

G - EUROPRIVACY GDPR CORE CRITERIA

Like ISO standards, this document and its content are subject to intellectual property rights, including registered copyright. It cannot be used, altered, adapted, copied or replicated in any format without explicit authorization by the [European Centre for Certification and Privacy](#).

If you wish to use these criteria, you can register on the [Europrivacy Community and Resources website](#). It will give you access to all required resources and documentation to use Europrivacy, including templates, editable forms and detailed guidance on the use of the criteria. Moreover, your subscription will support our effort to extend Europrivacy and to support its community of users.

G.1 Lawfulness of Data Processing

IF the Applicant is the Data Controller of the personal data processed in the Target of Evaluation, THEN:

G.1.1 Lawfulness of processing

G.1.1.1 Lawfulness assessment of the processing [C, S, A]

A) There shall be a written report or document demonstrating that the data processing in the Target of Evaluation has been assessed as lawful by the Applicant's DPO or by a legal expert with adequate expertise.

AND

B) Where the lawfulness is conditional to corrective actions, the Applicant shall have implemented them.

AND

C) The assessment (or reassessment) report of lawfulness shall:

- c.1) cover all personal data processing specified in the Target of Evaluation;
- c.2) (AND) indicate the lawfulness basis of the data processing;
- c.3) (AND) where applicable, include the justifications documents or references;
- c.4) (AND) have been performed within the last 12 months before the initial assessment.

G.1.1.2 Lawfulness justification [C, S, A]

The data processing shall comply with at least one of the following justifications:

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

- a.1) shall be collected before processing their personal data;
- a.2) (AND) shall be given by the data subjects in a clear and express manner (with a clear affirmative action).

OR

B) The data processing shall be required for the performance of the services specified in the contract.

OR

C) The Applicant shall demonstrate the existence of a legal obligation for the data processing.

OR

D) The data processing shall be required to protect vital interests of data subjects (i.e. life, health);

OR

E) The Applicant shall demonstrate that the data processing:

- e.1) is based on public interest or official authority;
- e.2) (AND) with the documentation on the legal basis for such public interest or official authority.

OR

F) The data processing shall be based on legitimate interests for which the Applicant shall demonstrate:

- f.1) the written description of the claimed legitimate interest;
- f.2) (AND) the DPO or a legal expert with adequate expertise has assessed in writing the impact of the data processing on the rights and freedoms of the data subjects;
- f.3) (AND) the DPO or a legal expert with adequate expertise has concluded in writing that the legitimate interest is not overridden by the rights and freedoms of the data subjects.

G.1.1.3 National Regulation Compliance [C, S, A]

A) A legal expert shall have assessed the compliance of the data processing with the complementary national obligations related to personal data protection applicable to the Applicant and provided its assessment in a National Obligations Compliance Assessment Report (NOCAR).

AND

B) The NOCAR shall contain:

- b.1) a clear identification of the Target of Evaluation that has been assessed;
- b.2) (AND) the description of the qualification of the legal expert;
- b.3) (AND) the list of identified complementary national data protection obligations applicable to the Target of Evaluation;
- b.4) (AND) the evaluation of compliance of the Target of Evaluation with the identified complementary national obligations;
- b.5) (AND) where data are processed for archiving, research or statistical purpose, the technical and organisational measures in place to respect the fundamental rights and interests of the data subjects, in particular data minimisation measures;
- b.6) (AND) where the assessment concludes that actions are required to comply with the national obligations, these actions shall be documented

AND

C) The legal expert shall have:

- c.1) taken into account at least all applicable complementary national obligations listed in the National Data Protection Obligations profiles made available by ECCP;
- c.2) (AND) checked if other domain specific national laws and regulations are applicable;
- c.3) (AND) checked if the data processing requires a national authorization, and if so checked the validity of the required authorization.

AND

D) The NOCAR shall:

- d.1) be complete and consistent;
- d.2) (AND) conclude that the Target of Evaluation is complying with the national obligations.

AND

E) The Applicant shall have:

- e.1) committed to apply the measures documented in the NOCAR report over time;
- e.2) (AND) where applicable, established a detailed action plan to comply with the NOCAR recommended measures;
- e.3) (AND) where applicable, applied and documented the actions contained in the action plan that are required to comply with the national obligations.

G.1.1.4 Adequate qualification of the expert [C, S, A]

A) The legal expert who has prepared the National Obligations Compliance Assessment Report (NOCAR) shall have:

- a.1) a Master of Laws (LL.M.) or an adequate level of qualification, or a significant professional experience in data protection;
- a.2) (AND) a documented expertise or practice in the national law addressed by the NOCAR;
- a.3) (AND) knowledge in data protection law.

G.1.2 Complementary requirements for consent to be valid

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

G.1.2.1 Formal requirements for consent [C, S, A]

A) The consent of the data subject 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 subject 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 distinguishable from other matters;
- a.5) (AND) consent shall be collected before the Applicant processes their personal data;
- a.6) (AND) consent shall be given by the data subjects in a clear and express manner (with a clear affirmative action).

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;
- 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.

G.1.2.2 Absence of unnecessary constraints for consent [C, S, A]

A) IF the Target of Evaluation encompasses several distinct purposes of data processing, THEN the Applicant shall provide a granular consent mechanism enabling the data subject to freely select which purpose to consent with.

