal data;

b.5) (AND) specify the categories of data subjects;

b.6) (AND) specify the rights and obligations of the Controller;

b.7) (AND) specify the requirements for transfers to third countries or international organisations;

b.8) (AND) require that any transfer of personal data by the Data Processors and Sub-Processors are performed upon the Controller's documented instructions;

b.9) (AND) require that any use of data processor is conditioned to technical and organisational measures to protect transferred data;

b.10) (AND) where Sub-Processors are involved, require all data protection obligations set out by the Controller.

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.5.1.5 Contractual obligations of Processors and Sub-Processors *(GDPR Art. 28.3) (CP; S; A)*

A) The contractual relationship with each and every data Processors involved in the Target of Evaluation shall stipulate that the Processor must:

a.1) process personal data only on documented instructions from the Controller;
a.2) (AND) ensure that all those who authorized to process personal data in the Target of Evaluation are bound by confidentiality obligations;
a.3) (AND) implement all measures required pursuant to Security of Processing;
a.4) (AND) commit not to engage other Processors (or sub-processors) without the agreement of the Controller;
a.5) (AND) fulfil its obligation to respond to requests of data subjects;
a.6) (AND) assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights;
a.7) (AND) assist the Controller in ensuring compliance with the obligations for security of data processing, such as risk assessment, data breach management and notification, data protection impact assessment, and prior consultation with the authority;
a.8) (AND) at the choice of the Controller, delete or return all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless the conservation of the data is required by EU or EEA Member State law (or a legal obligation prescribed by Third Country law applicable to Applicant acting as a Data Importer based outside of the EEA);
a.9) (AND) make available to the Controller all information necessary to demonstrate compliance with the data protection regulation;
a.10) (AND) authorize inspections conducted by the Controller or another auditor mandated by the Controller;
a.11) (AND) require that the same obligations and protections be required from sub Processors that the Processor contract for carrying out specific processing activities on behalf of the Controller.

GI.5.1.6 Complementary demonstration of Processors' compliance *(GDPR Art. 24.3; 28.5; 25.3; 32.2) (CP; S; A)*

A) For each Data Processor, the Applicant shall collect information and keep record of their certification, approved code of conduct, and binding commitments to respect the applicable data protection regulations.

GI.5.2 Processing carried out by Processors or Sub-processors on behalf of the Controller

GI.5.2.1 Processing solely on instruction from the Controller *(GDPR Art. 29) (P; S; A)*

IF the Applicant acts as Processor, THEN:
A) The Applicant shall have rules, a procedure or a mechanism in place to:

a.1) prevent data processing without instructions from the Controller;
a.2) (AND) receive and record instructions from the Controller.

AND
B) The Applicant shall have record of:

b.1) the processing instructions received from the Controller;
b.2) (AND) the processing activities.

AND
C) The processing activities shall comply with the instructions received from the Controller.

GI.5.3 Record of processing activities

GI.5.3.1 Record of data processing by the Controller *(GDPR Art. 30) (C; G; A)*

IF the Applicant acts as Controller, THEN:
A) The Applicant shall maintain a record in writing (including electronic form) of processing activities falling under ToE, which shall contain the following information:

a.1) the name and contact details of the Controller;
a.2) (AND) if applicable, the name and contact details of the joint Controllers;
a.3) (AND) if applicable, the name and contact details of the Controller's representative;

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

a.4) (AND) the name and contact details of the data protection officer;
a.5) (AND) the purposes of processing;
a.6) (AND) the description of the categories of data subjects and personal data;
a.7) (AND) the categories of recipients to whom personal data have been or will be disclosed (including recipients in third countries or international organizations);
a.8) (AND) the data retention policy specifying the envisaged time limits for erasure of the different categories of data;
a.9) (AND) the general description of the technical and organisational security measures.

AND

B) IF personal data are transferred to third countries THEN:

b.1) the information on transfers of personal data to a third country or an international organization;
b.2) (AND) the list of the third country or international organisation, including identification, to which data are transferred;
b.3) (AND) documentation of suitable safeguards for transfers, including supplementary measures, to ensure the level of protection will not be undermined by such transfer.

GI.5.3.2 Record of data processing by the Processor *(GDPR Art. 30.2) (P; G; A)*

IF the Applicant acts as Processor, THEN:

A) The Applicant shall maintain a record of all categories of processing activities carried out in the Target of Evaluation on behalf of the Controller, with the following information:

a.1) the name and contact details of the Processor(s);
a.2) (AND) the name and contact details of each Controller, including joint Controllers, on behalf of which the Processor is acting;
a.3) (AND) if applicable, the name and contact details of the Controller's or the Processor's representative;
a.4) (AND) the name and contact details of the data protection officer;
a.5) (AND) the general description of the technical and organisational security measures set in place;
a.6) (AND) the categories of processing carried out on behalf of each Controller.

AND

B) IF personal data are transferred to third countries THEN the following information shall be provided:

b.1) the information on transfers of personal data to a third country or an international organization;
b.2) (AND) the list of the third country or international organisation, including the identification, to which data are transferred;
b.3) (AND) documentation of suitable safeguards for transfers, including supplementary measures, set in place to ensure that the level of protection will not be undermined (See GI.10.1.3).

Subject to copyrights

GI.5.3.3 Data Processing instructions records *(GDPR Art. 30) (CP; S; A)*

A) There shall be a registry and/or documentation of written instructions communicated by the Controller to the Processor(s) (or where applicable by the Processor, on behalf of the Controller, to the Sub-processors).

AND

B) There shall be a registry and/or documentation of written authorization, and conditions provided by the Controller permitting the Processor to engage a Sub-Processor.

GI.5.3.4 Completeness of the Record of processing activities *(GDPR Art. 30) (CP; S; A)*

A) All processing activities in the scope of the Target of Evaluation shall be recorded in the Record of processing activities.

GI.5.3.5 Duty to cooperate with the Competent Data Protection Authorities in the EEA *(GDPR Art. 30.4) (CP; S; A)*

A) The Applicant shall have rules, policies or procedures in place to:

a.1) cooperate with requests made by the Competent Data Protection Authorities in the EEA;
a.2) (AND) make available, upon request, its record of Processing Activities.

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.6 Data Protection by Design and Default, and Security of Processing

GI.6.1 Data protection by design and by default

GI.6.1.1 Data protection by design and by default *(GDPR Art. 25.1) (C; S; A)*

A) The Applicant shall have policies, rules, or procedures in place requiring to apply and maintain data protection by design and by default to its data processing, including the minimization of:

a.1) the collection and processing of personal data;

a.2) (AND) the storage and retention of personal data;

a.3) (AND) the access to the processed personal data.

AND

B) The Applicant shall have formally assessed in writing the data processing of the Target of Evaluation to comply with the data protection by design and by default requirement, including by:

b.1) analysing the risks for the freedom and rights of the data subjects in terms of likelihood and severity;

b.2) (AND) assessing if the collection of personal data has been limited to the fulfilment of its purpose and lawfulness basis, and if not making recommendations;

b.3) (AND) assessing if the processing of personal data is limited to the fulfilment of its purpose and lawfulness basis, and if not making recommendations;

b.4) (AND) assessing if the retention period of personal data is limited to the fulfilment of its purpose and lawfulness basis, and if not making recommendations;

b.5) (AND) assessing if the access to the processed personal data is limited to who needs to access it for its processing, and if not making recommendations;

b.6) (AND) assessing where the use of encryption, pseudonymization and anonymization techniques shall be applicable;

b.7) (AND) assessing whether the technical and organizational measures implemented are in line with the state of the art.

AND

C) the DPO or a legal expert shall confirm that:

c.1) the analysis and recommendations on the measures that are appropriate;

c.2) (AND) he/she did not identify less privacy intrusive solution in terms of personal data collection for achieving the purposes for the processing;

c.3) (AND) the applicable recommendations have been implemented.

subject to copyrights

GI.6.1.2 Data minimization by default *(GDPR Art. 25.1) (C; S; A)*

A) The Applicant shall have implemented organizational or technical measures to:

a.1) only collect personal data which is necessary for the purposes of the processing;

a.2) (AND) not store personal data if it is not necessary for the purpose of the processing and there is no compatible purpose and legal ground;

a.3) (AND) delete or anonymize personal data by default at the end of the retention period.

a.4) (AND) restrict access to personal data on the basis of a registry of authorized personnel;

a.5) (AND) have used a risk analysis to implement technical and organizational measures for mitigating the identified risks of the processing to the rights and freedoms of the data subjects.

AND

B) The Applicant shall have rules, a procedure, or a mechanism in place to effectively erase the personal data transferred that encompasses the following cases, where applicable to the Target of Evaluation:

b.1) data are no longer necessary (in relation with the purpose for which they were transferred);

b.2) (OR) consent has been withdrawn by data subjects;

b.3) (OR) data subjects have objected successfully to their personal data processing;

b.4) (OR) personal data have been unlawfully processed;

b.5) (OR) the erasure is required by EU law or EEA Member State law applicable to the Applicant's Data Exporter;

b.6) (OR) the personal data have been transferred in relation to the offer of information society services to a child.

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.6.2 Security of processing

GI.6.2.1 Security policy (GDPR Art. 32.1) (CP; G; A)

A) The Applicant shall have written rules and/or policies in place of the implemented technical and organisational measures which demonstrate a level of security which is appropriate to the risk of processing, covering at least:

a.1) the pseudonymization and encryption policy;
a.2) (AND) the data confidentiality policy;
a.3) (AND) the data minimization policy;
a.4) (AND) the data access control policy;
a.5) (AND) the data processing restrictions;
a.6) (AND) the data storage and retention period policy;
a.7) (AND) the data integrity, availability and backup policy;
a.8) (AND) the data breach policy;
a.9) (AND) the "bring your own device" policy and restrictions on copying data;
a.10) (AND) updates and patches policy;
a.11) (AND) the cryptographic and password policy;
a.12) (AND) the network security policy.

AND

B) The Applicant shall communicate those policies and rules to all employees and agents handling personal data, including as part of its training activities (See Criterion GI.9.3.2).

GI.6.2.2 Process on instruction only *(GDPR Art. 32.4) (CP; G; A)*

A) The Applicant shall have legally binding rules, policies, contractual clauses, guidelines or mechanisms in place to ensure that any natural person acting under its authority does not process personal data except if:

a.1) instructed by the Controller;
a.2) (OR) required by EU or EEA Member State law applicable to the Data Exporter.

GI.6.2.3 Contractual obligation to confidentiality *(GDPR Art. 32) (CP; G; A)*

A) The Applicant shall have rules, policies or procedures in place to ensure that all natural persons who handle personal data shall be legally bound by confidentiality obligations which extend beyond the end of their activities.

GI.6.2.4 Risk assessment for the data processing *(GDPR Art. 32.2) (CP; S; A)*

A) The Applicant shall have assessed, with a repeatable methodology, the risks that are presented by the processing, that may impact the rights and freedoms of the natural persons, including the risks related to:

a.1) the processing itself, considering its scope, purpose, context and nature;
a.2) (AND) data availability and continuity, including the accidental or unlawful destruction or loss of personal data;
a.3) (AND) data integrity, including the accidental or unlawful alteration of personal data;
a.4) (AND) data confidentiality, including the accidental, unlawful or unauthorised disclosure of personal data or access to personal data, including third-country data transfers;
a.5) (AND) data resilience, including the risk of data breaches;
a.6) (AND) mishandling the data, including unlawful or unauthorized processing, or data misuse;
a.7) (AND) the data subjects' rights and freedoms, including the risk of discrimination, identity theft or fraud, unauthorized reversal of pseudonymization, reputational or financial damage;
a.8) (AND) where applicable, the Bring Your Own Device practices;
a.9) (AND) the physical and electronic data environments;
a.10) (AND) the monitoring and logging activities;
a.11) (AND) the access and authentication mechanisms;
a.12) (AND) where applicable, the re-identification of encrypted, pseudonymized, or anonymized data;
a.13) (AND) where applicable, the web-interfaces, wireless communications, and networks.

AND

B) The identified risks of the risk analysis shall, in any case, be provided for advice to the DPO and CISO, and shall result in a risk mitigation plan to mitigate the identified risks.

AND

C) The risk assessment and risk mitigation plan shall:

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

c.1) include any security measures to be implemented and those already implemented;
c.2) (AND) where applicable, specify the security measures required by Data Exporters;
c.3) (AND) be regularly reviewed and updated, at least on annual basis or whenever new risks emerge or when organizational, legal or technical changes take place.

AND

D) Where the risk assessment concludes that it is necessary to take additional technical or organisational measures to ensure that the personal data is secure, then the mitigation plan shall be implemented.

GI.6.2.5 Complementary Technical and Organization Measures *(GDPR Art. 32) (CP; S; A)*

A) The Applicant shall have:

a.1) assessed the appropriateness of its Technical and Organisational Measures (TOM);
a.2) (OR) a complementary certification of the Technical and Organizational Measures in place to secure and protect the data processed in the Target of Evaluation that is at least equivalent to the certification requirements.

AND

B) The Applicant's DPO or a legal expert, and a technical expert shall have reviewed and shall have provided their findings on whether they are sufficient and adequate to protect the rights and freedoms of the data subjects.

GI.6.2.6 Data Exporter Validation of Technical and Organizational Measures *(GDPR Art. 32) (CP; S; A)*

A) Before receiving data from its Data Exporter, the Applicant shall have:

a.1) shared a description of their Technical and Organizational measures and any relevant documentation to the Data Exporter for review;
a.2) (AND) received the Data Exporter's written validation of the Technical and Organizational measures;
a.3) (AND) clarified the respective responsibilities of the parties involved in the transfer regarding the implementation of the Technical and Organizational measures.

AND

B) The Applicant shall have rules, procedures or a mechanism in place to notify the Data Exporter of any changes to their Technical and Organizational measures.