G.1.2.3 Right to withdraw consent [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.

G.1.3 Conditions applicable to a child's consent in relation to information society services

IF the Target of Evaluation includes Information Society Services offered directly to children below 16 years old, THEN:

G.1.3.1 Lawfulness of data processing of minors of age and Verification of parental consent [C, S, A]

A) The applicable limits of age for consent shall be clearly communicated to potential new data subjects involved in the data processing.

AND

B) There shall be a procedure and/or a mechanism:

- b.1) to request the age of data subjects that are minor of age;
- b.2) (AND) to block the collection of personal data of minors of age below the age of consent OR to request the consent of the holder of the parental responsibility for minor below the age of consent.

G.2 Special Data Processing

G.2.1 Adequacy of processing special categories of data

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

G.2.1.1 Special categories of data – DPO validation [C, S, A]

A) The DPO or an expert with adequate expertise shall have:

- a.1) assessed the risks and impact of processing the special categories of data on the rights, freedoms and legitimate interests of the data subjects;
- a.2) (AND) confirmed the lawfulness of the processing of the special categories of data, including with the applicable national obligations.

G.2.1.2 Legal basis for processing special categories of data [C, S, A]

The Applicant shall demonstrate that the processing of Special Categories of Personal Data in the Target of Evaluation is lawful according to at least one of the following justifications:

A) The Applicant shall demonstrate that the processing of the special categories of data is based on the explicit consent of the data subjects.

OR

B) The Applicant shall demonstrate that the processing of special categories of data is based on employment and social necessity.

OR

C) The Applicant shall demonstrate that the processing of special categories of data is based on vital interests where:

- c.1) vital interests of data subjects were at risk (life, health);
- c.2) (AND) the related data subjects or protected natural persons were physically or legally incapable of providing consent.

OR

D) The Applicant shall demonstrate that the processing of special categories of data is based on not-for-profit activities where:

- d.1) the Applicant is a non-for-profit entity;
- d.2) (AND) the processed data relate solely to the members and former members of the Applicant and/or to persons who have regular contacts with the Applicant in connection with its purposes;
- d.3) (AND) internal rules and/or procedures shall be in place to prevent that personal data are disclosed to third parties without data subject consent.

OR

E) The Applicant shall demonstrate that the processing of special categories of data is based on data that are manifestly made public by the data subjects.

OR

F) The Applicant shall demonstrate that the processing of special categories of data is necessary for the establishment, exercise, or defence of legal claims, or for court actions in their judiciary capacity.

OR

G) The Applicant shall demonstrate that the processing of special categories of data is necessary for reasons of public interest, where:

- g.1) the public interest shall be based on Union or Member State law;
- g.2) (AND) specific measures shall have been adopted to protect the fundamental rights and the interests of the data subjects.

OR

H) The Applicant shall demonstrate that the processing of special categories of data is necessary for medical or social care purpose, where:

- h.1) the processing shall relate to one of the following activities: preventive or occupational medicine; assessment of the working capacity of the employee; medical diagnosis; provision of health or social care or treatment; management of health or social care systems and services;
- h.2) (AND) the data shall be processed by or under the responsibility of a professional subject to the obligation of professional secrecy.

OR

I) The Applicant shall demonstrate that the processing of special categories of data is necessary for reasons of public interest in the area of public health where:

- i.1) the public interest in the area of public health shall be based on a legal basis;
- i.2) (AND) the data shall be processed by or under the responsibility of a professional subject to the obligation of professional secrecy.

OR

J) The Applicant shall demonstrate that the processing of special categories of data is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes where:

- j.1) the DPO shall have assessed and confirmed that the processed data are useful and proportionate for the declared purpose;
- j.2) (AND) public information shall be provided on the purpose of the data processing activities with a means of contact for the data subjects;
- j.3) (AND) specific measures shall have been adopted to protect the rights and interests of the data subjects, such as pseudonymisation and anonymisation techniques.

G.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:

G.2.2.1 Data to criminal convictions and offences [C, S, A]

A) The Applicant shall demonstrate that the processing of personal data related to criminal convictions and offenses:

- a.1) shall be carried out under the control of an official authority, or shall be specifically authorized by Union or Member State law that is clearly identified, or shall be strictly limited and based on a legitimate interest (such as recruitment processes);
- a.2) (AND) shall not constitute a comprehensive register of criminal convictions, except if kept under the control of official authority.

AND

B) The processing of data relating to criminal convictions and/or offences shall have been:

- b.1) assessed by a qualified legal expert as being compliant with the applicable national obligations;
- b.2) (AND) controlled and assessed as being compliant by the DPO;
- b.3) (AND) approved by the management of the Applicant.

G.3 Rights of the Data Subjects

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

G.3.1.1 Duty to inform in clear language [C, S, A]

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

- a.1) intelligible in a clear and plain language;
- a.2) (AND) available in the official national language of the Applicant;
- a.3) (AND) available in the language of the targeted data subjects.

AND

B) IF the Target of Evaluation is intended for processing personal data of minor of ages, THEN the DPO shall have assessed and validated the adequacy of the wording of the information with the ability of minor of ages to understand it.