Subject to copyrights

GI.7 Management of Data Breaches

GI.7.1 Notification of a personal data breach to the Competent Data Protection Authority

GI.7.1.1 Duty to document data breaches *(GDPR Art. 33.5) (CP; G; A)*

A) The Applicant shall keep a record of its personal data breaches which shall include at least:

a.1) the nature of the personal data breach;
a.2) (AND) the categories of personal data that are or may be affected;
a.3) (AND) the approximate number of data subjects that are or may be affected;
a.4) (AND) the categories and approximate number of personal data records it concerns or may concern;
a.5) (AND) the likely consequences of the personal data breach;
a.6) (AND) the measures taken or proposed to address the personal data breach, including measures to mitigate its adverse effects.

GI.7.1.2 Duty of the Controller to notify and communicate data breaches *(GDPR Art. 33.1; 34.1) (C; G; A)*

A) The Applicant shall have rules, a procedure or a mechanism in place to:

a.1) record personal data breaches and actions taken with the date and time;
a.2) (AND) assess if the data breach is likely to result in a risk to the rights and freedoms of natural persons;
a.3) (AND) determine and take appropriate actions to minimise the risks, its likelihood, and potential impact on data subjects;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

a.4) (AND) when the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, inform the Competent Data Protection Authority without undue delay and no more than 72 hours after having become aware of it;
a.5) (AND) when the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, inform the data subject without undue delay, unless an exemption of GI.7.2.2 applies.

GI.7.1.3 Duty of the Processor to communicate data breaches with undue delay *(GDPR Art. 33.2) (P; G; A)*

A) The Applicant shall have rules, a procedure or a mechanism in place to:
a.1) record personal data breaches and actions taken with the date and time;
a.2) (AND) determine and take appropriate actions to minimize the risks and potential impact on data subjects.
a.3) (AND) assist the Controller in assessing the risk of the data breach for the rights and freedoms of natural persons;
a.4) (AND) communicate the breach to the related data Controller(s) without undue delay;
a.5) (AND) when the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, inform the Controller in a manner that allows them to inform the Competent Data Protection Authority without undue delay and no more than 72 hours after having become aware of it.

GI.7.1.4 Notification requirements *(GDPR Art. 33.3) (C; G; A)*

A) The procedure for notifying a data breach to the Competent Data Protection Authority shall require to include the following information:
a.1) the nature of the personal data breach;
a.2) (AND) the categories and approximate number of data subjects and personal data concerned (where possible);
a.3) (AND) the name and contact details of the data protection officer or other contact point where more information can be obtained;
a.4) (AND) the likely consequences of the personal data breach;
a.5) (AND) 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.

GI.7.2 Communication of a personal data breach to the data subject

GI.7.2.1 Breach communication requirements *(GDPR Art. 34.2) (C; G; A)*

A) The procedure or mechanism for communicating a data breach to the data subjects shall include at least the following information in a clear and plain language:
a.1) the nature of the personal data breach;
a.2) (AND) the categories of personal data records concerned;
a.3) (AND) the name and contact details of the data protection officer or other contact point where more information can be obtained;
a.4) (AND) the likely consequences of the personal data breach;a.5) (AND) 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 needed, the measures to mitigate its possible adverse effects.

GI.7.2.2 Tolerated Exemptions *(GDPR Art. 34.3) (C; S; E)*

IF the following conditions are met, THEN direct communication to the data subject is not required:
A) The communication was not carried out due to one of the following exceptions:
a.1) the Applicant has implemented appropriate technical and organisational measures (such as encryption) to render the personal data that have been breached unintelligible to any person who is not authorised to access it.
a.2) (OR) the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
a.3) (OR) direct information would have requested a disproportionate effort AND was replaced by a public communication (or similar measure whereby the data subjects are informed in an equally effective manner).
AND

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

B) The data breach does not result in a high risk to the rights and freedoms of the data subjects.

GI.8 Data Protection Impact Assessment (DPIA)

GI.8.1 Notification of a personal data breach to the Competent Data Protection Authority

GI.8.1.1 Data Protection Impact Assessment (DPIA) *(GDPR Art. 35.1; 35.3; 35.4) (C; S; A)*

A) The Applicant shall have performed a DPIA prior to the processing, if any one of the following cases applies to the Target of Evaluation:

a.1) the personal data processing, in particular using new technologies, is likely to result in a high risk for the rights and freedoms of the data subject;

a.2) (OR) a systematic and extensive evaluation of personal aspects of natural persons based on automated processing (including profiling) on which decisions are based that may affect natural persons;

a.3) (OR) a large scale processing of special categories of data or personal data related to criminal convictions or offences;

a.4) (OR) a systematic monitoring of a publicly accessible area on a large scale;

a.5) (OR) the processing operations falls in the list of data processing activities requiring a DPIA that is published by the Data Protection Authority of the Applicant that is not an Importer;

a.6) (OR) processing operations listed as requiring DPIA according to the Data Protection Authority of the Exporter of the personal data (or to the applicable legislation).

AND

B) The Applicant shall have performed a DPIA except if the Applicant:

b.1) has performed a preliminary written assessment of the risks for the rights and freedoms of the data subjects;

b.2) (AND) has concluded in its written assessment that there is no high risk to the rights and freedoms of the data subjects;

b.3) (AND) a procedure, policy or plan is in place to reassess the risk on a regular basis.

AND

C) The Applicant shall have policies, rules or procedures in place to review its conclusions to not perform a DPIA when the scope or purpose of the data processing of the Target of Evaluation are substantially modified or exposed to new risks.

Subject to copyrights

GI.8.1.2 Tolerated Exemption *(GDPR Art. 35.10) (C; S; E)*

DPIA is not required (except if required by EU or EEA Member State law of the Data Exporter) if:

A) Processing has a legal basis in EU or EEA Member State law of the Data Exporter AND an impact assessment has already been carried out in the legislative process.

OR

B) The Target of Evaluation is covered by the list or data processing activities that are exempted of DPIA by the Competent Data Protection Authority for the Exporter in the EEA.

GI.8.2 Data Protection Impact Assessment Check (DPIA) requirements

IF a DPIA is applicable, THEN:

GI.8.2.1 DPIA Process requirements *(GDPR Art. 35.2; 35.7.b) (C; S; A)*

A) The DPIA process shall have:

a.1) involved the DPO in the assessment and measures to reduce the risks to the rights and freedoms of natural persons;

a.2) (AND) taken into account the views of data subjects or their representatives;

a.3) (AND) where applicable, taken into account the compliance with approved codes of conduct, certifications, and other binding and enforceable commitments when assessing the impact of the processing operations falling in scope of the DPIA;

a.4) (AND) where applicable, adopted a plan for measures envisaged to address the risks, including safeguards, security measures and mechanisms;

a.5) (AND) where applicable, implemented the envisaged measures to reduce the risks to the rights and freedoms of data subjects;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

a.6) (AND) have consulted the Competent Data Protection Authority and recorded the communication, where the DPIA indicates that the processing would result in a high risk and no measures were taken to mitigate the risk.