G.3.1.2 Duty to facilitate data subject rights exercise [C, G, A]

A) The Applicant shall:

- a.1) inform the data subjects on how they can exercise their rights on the Applicant's website;
- a.2) (AND) have personnel trained on how to handle data subject requests.

G.3.1.3 Ensuring proper data subject rights management and recording [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) identify and authenticate the data subjects in case of uncertainty on their real identity;
- a.3) (AND) assess and verify that all conditions are satisfied to proceed with the request;
- a.4) (AND) comply with the request;
- a.5) (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 data subject requests with the date of reception;
- b.2) (AND) the communications with data subjects with their dates;
- b.3) (AND) the follow-up actions with their dates.
- b.4) (AND) where applicable, the reasons for not complying with received request.

G.3.1.4 Information without undue delay [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 for information received from the data subjects;
- a.2) (AND) reply to the received requests in no more than 30 days.

G.3.1.5 Electronic response [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.

G.3.1.6 Duty to inform and justify non action [C, G, A]

A) The Applicant shall have rules, procedures or a mechanism in place to inform and justify non-action to 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 30 days after receiving the request about:

- b.1) the reasons for not taking action;
- b.2) (AND) the possibility of lodging a complaint with a Supervisory Authority and the possibility of seeking a judicial remedy.

G.3.1.7 Free of charge [C, G, A]

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

AND

B) If the Applicant intends to charge the data subjects for non-justified or excessive requests, THEN it shall have a written procedure in place to:

- b.1) assess on factual criteria if the requests is reasonable 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 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.

G.3.1.8 Machine-readability of icons [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.

G.3.2 Information to be provided where personal data are collected from the data subject

IF the Target of Evaluation processes data that have been obtained directly from the data subjects [Except if an exemption can be demonstrated in conformity with G.3.2.3], THEN:

G.3.2.1 Duty to inform [C, S, A]

A) The information provided to the data subject at the time of data collection shall include at least the following information:

- a.1) the identity of the Controller;
- a.2) (AND) the contact details of the Controller;
- a.3) (AND) the contact details of the data protection officer (or contact mechanism);
- a.4) (AND) the purposes of processing;
- a.5) (AND) the legal basis for the processing;
- a.6) (AND) if applicable, the legitimate interests pursued by the Controller or by a third-party;
- a.7) (AND) the recipients or categories of recipients of the personal data;
- a.8) (AND) if personal data are likely to be transferred to any third country or to an international organisation, the list of non-European countries where the data are transferred;
- a.9) (AND) if personal data are likely to be transferred to any third country or to an international organisation, whether a valid adequacy decision applies to the data transfer;
- a.10) (AND) if personal data are likely to be transferred to any third country or to an international organisation, information on the safeguards measures adopted by the Controller to assess and minimize the risks for the data subjects and their rights when processed in third-countries;
- a.11) (AND) if automated decision-making and/or profiling is performed, meaningful information about the logic involved in the processing activities;
- a.12) (AND) if automated decision-making and/or profiling is performed, the significance of the processing activities;
- a.13) (AND) if automated decision-making and/or profiling is performed, the envisaged consequences of the processing activities;
- a.14) (AND) the retention period or the criteria for determining the retention period;
- a.15) (AND) information on the data subject's rights to access to personal data;
- a.16) (AND) information on the data subject's rights to rectification of personal data;
- a.17) (AND) information on the data subject's rights to erasure of personal data;
- a.18) (AND) information on the data subject's rights to restriction of data processing;
- a.19) (AND) information on the data subject's rights to objection to data processing;
- a.20) (AND) information on the data subject's rights to data portability;
- a.21) (AND) if processing is based on consent, the right to withdraw consent at any time;
- a.22) (AND) the right to lodge a complaint with the Supervisory Authority;
- a.23) (AND) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

G.3.2.2 Further processing [C, S, A]

A) The Applicant shall have rules, a procedure or a mechanism in place to inform data subject about any further processing, including on the purpose of the further processing and the rights of the data subjects.

AND

B) The Applicant shall keep records of:

- b.1) any extension of data processing with the reasons for such extension;
- b.2) (AND) the assessment of the lawfulness of the further processing;
- b.3) (AND) the communication with data subjects (with the dates).

G.3.2.3 Tolerated Exemption [C, S, A]

In order to derogate to the criteria G.3.2.1 and G.3.2.2, the Applicant shall demonstrate that the data subject already has been informed.

G.3.3 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 [Except if an exemption can be demonstrated in conformity with G.3.3.4], THEN:

G.3.3.1 Duty to inform [C, S, A]