GI.8.2.2 DPIA content requirements *(GDPR Art. 35.7) (C; S; A)*

A) The DPIA shall contain at least the following elements:

a.1) the systematic description of the envisaged processing operations for which a DPIA is performed;
a.2) (AND) the purposes for processing personal data;
a.3) (AND) where applicable, the legitimate interest pursued by the Controller in relation to the processing;
a.4) (AND) an assessment of the necessity and proportionality of the processing in relation to the purposes;
a.5) (AND) the assessment of the risks to the freedoms and rights of the data subjects;
a.6) (AND) the measures envisaged to address the risks, including, where applicable safeguards, security measures and mechanisms, taking into account the rights and legitimate interests of data subjects and other persons concerned;
a.7) (AND) where applicable, the recommendation to consult the Competent Data Protection Authority in the EEA.

GI.8.2.3 Data subjects involvement requirement *(GDPR Art. 35.9) (C; S; A)*

A) The Applicant shall keep records of the views of data subject and/or representatives consulted for the data protection impact assessment (or documented justification for not involving data subjects or their representatives).

GI.8.2.4 DPIA review in case of change of risks *(GDPR Art. 35.1.m) (C; G; A)*

A) The Applicant shall have rules or procedures in place to review the DPIA, or its decision to not perform a DPIA, whenever the scope or purpose of the data processing of the Target of Evaluation is substantially modified or exposed to new risks.

GI.8.2.5 Duty to consult the Competent Data Protection Authority in case of identified high risk *(GDPR Art. 36) (C; S; A)*

IF a DPIA identified residual high risks for the rights or freedom of data subjects, THEN:

A) The Controller shall have:

a.1) informed and consulted the Competent Data Protection Authority on the identified risks;
a.2) (AND) received the opinion of the Competent Data Protection Authority;
a.3) (AND) where applicable, implemented the recommended actions mentioned in the opinion.
a.4) (AND) notified the Competent Data Protection Authority on the implemented actions as mentioned in the opinion of the Authority;
a.5) (AND) recorded, with date and time, the communication and results of the communication with the Competent Data Protection Authority.

Subject to copyrights

GI.9 Data Protection Offices (DPO)

GI.9.1 Designation of the Data Protection Officer

GI.9.1.1 Designation of the data protection officer *(GDPR ART. 37.1) (CP; G; A)*

A) The Applicant shall have designated a Data Protection Officer.

GI.9.1.2 DPO requirements (GDPR Art. 37.5) (CP; G; A)

A) The data protection officer of the Applicant shall have the necessary professional qualities, including:

a.1) a formal qualification in EEA data protection law and practices, including the GDPR;
a.2) (OR) practical experience of minimum 5 years in applying data protection law, including the GDPR.

GI.9.1.3 DPO contact details communication *(GDPR Art. 37.7) (CP; G; A)*

A) The contact details and/or mechanism to communicate with the DPO shall:

a.1) be published and available to the data subjects;
a.2) (AND) have been communicated to the Competent Data Protection Authority, where required by EU or EEA Member State law of the Data Exporter.

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.9.2 Position of the data protection officers

GI.9.2.1 DPO mandate communication *(GDPR Art. 38.1) (CP; G; A)*

A) The Applicant shall have rules, policies, or procedures in place that:

a.1) request employees and management to involve the DPO in a timely manner in all data protection issues;

a.2) give authority and effective access to personal data to the DPO for monitoring the compliance of personal data processing operations.

GI.9.2.2 DPO support (GDPR Art. 38.2) (CP; G; A)

A) The Applicant shall have allocated resources for the DPO to enable them to perform their tasks and maintain their expertise (e.g. training and capacity building).

GI.9.2.3 DPO independence (GDPR Art. 38.3) (CP; G; A)

A) The Applicant shall have adopted rules, policies, or contractual clauses:

a.1) to protect the autonomy and independence of the DPO in performing their tasks;

a.2) (AND) to prevent a dismissal or penalization of the DPO in the performance of his/her tasks;

a.3) (AND) to enable the DPO to directly report to the highest management level of the Applicant.

GI.9.2.4 Data subjects access to the DPO *(GDPR Art. 38.4) (CP; G; A)*

A) The Data Subjects shall be able to contact the DPO regarding all issues related to their personal data processing and to exercise their rights.

GI.9.2.5 DPO contractual clauses *(GDPR Art. 38.5; 38.6) (CP; G; A)*

A) The contract with the DPO shall include clauses:

a.1) to bind the DPO to secrecy or confidentiality, even after the end of their contract, concerning the performance of his or her tasks;

a.2) (AND) to authorise the DPO to cooperate and communicate with Competent Data Protection Authorities;

a.3) (AND) to bind the DPO avoid or report conflict of interest in the performance of their duties.

GI.9.2.6 Appropriate DPO work time *(GDPR Art. 38.2) (CP; G; A)*

A) The Applicant shall have assessed and documented the required work time for the DPO considering the performance of his/ her tasks.

GI.9.3 Tasks of the data protection officer

GI.9.3.1 DPO tasks and duties *(GDPR Art. 39.1) (CP; G; A)*

A) The Applicant shall demonstrate that the following tasks have been assigned to the DPO:

a.1) to inform and advise the Applicant and its employees involved in data processing of their obligations regarding data protection;

a.2) (AND) to monitor the risks and compliance of data processing with the applicable data protection regulations, policies, and this certification;

a.3) (AND) to raise awareness and train of staff involved in processing operations;

a.4) (AND) to monitor data protection audits;

a.5) (AND) to provide advice on the performance of the data protection impact assessment and monitor its performance;

a.6) (AND) to cooperate with and act as the contact point with the Competent Data Protection Authority;

a.7) (AND) to act as a contact point for Data Subjects relating to all aspects regarding their personal data processing, including exercising their rights.

GI.9.3.2 Duty to train personnel on data protection *(GDPR Art. 39) (CP; G; A)*

A) The Applicant shall have a policy, rules or procedure in place to periodically train its personnel having permanent or regular access to personal data, at least on an annual basis.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.10 Transfers of personal data to third countries or international organizations (if applicable)

IF any personal data processed in the Target of Evaluation is onwards transferred (or made accessible), THEN:

GI.10.1 General obligations for international transfers of personal data by the Applicant to third countries or to international organizations

GI.10.1.1 Mapping of data flows and identification of transfers outside the EEA *(GDPR Art. 44; 46; 48; 49) (CP; S; A)*

A) The Applicant shall have a clear mapping or record of all personal data flows in scope of the ToE and identified transfers to third countries and to international organisations.

AND

B) The Applicant shall have assessed and recorded the ground for transfer of personal data falling in scope of the ToE, taking into account the obligation not to undermine the level of protection of the personal data as provided within the EEA.

AND

C) IF no Adequacy Decision of the European Commission is in force, THEN the Applicant shall assess and record that it only transfers personal data to third countries outside the EEA or an international organisation where:

c.1) appropriate safeguards, including supplementary measures if needed, have been taken;

c.2) (AND) enforceable data subject rights and effective legal remedies are available for the data subjects.

AND

D) IF the Applicant is a Processor, THEN there shall be rules or a procedure in place to ensure that the transfer only takes place on written instruction of the Controller.

GI.10.1.2 Transfer mechanism outside the EEA *(GDPR Art. 44) (CP; S; A)*

IF any personal data processed in the Target of Evaluation are transferred to third countries or to international organisations, THEN:

A) The third country to which the data are transferred shall benefit from an adequacy decision.

OR

B) In the absence of an adequacy decision, the transfer to a third country shall be based on appropriate safeguards and comply with the complementary criterion GI.10.1.3, GI.10.1.4, and GI.10.1.5.

OR

C) In the absence of an adequacy decision and appropriate safeguards referred to under case B, the data transfer shall be based on derogations for specific situations and comply with the complementary criterion GI.10.1.7.

GI.10.1.3 Transfer outside the EEA based on appropriate safeguards *(GDPR Art. 46) (CP; S; A)*

IF personal data are transferred to third countries (or to international organisations), on the basis of appropriate safeguards, THEN:

A) The Controller or Processor receiving these data in the third country shall have a procedure, rules, or mechanism in place to:

a.1) audit at least once a year the security of its infrastructure that processes and/or stores the data of the Target of Evaluation;

a.2) (AND) enable the data subjects to enforce their rights and to access effective legal remedies from the controller or processor located in the third country.

AND

B) The Applicant shall provide information to the data subject on how they can exercise their rights with regards to the processing of their data in the third countries involved in the processing.

AND

C) The DPO of the Applicant shall have assessed and confirmed that the data subjects can effectively exercise their rights and access legal remedies.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

GI.10.1.4 Use of a recognised mechanism for appropriate safeguards *(GDPR Art. 46.1; 46.2) (CP; S; A)*

IF any data processed in the Target of Evaluation is transferred to any third country or to an international organisation on the basis of appropriate safeguards, THEN:

A) The Applicant shall demonstrate that the data transfer benefits from appropriate safeguards (pursuant to Art. 46 GDPR) regarding the processing in question.

GI.10.1.5 Transfer Impact Assessment *(GDPR Art. 46) (CP; S; A)*

IF any personal data processed in the Target of Evaluation is onwards transferred to any third country or to an international organisation without adequacy decision applicable to the intended data transfer, THEN:

A) The Applicant shall have performed a Transfer Impact Assessment to assess if:

a.1) the access and processing by the public authorities of the third country is based on clear, precise and accessible rules;

a.2) (AND) there are mechanisms in place to respect and comply with the principles of necessity and proportionality of the data processing;

a.3) (AND) the authority of the country (and/or the international organisation) has established oversight mechanisms;

a.4) (AND) there are effective remedies made available to the Data Subjects;

a.5) (AND) the safeguards put in place by the transfer tools are effectively implemented;

a.6) (AND) the transfer undermines the level of protection of the transferred data.

AND

B) The Applicant shall have:

b.1) adopted supplementary measures to address the identified concerns in order to ensure that the level of protection of the transferred data is not undermined;

b.2) (AND) set in place an effective procedure or measure to re-assess the Transfer Impact Assessment on a regular basis.

AND

C) IF the Applicant is a Data Processor acting on behalf of the Data Controller, THEN the Transfer Impact Assessment shall be performed in accordance with the Data Controller's instructions and shall be shared with them.

Subject to copyrights

GI.10.1.6 Binding and Enforceable Commitment of the Data Importers in countries of onwards transfers *(GDPR Art. 42) (CP; S; A)*

IF any personal data processed in the Target of Evaluation is onwards transferred to any third country or international organisation without adequacy decision on the basis of a certification mechanism or a code of conduct, THEN:

A) The Applicant shall have binding and enforceable commitments of its Data Importers to apply the appropriate safeguards set forth in the certification or the code of conduct, including as regards rights of the data subjects.

GI.10.1.7 Transfer outside the EEA based on derogations for specific situations *(GDPR Art. 49) (CP; S; A)*

IF personal data are transferred to third countries or international organisations without adequacy decision (Art. 45 GDPR) and without appropriate transfer tool (Art. 46 GDPR), as a derogation for specific situations, THEN:

A) The transfer shall be based on consent where:

a.1) the data subjects shall have been informed about the country or international organisation to which data transfer is intended;

a.2) (AND) the data subjects shall have been informed of the risks for their rights and freedoms due to the absence of adequacy decision and appropriate safeguards;

a.3) (AND) the data subjects shall have given an explicit and valid consent to the proposed transfer;

OR

B) The necessity of the data transfer shall be evaluated and established for:

b.1) the performance of a contract agreed by the data subject or to implement pre-contractual measures taken at the request of the data subject;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

b.2) (OR) important reasons of public interest, based on a legal basis recognised in the jurisdiction of the EEA Data Controller acting as Data Exporter;
b.3) (OR) the establishment, exercise or defence of legal claims;
b.4) (OR) the protection of vital interests of natural persons.

OR

C) The transfer shall be made from a public register:
c.1) intended to provide information to the public according to applicable EU law or EEA Member State law;
c.2) (AND) open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

GI.10.1.8 Transfer based on Adequacy Decision *(GDPR Art. 46) (CP; S; A)*

IF the Applicant is transferring data to third countries on the basis of an adequacy decision, THEN:
A) There shall be rules, policies or mechanisms in place:
a.1) to check at least once a year that the adequacy decisions continue to be valid;
a.2) (AND) to suspend the transfer of data to countries that have lost their adequacy decision until a transfer impact assessment has been performed and concluded that the transfer can be continued.

GI.11 Binding and Enforceable Commitments and Assessment of the Third Country Law Applicable to the Applicant Acting as Data Importer

GI.11.1 Applicants Acting as Data Importer from a Third Country

IF the processing activities within the ToE are carried out by an Applicant based in a third country acting as a Data Importer, THEN:

GI.11.1.1 Binding and Enforceable Commitments for Data Importers *(GDPR Art. 46.2) (CP; S; A)*

A) The Applicant shall provide a Binding and Enforceable Commitments model to be signed with each Data Exporter and binding them by the following obligations:
a.1) to apply safeguards to the processing of personal data to ensure compliance with its obligations towards the Data Exporter;
a.2)(AND) to recognise, respect and facilitate the enforcement of the data subjects' rights as third party beneficiaries;
a.3) (AND) to be liable for any harm suffered by data subjects due to the Data Importer's non-compliance with the certification;
a.4) (AND) to cooperate with the Data Protection Authorities competent for the Data Exporters, including by accepting their audits and inspections, by taking into account their advice, and by abiding by their decisions;
a.5) (AND) to notify the Certification Body and the Data Exporter(s) in case of regulatory changes that may compromise the protection of the transferred data and/or the data subjects' rights and freedoms;
a.6) (AND) in case of requests for information from third country authorities, to review the legality of the request, to promptly inform the Data Exporter, and to minimise the information disclosed;
a.7) (AND) to protect data against massive and indiscriminate transfers as a result of access requests by third country public authorities;
a.8) (AND) to notify the Data Exporter and its Data Protection Authority of any measures taken by the certification body in response to a detected violation of the certification rules by the Applicant;
a.9) (AND) on request, to share information on the technical and organisation measures in place with the Certification Body and the Data Protection Authority of the Data Exporter;
a.10) (AND) to comply with the requirements of the certification criteria;
a.11) (AND) the right for the exporter to enforce against the data importer holding a certification the rules under the certification as a third-party beneficiary;
a.12) (AND) to recognize the right for the data subjects to enforce against the data importer holding a certification the rules under the certification as third-party beneficiaries;

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

a.13) (AND) to abide by any binding decision issued in EEA Member States' jurisdiction and courts related to the certification;
a.14) (AND) to only process the received data while the certificate is valid;
a.15) (AND) to return and/or delete the received data if the certificate is withdrawn;
a.16) (AND) to warrant that it has no reason to believe the laws and practices in the third country applicable to the processing in the ToE, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent it from fulfilling its commitments under the Certification;
a.17) (AND) to inform the Data Exporter of any relevant changes in the legislation or practice in this regard.