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

- a.1) the identity of the Controller;
- a.2) (AND) the contact details of the Controller;
- a.3) (AND) the contact details of the data protection officer (or contact mechanism);
- a.4) (AND) the purposes of processing;
- a.5) (AND) the legal basis for the processing;
- a.6) (AND) if applicable, the legitimate interests pursued by the Controller or by a third-party;
- a.7) (AND) the categories of personal data concerned;
- a.8) (AND) the recipients or categories of recipients of the personal data;
- a.9) (AND) if personal data are likely to be transferred to any third country or to an international organisation, the list of non-European countries where the data are transferred;
- a.10) (AND) if personal data are likely to be transferred to any third country or to an international organisation, whether a valid adequacy decision applies to the data transfer;
- a.11) (AND) if personal data are likely to be transferred to any third country or to an international organisation, information on the safeguards measures adopted by the Controller to assess and minimize the risks for the data subjects and their rights when processed in third-countries;
- a.12) (AND) if automated decision-making and/or profiling is performed, meaningful information about the logic involved in the processing activities;
- a.13) (AND) if automated decision-making and/or profiling is performed, the significance of the processing activities;
- a.14) (AND) if automated decision-making and/or profiling is performed, the envisaged consequences of the processing activities;
- a.15) (AND) the retention period or the criteria for determining the retention period;
- a.16) (AND) information on the data subject's rights to access to personal data;
- a.17) (AND) information on the data subject's rights to rectification of personal data;
- a.18) (AND) information on the data subject's rights to erasure of personal data;
- a.19) (AND) information on the data subject's rights to restriction of data processing;
- a.20) (AND) information on the data subject's rights to objection to data processing;
- a.21) (AND) information on the data subject's rights to data portability;
- a.22) (AND) if processing is based on consent, the right to withdraw consent at any time;
- a.23) (AND) the right to lodge a complaint with the Supervisory Authority;
- a.24) (AND) the source from which personal data originate;
- a.25) (AND) if applicable, whether information were collected from publicly applicable sources.

G.3.3.2 Duty to inform in due time [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 collected;
- 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 30 days;
- c.2) (AND) if the personal data are to be used for communication with the data subject, at the time of the first communication to data subjects;
- c.3) (AND) if disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

G.3.3.3 Duty to inform on purpose extension [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 other purpose than the declared purpose for which the data were initially collected.

AND

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

G.3.3.4 Tolerated Exemption [C, S, E]

IF one of the following cases apply, THEN G.3.3.1 can be skipped:

IF one of the following cases apply, THEN G.3.3.1 can be skipped:

Case 1 - Already informed:

A) The Applicant shall demonstrate that the data subjects are already in possession of the information listed in G.3.3.1.

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 basis:

A) The Applicant shall demonstrate that it is bound by a specific legal obligation which expressly requires the obtention or disclosure of personal data.

OR

Case 4 - Secrecy:

A) The Applicant shall demonstrate that it is subject to an obligation of secrecy regulated by law, including a statutory obligation of secrecy.

G.3.4 Right of access by the data subject

G.3.4.1 Right of access by the data subject [C, S, A]

A) The Applicant shall have an effective mechanism or procedure in place enabling the data subjects to request and access the following information:

- a.1) the purposes of the processing;
- a.2) (AND) the categories of processed personal data;
- a.3) (AND) the recipients or categories of recipients;
- a.4) (AND) the retention period or the criteria for determining the retention period;
- a.5) (AND) information on the data subject's rights to access his/her data;
- a.6) (AND) information on the data subject's rights to rectification;
- a.7) (AND) information on the data subject's rights to erasure of personal data;
- a.8) (AND) information on the data subject's rights to restriction of processing;
- a.9) (AND) information on the data subject's rights to objection;
- a.10) (AND) information on the data subject's rights to data portability;
- a.11) (AND) the right to lodge a complaint with the Supervisory Authority;
- a.12) (AND) the source from which personal data originate and if applicable whether the personal data came from publicly applicable source;
- a.13) (AND) whether the Controller implemented automated decision-making and profiling;
- a.14) (AND) if the Controller implemented automated decision-making or profiling, meaningful information about the logic involved in the processing activities;
- a.15) (AND) if the Controller implemented automated decision-making or profiling, the significance of the processing activities;
- a.16) (AND) if the Controller implemented automated decision-making or profiling, the envisaged consequences of the processing activities;
- a.17) (AND) whether personal data are transferred to any third country or to an international organisation;
- a.18) (AND) if personal data are transferred to any third country or to an international organisation, the list of third countries where the data are transferred;
- a.19) (AND) if personal data are transferred to any third country or to an international organisation, whether a valid adequacy decision applies to the data transfer;
- a.20) (AND) if personal data are transferred to any third country or to an international organisation, information on the safeguards measures adopted by the Controller to assess and minimize the risks for the data subjects and their rights when processed in third-countries

G.3.4.2 Duty to provide a copy [C, S, A]

A) The personal data processed in the Target of Evaluation shall be extractable and transferable to the Data Subject who has made the request in a commonly used electronic format.

G.3.4.3 Duty to protect the rights of others [C, S, A]

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

G.3.5 Right to rectification

G.3.5.1 Right to rectification [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 implement the request.

G.3.6 Right to erasure ('right to be forgotten')

G.3.6.1 Right to erasure [C, S, A]

A) The Applicant shall have rules, a procedure, or a mechanism in place to effectively erase the personal data that are no longer necessary (in relation with the purpose for which they were collected or processed).

G.3.6.2 Duty to relay the request to other data Controllers [C, S, A]

IF the Applicant has made personal data of the Target of Evaluation publicly available to other controllers, 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.

G.3.6.3 Tolerated Exemption [C, S, E]

The right to erasure is subject to restrictions in the following cases:

Exercising the right of freedom of expression and information:

A) Evidence shall demonstrate that the retained data are used in the context of public information or expression.

OR

A) Evidence shall demonstrate that the Applicant is bound by the obligation to comply with such a legal obligation.

OR

A) Evidence shall demonstrate that there is a public interest in the area of public health.

OR

A) Evidence shall demonstrate that the data retention is related to:

- a.1) archiving purposes in the public interest;
- a.2) (OR) scientific purposes;
- a.3) (OR) historical research purposes;
- a.4) (OR) statistical purposes.

OR

A) Evidence shall demonstrate that the data retention is related to the establishment, exercise or defence of legal claims.

G.3.7 Right to restriction of processing**G.3.7.1 Right to restriction of processing [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;
- a.2) (AND) to ensure that personal data processing whose processing is restricted can only be processed:
 - with the data subject's consent;
 - for the establishment, exercise or defense of legal claims;
 - for protecting the rights of another natural or legal person;
 - for reasons of important public interest;
- 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.

G.3.8 Notification obligation regarding rectification or erasure of personal data or restriction of processing**G.3.8.1 Duty to inform recipients [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.

G.3.8.2 Duty to inform data subjects on recipients if requested [C, S, A]

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

G.3.9 Right to data portability

IF the personal data are collected by consent or through a contract with the data subjects, THEN:

G.3.9.1 Right to data portability [C, S, A]

A) The Applicant shall have a procedure or mechanism in place for data portability that:

- a.1) shall enable data subjects to obtain a copy of their provided personal data in electronic format;
- a.2) (AND) shall filter out personal data pertaining to other data subjects if this may adversely affect the rights and freedom of the latter;

AND

B) The data format used to transfer personal data to the data subject shall be:

- b.1) structured;
- b.2) (AND) commonly used;
- b.3) (AND) machine readable.

G.3.10 Right to object**G.3.10.1 Effectiveness of the right to object [C, S, A]**

A) The Applicant shall demonstrate the effectiveness of the procedure or mechanism in place to comply with the requests of data subjects to object to the processing of their personal data.

G.3.10.2 Clear information on the right to object [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.

G.3.11 Right not to be subject to automated individual decision-making, including profiling**G.3.11.1 Automated individual decision-making, including profiling [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 if the automated decision process complies with at least one of the following conditions:

- a.1) the necessity of the processing for entering into, or performing, a contract between the data subject and the data Controller is justified by a written analysis of the process that shall have considered alternatives to automated decision-making for reaching an equivalent result and shall conclude that the automated decision making is necessary;
- a.2) (OR) the processing shall be authorised by law to which the Controller is subject;
- a.3) (OR) the processing shall be based on the data subject's explicit consent.

G.3.11.2 Rights to obtain human intervention and to contest [C, S, A]

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

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

- a.1) to obtain human intervention on the part of the Controller;
- a.2) (AND) to express their points of view and to contest the decision.

G.4 Data Controller Responsibility

G.4.1 Responsibility of the Controller

IF the Applicant is a data Controller, THEN:

G.4.1.1 Documentation on technical and organization measures [C, S, A]

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

G.4.1.2 Duty to review and update [C, S, A]

A) The Applicant shall have a procedure in place to review on a regular basis (at least yearly) the adequacy of the technical and organizational measures in place.

AND

B) The Applicant shall keep documented records of:

- b.1) the review of the technical and organizational measures;
- b.2) the identified vulnerabilities and actions taken to address these vulnerabilities.

G.4.1.3 Data Protection Policies [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 Supervisory Authority;
- a.6) (AND) policy regarding data protection by design and by default, such as data minimization and data pseudonymization;
- a.7) (AND) management of data transfer to third parties and to third countries.

G.5 Data Processors (or sub Processors)

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

G.5.1 Processor

G.5.1.1 Restriction on use of Processors [CP, S, A]

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

- a.1) request and record information from its Data Processors about their technical and organizational measures to protect personal data and/or GDPR-related certification;
- a.2) (AND) assess the appropriateness of the technical and organizational measures reported by the Processor for protecting personal data;
- a.3) (AND) document 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 on its Technical and Organization Measures;
- b.2) (AND) the evaluation and decision process to accept the data 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 its contractual clauses and guarantees provided by its processors that demonstrate the adequacy of its technical and organizational measures.

G.5.1.2 Contractual necessity for Controllers [C, S, A]

A) The Applicant shall have written contractual relationships with each and every Data Processor in charge of processing 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.

G.5.1.3 Contractual necessity for Processors [P, S, A]

IF the Applicant acts as Processor, THEN:

A) The Applicant shall have written contractual relationships 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 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.

G.5.1.4 Contractual obligations of data Processors [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 required by law;
- a.9) (AND) make available to the Controller all information necessary to demonstrate compliance with the 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.

G.5.1.5 Complementary demonstration of Processors' compliance [CP, S, A]

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

G.5.2 Processing under the authority of the Controller of Processor**G.5.2.1 Process on instruction only** [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.

G.5.3 Records of processing activities**G.5.3.1 Record of data processing by Controller** [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, 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;
- 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 to which data are transferred;
- b.3) (AND) documentation of safeguards set in place to mitigate the risk of such transfer (See G.10.5.2).

G.5.3.2 Record of data processing by Processor [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 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;
- 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.

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 to which data are transferred;
- b.3) (AND) documentation of safeguards set in place to mitigate the risk of such transfer (See G.10.5.2).

G.5.3.3 Data Processing instructions records [CP, S, A]

A) There shall be a registry and/or documentation of instructions communicated by the Controller to the Processors (or where applicable by the Processor to the Sub processors).