GI.11.1.2 Assessment of Binding and Enforceable Commitments *(GDPR Art. 46.2) (CP; S; A)*

A) The Binding and Enforceable Commitment of GI.11.1.1 shall be:
a.1) made in writing;
a.2) (AND) assessed to ensure that it is binding and enforceable;
a.3) (AND) signed by both the Applicant and the Data Exporter before any personal data transfer takes place on the basis of the Certification.

GI.11.1.3 Assessment of Third Country Law by the Data Importer and implementation of supplementary measures *(GDPR Art. 46.1) (CP; S; A)*

IF the Applicant is based in a third country without adequacy decision, THEN:
A) The Applicant shall have:
a.1) analysed the local laws and practices in its country and identified the potential impact on the rights and freedoms of the Data Subject whose data may be imported;
a.2) (AND) adopted supplementary measures to ensure that the level of protection of the transferred data is not undermined;
a.3) (AND) rules, procedures or policies to make its written analysis on the local laws and practices available to the Certification Body and to competent Data Protection Authorities on request;
a.4) (AND) warranted it has no reason to believe that the laws and practices in the third country applicable to the processing at stake, including any requirements to disclose personal data or measures authorising access by public authorities, prevent it from fulfilling its commitments under the certification.

AND

B) IF the Applicant is acting as Data Processor, THEN there shall be rules, a policy, or a procedure in place to:
b.1) comply with the Data Controller's instructions when performing the Transfer Impact Assessment and implementing the supplementary measures;
b.2) (AND) suspend or stop the data transfer in case the incoming personal data are not sufficiently protected any more.

Subject to copyrights

GI.11.1.4 Data Importer procedures *(GDPR Art. 46.2) (CP; G; A)*

A) The Applicant shall have procedures in place with a description of the steps to be taken:
a.1) to notify the Data Exporter and take appropriate supplementary measures in case it becomes aware of legislations that would prevent compliance with its obligations under the certification;
a.2) (AND) to review the legality of access requests, promptly inform the Data Exporter, and minimise the information disclosed, in case of requests for information from third country authorities;
a.3) (AND) to protect the imported data against massive and indiscriminate transfers as a result of access requests by non-EEA authorities.

GI.11.1.5 Data in transit risk assessment and supplementary measures determination *(GDPR Art. 32) (CP; S; A)*

IF the Target of Evaluation includes data in transit under the control of the Data Importer, THEN:
A) Supplementary measures to mitigate the risks shall be identified, implemented, and documented in a report including:
a.1) the measures adopted to protect the data in transit against active and passive attacks on the sending and receiving systems;
a.2) (AND) the roles and obligations of the implementing parties;
a.3) (AND) the planning, timing, and duration of implementation;

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

a.4) (AND) the analysis of any residual risks and recommended measures to address them.

GI.11.1.6 Data in transit additional encryption-related requirements *(GDPR Art. 32) (CP; S; A)*

IF the Applicant's risk assessment has concluded that encryption of data in transit is needed to preserve the rights and freedom of the Data Subjects, THEN:

A) The risk of unauthorized access to the data in transit for the data subjects shall be identified and assessed in a report that shall:

a.1) take into account the risk of unauthorized access, including by public authorities;

a.2) (AND) determine the level and scope of encryption required according to the identified risks;

a.3) (AND) specify the encryption policy for data in transit and its justification.

AND

B) There shall be a policy, procedure, or mechanism in place:

b.1) to ensure that encryption algorithms are implemented by up-to-date software without known vulnerabilities;

b.2) (AND) to ensure that encryption keys are managed by the Data Exporter or a third-party trusted by the Data Exporter;

b.3) (AND) to review supplementary measures at least on an annual basis to ensure they remain up-to-date with the state of the art.

AND

C) The Applicant shall warrant that it is neither exposed to the obligation to disclose the cryptographic keys nor to modify the equipment used for the transit in order to undermine its security properties.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

T - TECHNICAL AND ORGANIZATIONAL MEASURES CHECKS & CONTROLS (TOM)

All rights reserved. The content of this document is subject to intellectual property rights, including registered copyright and cannot be re-used, altered, adapted, copied or replicated in any format without explicit authorisation by the European Centre for Certification and Privacy ('ECCP').

The following criteria are complemented by complementary criteria and resources which can be accessed through the Europrivacy Community and Resources website.

T.1 Core Security Requirements

T.1.1 Data Access Restriction

T.1.1.1 Access control policy and registry *(GDPR Art. 32) (CP; G; A)*

A) The Applicant shall have established and documented an access control policy that is defined around roles and responsibilities, which takes into account the processing of personal data.
AND
B) The access control policy shall clarify at least the following:

- b.1) who needs to access and use the data on a role basis, in line with the principle of least access privilege;
- b.2) (AND) information on electronic and physical access to personal data;
- b.3) (AND) security requirements in relation to the information classification scheme, including personal data;
- b.4) (AND) information on access control responsibilities.

AND
C) The Applicant shall keep an updated registry of access rights of its employees who can access the personal data.
AND
D) The Applicant shall have a procedure, policy or mechanism in place to:

- d.1) regularly review the registry of user access rights;
- d.2) (AND) record individual changes and broader system access rights;
- d.3) (AND) regularly audit access rights, including implementing, assigning or revoking access rights;
- d.4) (AND) to register and de-register users.

AND
E) The access right policy shall be enforced and verifiable for both:

- e.1) physical access to the place where the data are stored
- e.2) electronic access to the personal datasets.

T.1.1.2 Access rights minimization (least privilege) *(GDPR Art. 25; 32) (CP; G; A)*

A) Access rights shall be limited and delivered on a need basis in conformity with the "Least privilege" principle.
AND
B) Least privilege policy shall encompass:

- b.1) physical access to facilities and systems processing data;
- b.2) (AND) general access to systems and applications processing data;
- b.3) (AND) specific data access.

T.1.1.3 Password policy (GDPR Art. 32) (CP; G; A)

A) There shall be a password policy in place that specifies a minimum length, complexity requirements, and renewal frequency (or alternative measure), to ensure password reliability.
AND
B) Where required by law, the password policy to access stored data shall be compliant with the national laws and regulations.