G.5.3.4 Completeness of the Registry [CP, S, A]

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

G.6 Security of Processing and Data Protection by Design

G.6.1 Data protection by design and by default

G.6.1.1 Data protection by design and by default [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 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.

AND

C) the DPO or an expert with adequate expertise shall confirm that:

- c.1) the analysis and recommendations are adequate;
- c.2) (AND) he/she did not identify less privacy intrusive solution in terms of personal data collection for achieving the same results and delivering the same services;
- c.3) (AND) the applicable recommendations have been implemented.

G.6.1.2 Data minimization by default [C, S, A]

A) The Applicant shall have implemented technical measures to:

- a.1) restrict access to personal data on the basis of a registry of authorized personnel;
- a.2) (AND) have used a risk analysis to implement technical and organizational measures for mitigating the identified risks;
- a.3) (AND) delete personal data at the end of the retention period.

G.6.2 Security of processing

G.6.2.1 Security Policy [CP, G, A]

A) The Applicant shall have written security rules and/or policies to protect and secure the data processing, that covers at least:

- a.1) the data confidentiality policy;
- a.2) (AND) the data minimization policy;
- a.3) (AND) the data access policy;
- a.4) (AND) the data processing restrictions (on instruction);
- a.5) (AND) the data storage and retention period policy;
- a.6) (AND) the data continuity and backup policy;
- a.7) (AND) the data breach policy;
- a.8) (AND) the restrictions on copying data and "bringing your own device".

G.6.2.2 Process on instruction only [CP, G, A]

A) The Applicant shall have 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 instructed by the Controller (unless he or she is required to do so by law).

G.6.2.3 Contractual obligation to confidentiality [CP, G, A]

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

G.6.2.4 Risk assessment for the data processing [CP, S, A]

A) The Applicant shall have assessed with a repeatable methodology the risks on the data processing that may impact the rights and freedoms of the natural persons by considering at least the risks of:

- a.1) accidental or unlawful destruction or loss of personal data;
- a.2) (AND) accidental or unlawful alteration of personal data;
- a.3) (AND) accidental, unlawful or unauthorised disclosure and access of personal data;
- a.4) (AND) intrusion attacks;
- a.5) (AND) the risk attached to high-privilege profiles access.

AND

B) The identified risks of the risk analysis shall be complemented by recommendations and/or a risk mitigation plan to mitigate the identified risks.

AND

C) Where applicable, the risk assessment shall be updated taking into account the recommendations and/or risk mitigation plan.

AND

D) Where the risk assessment concludes that an action plan is a condition to mitigate the risk to an acceptable level, then the mitigation measures issued from the risk assessment shall be implemented.

G.6.2.5 Access rights policy and registry [CP, S, A]

A) The Applicant shall have established an access control policy that is defined around roles and responsibilities.

AND

B) The Applicant shall keep an updated registry of access rights of its employees and agents who can access the personal data.

AND

C) The Applicant shall have procedure, policy or mechanism in place to regularly review the registry of access rights.

AND

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

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

G.6.2.6 Access and transfer logs [CP, S, A]

A) The Applicant shall have a monitoring system, a mechanism or a process in place to record and keep a log of:

- a.1) access to personal data by employees and agents of the Applicant;
- a.2) (AND) transfer of personal data to third parties, including processors and cross-border transfers.

G.6.2.7 Continuity, Integrity and availability [CP, S, A]

A) The Applicant shall have policies, procedures, or plans in place to ensure the continuity of the processing and associated services in case of physical or technical incidents, including:

- a.1) for ensuring the ongoing confidentiality and integrity of the personal data;
- a.2) (AND) for ensuring availability and resilience of the access of the data subjects to their personal data.

G.6.2.8 Communication encryption [CP, S, A]

A) Where communications of personal data across public networks can be encrypted, they shall be encrypted.

G.6.2.9 Duty to backup [CP, S, A]

A) The personal data stored by the Applicant shall be backed up.

G.6.2.10 Complementary Contextual Requirements [CP, S, A]

A) The data processing activities of the Target of Evaluation shall comply with the applicable Complementary Contextual Checks and Controls specified by Europrivacy.

G.6.2.11 Complementary Technical and Organization Measures [CP, S, A]

A) The Applicant shall have:

- a.1) assessed the adequacy 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.

AND

B) The assessment of the TOM shall have been validated by the DPO as being sufficient and adequate to protect the rights and freedoms of the data subjects.

G.7 Management of Data Breaches

G.7.1 Notification of a personal data breach to the Supervisory Authority

G.7.1.1 Duty to document data breaches [CP, G A]

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

- a.1) the facts relating to the personal data breach;
- a.2) (AND) the effects of the data breach;
- a.3) (AND) the remedial action taken.

G.7.1.2 Duty of the Controller to notify and communicate data breaches [C, G, A]

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

- a.1) record data breaches and follow-up actions 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 minimize the risks, its likelihood, and potential impact on data subjects;
- a.4) (AND) if the risk is likely to result in a risk to the rights and freedoms of natural persons, inform the Supervisory Authority without undue delay and no more than 72 hours after having been aware of it;
- a.5) (AND) if the risk is likely to result in a risk to the rights and freedoms of natural persons, inform the data subject without undue delay (except where not required by the regulation).

G.7.1.3 Duty of the Processor to communicate data breaches with undue delay [P, G, A]

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

- a.1) record data breaches and follow-up actions 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.

G.7.1.4 Notification requirements [C, G, A]

A) The procedure for breach notification to the Supervisory 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.

G.7.2 Communication of a personal data breach to the data subject**G.7.2.1 Breach communication requirements [C, G, A]**

A) The procedure or mechanism for communicating a data breach to the data subjects shall include at least the following information:

- 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 appropriate the measures to mitigate its possible adverse effects.

G.7.2.2 Tolerated Exemption [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

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

G.8 Data Protection Impact Assessment (DPIA)**G.8.1 Duty to assess if Data Protection Impact Assessment (DPIA) is required**

G.8.1.1 Data Protection Impact Assessment (DPIA) [C, S, A]

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

- a.1) the data processing entails inherent high risk for the rights and freedoms of the data subject;
- a.2) (OR) a systematic evaluation of personal aspects of natural persons based on automated processing (such as profiling) 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) the processing operations falls in the list of data processing activities requiring a DPIA that is published by the Supervisory Authority of the Applicant;
- a.5) (OR) processing operations listed as requiring DPIA according to the Supervisory Authority or to the applicable legislation.

AND

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

- 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.

G.8.1.2 Tolerated Exemption [C, S, E]

DPIA is not required (except if required by Member State) if:

A) Processing has a legal basis in Union or Member State law and the Controller is subject to such law AND an impact assessment has already been carried out on similar data processing that are:

- a.1) involving similar Data subjects;
- a.2) (AND) for similar purpose.

OR

B) The Target of Evaluation is covered by the list or data processing activities that are exempted of DPIA by the national supervisory authority.

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

IF a DPIA is applicable, THEN:

G.8.2.1 DPIA Process requirements [C, S, A]

A) The DPIA process shall have:

- a.1) involved the DPO in the DPIA process;
- a.2) (AND) where applicable, involved data subjects or their representatives in the impact assessment;
- a.3) (AND) where applicable, taken into account the adoption of code of conducts, certifications, and other binding and enforceable commitment, via contractual or other legal binding instruments;
- a.4) (AND) where applicable, adopted a plan for corrective actions;
- a.5) (AND) where applicable, taken actions to address and reduce the risk identified by the DPIA to a level assessed by the DPO as acceptable for the data subjects;
- a.6) (AND) consulted the Supervisory Authority if the DPIA concluded that the processing would result in high risks for the data subjects.

G.8.2.2 DPIA content requirements [C, S, A]

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

- a.1) the systematic description of the envisaged processing operations;
- a.2) (AND) the purposes for processing personal data;
- a.3) (AND) where applicable, the legitimate interest of the Controller;
- a.4) (AND) an assessment of the necessity and proportionality of the processing operation 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;

a.7) (AND) where applicable, the recommendation to consult the Supervisory Authority.

G.8.2.3 Data subjects involvement requirement [C, S, A]

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

G.8.2.4 DPIA review in case of change of risks [C, S, 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.

G.8.2.5 Duty to consult the Supervisory Authority in case of identified high risk [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 Supervisory Authority on the identified risks;
- a.2) (AND) received the opinion of the Supervisory Authority;
- a.3) (AND) where applicable, implemented the recommended actions mentioned in the opinion.

G.9 Data Protection Officer (DPO)

G.9.1 Designation of the data protection officer

G.9.1.1 Designation of the data protection officer [CP, G, A]

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

G.9.1.2 DPO requirements [CP, G, A]

A) The data protection officer of the Applicant shall have an education in law or a certified training in data protection regulations.

G.9.1.3 DPO contact details communication [CP, G, A]

A) Records shall demonstrate that the contact details and/or mechanism to communicate with the DPO:

- a.1) are published and available to the data subjects;
- a.2) (AND) have been communicated to the Supervisory Authority.

G.9.2 Position of the data protection officers

G.9.2.1 DPO mandate communication [CP, G, A]

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

- a.1) request employees to inform and involve the DPO in a timely manner in all data protection issues;
- a.2) give authority and effective access to the DPO for controlling personal data processing operations.

G.9.2.2 DPO support [CP, G, A]

A) The Applicant shall have allocated resources to support continuous training and capacity building of the DPO.

G.9.2.3 DPO independence [CP, G, A]

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

- a.1) to protect the autonomy and independence of decision of the DPO;
- a.2) (AND) to protect the DPO against any form of undue pressure related to the performance of his task;
- a.3) (AND) to enable the DPO to directly report to the highest management level of the Applicant.

G.9.2.4 Data subjects access to the DPO [CP, G, A]

A) The data subjects shall be able to contact the DPO from the website of the Applicant.

G.9.2.5 DPO contractual clauses [CP, G, A]

A) The contract with the DPO shall include clauses:

- a.1) to bind the DPO to secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law;
- a.2) (AND) to authorise the DPO to collaborate and communicate with the Supervisory Authority;
- a.3) (AND) to commit the DPO to avoid and report any conflict of interest.

G.9.2.6 Adequacy of DPO work time [CP, G, A]

A) The Applicant shall have assessed:

- a.1) the required work time for the DPO considering the types of data processing and the risks for the rights and freedom of data subjects;
- a.2) (AND) that the DPO has sufficient resources to perform its tasks.