T.1.1.4 Physical access restriction *(GDPR Art. 25; 32) (CP; G; A)*

A) The Applicant shall have:

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

a.1) identified the locations and devices where personal data is stored or otherwise accessed or processed;
a.2) (AND) assessed the risks for each location and category of device;
a.3) (AND) implemented effective access control mechanisms to mitigate those risks.

T.1.1.5 Access and transfer logs *(GDPR Art. 32) (CP; G; A)*

A) The Applicant shall have:
a.1) identified any information that needs to be logged, based on the risk assessment performed;
a.2) (AND) implemented security measures to protect the logs, including encryption;
a.3) (AND) determined the logs' retention period, in line with data minimization requirements.
AND
B) The Applicant shall have a monitoring system, a mechanism or a process in place to record and keep a log of:
b.1) the purpose and use of the data;
b.2) (AND) access to personal data and the systems containing the data by employees and agents of the Applicant;
b.3) (AND) remote access to personal data and related systems within the EEA and from third countries;
b.4) (AND) information on transfer rules for all types of personal data transfer facilities within the organization, and between the organization and other parties;
b.5) (AND) any changes to the personal data and related systems, including modifications, alterations, and deletions.

T.1.1.6 Bring Your Own Device policy *(GDPR Art. 32) (CP; G; A)*

IF employees are using their own devices to access or otherwise process personal data, THEN:
A) The Applicant shall have written rules, or policies in place that:
a.1) specify the data that may be accessed;
a.2) (AND) specify the permitted devices;
a.3) (AND) specify the appropriate use of personal mobile devices to limit the risks for data subjects;
a.4) (AND) provides for access controls and limitations to the use of mobile devices to ensure the data remains protected;
a.5) (AND) includes security measures to protect the data to address the identified risks;
a.6) (AND) are known by the employees who have access to the servers.
AND
B) The Applicant shall have procedures or mechanisms in place to:
b.1) implement the policy;
b.2) (AND) document the devices used and the corresponding access rights;
b.3) (AND) document the security measures that are in place to address the identified risks;
b.4) (AND) regularly assess and update the access rights granted and security measures in place, at least when a device is added or removed.

Subject to copyrights

T.1.1.7 Automated session logout *(GDPR Art. 25; 32) (CP; G; A)*

A) Access to systems used for processing personal data shall be protected by an automated session log out mechanism.
AND
B) The Applicant shall document and justify the timeframe after which sessions shall be terminated to address any risks identified.

T.1.1.8 Multi-factor authentication *(GDPR Art. 32) (CP; S; A)*

A) The Applicant shall have:
a.1) assessed the need to have multi-factor authentication in place, taking into account the risks related to the data processing;
a.2) (AND) where deemed necessary, put in place multi-factor authentication for its employees, agents and other users.

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

T.1.2 Data Encryption, Pseudonymization and Anonymization

T.1.2.1 Encryption (GDPR Art. 32.1.a) (CP; S; A)

IF the Applicant's risk assessment has concluded that data encryption is required to ensure a level of security that addresses the risk that the processing of personal data poses to the rights and freedoms of natural persons, THEN:

A) The risk of unauthorized access to electronic data for the data subjects shall be identified and assessed in a report that shall:

a.1) take into account the risk of unauthorized access, including by public authorities, for the rights and freedoms of natural persons;

a.2) (AND) take into account risks related to data transmission and data at rest;

a.3) (AND) take into account risks related unauthorized access to or misuse of encryption keys;

a.4) (AND) determine the level and scope of encryption required according to the identified risks;

a.5) (AND) specify the encryption policy for the processed data;

a.6) (AND) identify any residual risks and measures to address them.

AND

B) There shall be a policy, procedure, or mechanism in place:

b.1) to ensure that encryption algorithms are implemented by up-to-date software without known vulnerabilities;

b.2) (AND) to protect encryption keys and store them separately from the encrypted data;

b.3) (AND) maintain a record of access rights to the encryption keys based on least priviledge access right principle;

b.4) (AND) to review supplementary measures at least on an annual basis to ensure they remain up-to-date with the state of the art.

AND

C) Data shall be encrypted in accordance with the specified encryption policy.

AND

D) The Applicant shall have a procedure, rules, or policies in place to periodically review and update the encryption process and any residual risks, at least when changes are implemented in the technical measures.

T.1.2.2 Backups encryption (GDPR Art. 25; 32) (CP; G; A)

IF the Applicant's risk assessment has concluded that backup encryption is needed to ensure a level of security that addresses the risk that the processing of personal data poses to the rights and freedoms of natural persons, THEN:

A) The backup files containing personal data shall be encrypted.

T.1.2.3 Pseudonymization *(GDPR Art. 32) (CP; G; A)*

IF the Applicant's risk assessment has concluded that data pseudonymization is required to ensure a level of security that addresses the risk that the processing of personal data poses to the rights and freedoms of natural persons, THEN:

A) Personal data shall be pseudonymized.

AND

B) The Applicant shall document the pseudonymization process, including:

b.1) the technique used along with the justification for such choice;

b.2) (AND) the configuration parameters;

b.3) (AND) the measures for storing and protecting the re-identification keys and any lookup tables;

b.4) (AND) the expected residual risks and the additional measures to mitigate them.

AND

C) The Applicant shall demonstrate that:

c.1) the deployed pseudonymization techniques produce non-reversible outputs without access to the additional information;

c.2) (AND) pseudonyms cannot be linked back to natural persons without the re-identification key using reasonably likely means;

c.3) (AND) the technique applied is appropriate for the risk associated to each category of personal data.

AND

D) The re-identification key(s) shall be stored separately from the pseudonymized data.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

AND

E) The Applicant shall have a procedure, rules, or policies in place to periodically review and update the pseudonymization process and any residual risks, at least when changes are implemented in the technical measures.

T.1.2.4 Anonymization (GDPR Art. 25; Rec. 26) (CP; S; A)

IF the Applicant's risk assessment has concluded that data anonymisation is required to ensure a level of security that addresses the risk that the processing of personal data poses to the rights and freedoms of natural persons, THEN:

A) Personal data shall be anonymized.

AND

B) The Applicant shall ensure that the anonymized data cannot be linked to any data subjects, taking into account all means reasonably likely to be used for re-identification.

AND

C) The Applicant shall document the anonymization process, including:

c.1) the techniques used and the justification for such choice;

c.2) (AND) the expected residual risks and the additional measures to mitigate them.

AND

D) The Applicant shall demonstrate that the anonymized datasets prevent re-identification of data subjects by:

d.1) singling individual data subjects out;

d.2) (AND) linkability between records within the dataset or across different datasets;

d.3) (AND) interference of sensitive or unique attributes.

AND

E) The Applicant shall have a procedure, rules, or policies in place to periodically review and update the anonymization process and any residual risks, at least when changes are implemented in the technical measures.