G.9.3 Tasks of the data protection officer

G.9.3.1 DPO tasks and duties [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 and policies;
- a.3) (AND) to provide advice on the performance of the data protection impact assessment and monitor its performance (in accordance with Art. 35 GDPR);
- a.4) (AND) to cooperate and act as the contact point with the Supervisory Authority;
- a.5) (AND) to handle or overview the requests of the data subjects when exercising their rights.

G.9.3.2 Duty to train personnel on data protection [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.

G.10 Transfers of personal data to third countries or international organisations (if applicable)

IF any data processed in the Target of Evaluation is transferred (or made accessible) to any third country or to an international organization, THEN:

G.10.1 General principles for transfers

G.10.1.1 Cross border transfer to third countries validation [CP, S, A]

A) The Applicant shall have a clear mapping or record of all personal data transfers to third countries and international organizations by the Target of Evaluation.

AND

B) The transfer of personal data shall have been assessed as lawful by the DPO or by a legal expert with adequate expertise by taking into account:

- b.1) the risks for the freedoms and rights of the data subjects;
- b.2) (AND) the safeguards and measures set in place to protect the transferred data.

G.10.1.2 Cross-border transfer legal basis [CP, S, A]

IF personal data are transferred to third countries, THEN it shall comply with at least one of the following options:

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

OR

B) The transfer to a third country shall be based on appropriate safeguards and comply with the complementary criterion G.10.1.3.

OR

C) The data are transferred on the basis of binding corporate rules (BCR) that have been approved by the Supervisory Authority of the Applicant.

OR

D) The data transfer shall be based on derogations for specific situations and comply with the complementary criterion G.10.1.4.

G.10.1.3 Cross-border transfer based on appropriate safeguards [CP, S, A]

IF personal data transfers to third countries or to international organizations are based on appropriate safeguards, THEN:

A) The Controller or Processor in the third country shall:

- a.1) regularly audit the security of its infrastructure that processes and/or stores the data of the Target of Evaluation;
- a.2) (AND) the last audit report shall have been reviewed by the DPO of the Applicant and assessed as satisfactory.

AND

B) The Controller or Processor in the third country shall have a procedure in place to 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

C) 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

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

G.10.1.4 Cross-border transfer based on derogations for specific situations [CP, S, A]

IF personal data are transferred to third countries or to international organizations on derogations for specific situations, THEN:

A) The transfer shall be based on consent where:

- a.1) the data subjects shall have given an explicit and valid consent to the proposed transfer;
- 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.

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;
- b.2) (OR) important reasons of public interest, based on a legal basis recognized in the jurisdiction of the data controller;
- 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 Union or 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.

G.10.1.5 Complementary risk assessment of data transfer to third countries without adequacy decision [CP, S, A]

IF any personal data processed in the Target of Evaluation is transferred to any third country or to international organizations without adequacy decision, THEN:

A) The Applicant shall have collected information on the third country data protection regulation and practice (and/or on the international organization) in order to assess if:

- a.1) the assess and processing by the 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 organization) has established oversight mechanism;
- a.4) (AND) there are effective remedies made available to the individuals;
- a.5) (AND) the data protected regulation is effectively implemented.

AND

B) The Applicant shall have:

- b.1) adopted measures to address the identified risks and to bring the level of protection of the personal data transferred up to the required level essential data protection equivalence;
- b.2) (AND) set in place an effective procedure or measures to re-assess the risks related to the transfer of personal data to third countries and to international organizations (as applicable) on a regular basis.

G.10.1.6 Commitment of the data receiver [CP, S, A]

IF any personal data processed in the Target of Evaluation is transferred to any third country or international organization without adequacy decision, THEN:

A) The recipient of the personal data shall have made binding and enforceable commitments to apply appropriate safeguards to protect the processed data with regards to the rights of the data subjects.

G.10.2 Transfers subject to appropriate safeguards

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

G.10.2.1 Complementary requirements for appropriate safeguards [CP, S, A]

The Applicant shall demonstrate that the data transfer benefits from appropriate safeguard through at least one of the following mechanisms:

A) The data transfer has adequate safeguards thanks to a legally binding and enforceable instrument between public authorities or bodies.

OR

B) The data transfer has adequate safeguards thanks to binding corporate rules that have been approved by the Supervisory Authority.

OR

C) The data transfer has adequate safeguards thanks to standard data protection clauses signed together by the data importer and exporter.

OR

D) The data transfer has adequate safeguards thanks to an approved code of conduct with binding and enforceable commitment to apply appropriate safeguard.

OR

E) The data transfer has adequate safeguards thanks to a certification mechanism, where:

- e.1) the certification mechanism is approved by the data protection authority;
- e.2) (AND) the Controller or Processor in the third country is bound by and enforceable commitment to apply the appropriate safeguards to the data processing, including as regards data subjects' rights.

OR

F) The data transfer is authorized by the Supervisory Authority on the basis of approved contractual clauses with the Controller or Processor.

OR

G) The data transfer is authorized by the Supervisory Authority on the basis of an administrative arrangements between public authorities or bodies which shall include:

- g.1) the provisions approved by the Supervisory Authorities;
- g.2) (AND) provisions to ensure enforceable and effective data subject rights.