T.1.2.5 Cryptographic Policy *(GDPR Art. 32) (CP; G; A)*

IF the data in the ToE are protected by encryption methods, THEN:

A) The Applicant shall have a cryptographic policy in place that specifies:

a.1) the cryptographic algorithms to be used for each data category, including the justification of such decisions;

a.2) (AND) the generation, update, distribution (where relevant), installation, usage, separation, escrow, and revocation (destruction) of keys;

a.3) (AND) the adequate key length requirements;

a.4) (AND) the time period after which the keys must be changed or the conditions under which keys must be rotated;

a.5) (AND) the storage requirements for the keys;

a.6) (AND) the measures in place to protect the keys, including backups;

a.7) (AND) the access rights to the keys.

AND

B) There shall be a procedure, rules, or mechanisms in place to review the cryptographic policy at least on an annual basis to ensure it remains up-to-date with the state of the art.

AND

C) The Applicant shall document the implementation of its cryptographic policy.

T.1.3 Connectivity Checks for Internet Access

IF the Target of Evaluation includes Internet access, THEN:

T.1.3.1 HTTPS enabled (GDPR Art. 32) (CP; G; A)

A) HTTPS shall be enabled by default for accessing the web interface.

T.1.3.2 SDNS enabled (GDPR Art. 32) (CP; G; A)

A) The Applicant shall have:

a.1) assessed the risks related to the processing of the data through the web interface;

a.2) (AND) implemented mitigation measures to address any risks identified, including Secure DNS (DNSSEC) for resolving public domain names resolution to prevent manipulation or misdirection.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

T.1.3.3 SSL (GDPR Art. 32) (CP; G; A)

A) Unsecure SSL shall NOT be used.

T.1.3.4 TLS (GDPR Art. 32) (CP; G; A)

A) Unsecure TLS shall NOT be used.

T.1.3.5 SSH (GDPR Art. 32) (CP; G; A)

A) Unsecure SSH shall NOT be used.

T.1.3.6 Backward incompatibility *(GDPR Art. 32) (CP; G; A)*

A) Backward compatibility with unsecure SSL or TLS versions shall be disabled.

T.1.3.7 Wireless Communication Networks *(GDPR Art. 32) (CP; G; A)*

A) The connection to the Wireless Communication Network shall be protected by password.
AND
B) The Wireless Communication Network accessible to visitors shall be separated from the WiFi networks used for internal purpose.

T.1.4 Other Security Measures

T.1.4.1 Confidentiality, Integrity, Availability, and Resilience (GDPR Art. 32) (CP; G; A)

A) The Applicant shall have a continuity plan in place to ensure the availability and integrity of personal data, and resilience of processing systems and services in the ToE in case of security incidents, including:

a.1) for ensuring the ongoing availability and integrity of the personal data;
a.2) (AND) for ensuring resilience of processing systems and services.

AND

B) The plan shall include at least the following information:

b.1) the purpose and scope of the plan;
b.2) (AND) the roles and corresponding responsibilities within the Applicant's organization;
b.3) (AND) the critical processes and systems;
b.4) (AND) the measures in place to address the risks related to data confidentiality, integrity, availability, and resilience of processing systems and services;
b.5) (AND) the procedure to respond to security incidents;
b.6) (AND) the data recovery procedures.

AND

C) The Applicant shall regularly review and update the continuity plan, at least on an annual basis.

T.1.4.2 Backup policy and recovery test *(GDPR Art. 32) (CP; G; A)*

A) There shall be a backup policy specifying:

a.1) the frequency of the back-ups;
a.2) (AND) the data that is backed up;
a.3) (AND) the backup method, in line with data minimization requirements;
a.4) (AND) the storage location of the backed up data;
a.5 (AND) the measures in place to protect the back-up files from unauthorised access.

AND

B) A Procedure shall be in place to perform a data recovery test at least once a year.

AND

C) Where recovery tests identify issues to be addressed, the Applicant shall have taken action on the identified issues.

T.1.4.3 Duty to backup (GDPR Art. 32.1.c) (CP; S; A)

A) The Applicant shall back-up electronic personal data in intervals which provide for the ability to restore the availability and access to personal data in case of a security incident in a timely manner, and at least once a week.

AND

B) The back-ups shall be:

b.1) stored in a secure location;
b.2) (AND) accessed only by authorised personnel.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.

T.1.4.4 Regular server devices and systems updates *(GDPR Art. 32) (CP; G; A)*

A) There shall be a procedure, configuration or a mechanism in place to ensure that the Applicant:

a.1) assesses the need to update servers, devices and systems used to process or store personal data based on their associated risks:

a.2) (AND) patches them on a regular basis;

a.3) (AND) monitors critical security patches issued by the respective provider and installs them any time there is a critical security patch available without undue delay.

T.1.4.5 Data continuity (GDPR Art. 32) (CP; G; A)

A) Where such risks exist, protection measures shall be set in place to protect the physical and logical environments in which personal data is stored or processed (including servers, devices and copies) to ensure data continuity.

AND

B) The measures shall:

b.1) be based on the documented risk assessment performed by the Applicant;

b.2) (AND) address foreseeable threats to the availability, integrity and confidentiality of the data (including fire, flood, power outage, and other relevant incidents);

b.3) (AND) form part of the plan for disaster recovery and business continuity to support the timely restoration of affected systems and data.

T.1.4.6 Network security policy *(GDPR Art. 25; 32) (CP; G; A)*

A) The Applicant shall have a network security policy in place that:

a.1) identifies the servers, devices and systems where personal data is processed or stored, and for which a network security policy is required based on their risks;

a.2) (AND) identifies the network security controls that are required to address the risks, including firewalls, intrusion detection and prevention mechanisms;

AND

B) There shall be a policy, procedure, or mechanism in place to regularly check and control the network security policy and the measures implemented.

T.1.4.7 Updated antivirus *(GDPR Art. 32) (CP; G; A)*

A) A security solution, containing at least an antivirus application, shall be deployed to protect the servers, mobile and terminal devices that are used for the processing in the Target of Evaluation.

AND

B) A policy, procedure or a mechanism shall be in place to ensure that the security solution is kept up-to-date.

T.1.4.8 PEN Test or equivalent *(GDPR Art. 32) (CP; G; A)*

IF the Applicant's risk assessment has concluded that a penetration test (PEN test) or equivalent is required to ensure a level of security that addresses the risk that the processing of personal data poses to the rights and freedoms of natural persons, THEN:

A) The nature, scope, and frequency of the required tests shall be determined and justified according to the identified risks and the monitoring of security incidents (See T.1.4.9).

AND

B) The Applicant shall:

b.1) perform tests to assess the exposure to data breach according to the determined frequency (at least after significant changes that may affect the security);

b.2) (AND) document the results of the tests;

b.3) (AND) have a procedure in place to ensure that the results of the tests are addressed.

T.1.4.9 Security Incidents Detection *(GDPR Art. 32) (CP; G; A)*

A) The Applicant shall have policies, rules, procedures, or mechanisms in place to detect, report and remediate security incidents.

Subject to copyrights

© European Centre for Certification and Privacy (ECCP), all rights reserved. Europrivacy is an international trademark registered in several jurisdictions.