GDPR-CERTIFIED ASSURANCE REPORT-BASED PROCESSING ACTIVITIES CERTIFICATION CRITERIA

Version for public consultation – Focus on the certification criteria – Extract from the full certification scheme

Commission Nationale pour la Protection des Données

The Commission Nationale Pour la Protection des Données ('CNPD') prepared this document in its quality as scheme owner of the GDPR-CARPA certification scheme.

This document is an extract of the full GDPR-CARPA certification scheme that contains information relating to the GDPR-CARPA certification criteria and the certification criteria themselves. The CNPD shares this document as part of a public consultation on the certification criteria.

These certification criteria are a mandatory requirement to evaluate and report on controls over organisational and technical data protection measures, to be eligible for certification. Evaluation and reporting needs to follow the ISAE 3000 standard. Certification will only be able to be granted by certification bodies that have been accredited by the CNPD.

About CNPD:

The National Commission for Data Protection (Commission Nationale pour la Protection des Données – CNPD) is an independent authority created by the Act of 2 August 2002 on the *protection of individuals with regard to the processing of personal data*. It verifies the lawfulness of the processing of personal data and ensures the respect of personal freedoms and fundamental rights with regard to data protection and privacy. Its mission also extends to ensuring the respect of the amended Act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications. Under Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework, the CNPD is the independent public authority responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

About ISAE 3000:

This International Standard on Assurance Engagements (ISAE) deals with assurance engagements other than audits or reviews of historical financial information. Assurance engagements include direct engagements, in which the practitioner measures or evaluates the underlying subject matter against a set of criteria. International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements other than Audits or Reviews of Historical Financial Information, should be read in conjunction with the Preface to the International Standards on Quality Control (ISQC), Auditing, Review, Other Assurance and Related Services Pronouncements.

About ISQC 1:

This International Standard on Quality Control (ISQC) 1 deals with a firm's responsibilities for its system of quality control for audits and reviews of financial statements, and other assurance and related services engagements. This standard is to be read in conjunction with relevant ethical requirements.

Versioning:

This document is a draft version of an extract of the GDPR-Carpa certification scheme (adoption planned to occur in mid-2021). It is aimed to be used only in the context of a public consultation.

CONTENTS

1 INTRODUCTION

1.1 CONTEXT

The European Union General Data Protection Regulation (Regulation 2016/279) ('the GDPR'), which came into full effect on 25 May 2018, provides a modernised, accountable and fundamental rights compliance framework for data protection in Europe. A range of principles that facilitate compliance with the provisions of the GDPR are central to this new framework. These include mandatory requirements in specific circumstances (including the appointment of Data Protection Officers and carrying out data protection impact assessments) and voluntary measures such as codes of conduct and certification mechanisms.

Article 42.1 of the GDPR states that: "The Member States, the supervisory authorities, the [European Data Protection] Board and the European Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account".

Certifications are a virtuous business practice that can greatly improve transparency and accountability for data subjects, but also in business-to-business relations, for example between controllers and processors which are often seen as customers and providers. Recital 100 of the GDPR states that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation and allow data subjects to assess the level of data protection of relevant products and services.

Certification under GDPR is a voluntary process to assist controllers and/or processors in supporting their demonstration of compliance to the GDPR to other businesses, to a supervisory authority or the data subjects, meaning that they demonstrated the existence and implementation of appropriate measures as required by the GDPR. Article 42.4 of GDPR clarifies that certification "does not reduce the responsibility of the controller or the processor for compliance" and therefore "is without prejudice to the tasks and powers of the supervisory authorities which are competent". It is however contributing to enhance trust between data protection authorities and other entities where certification bodies play a major role.

2 GENERAL CONSIDERATIONS

2.1 SCOPE OF THE GDPR-CARPA CERTIFICATION

The GDPR-CARPA certification is designed to provide data controllers and processors with a high level of reasonable assurance that they have setup, implemented and that they are operating technical and organisational measures to comply with their GDPR obligations for the processing activities in scope of the certification. It constitutes an element that allows controllers and processors to demonstrate compliance of those certified processing operations with the GDPR.

The purpose of GDPR-CARPA is to support controllers and processors in their obligation to implement appropriate technical measures and organisational measures to ensure and to be able to demonstrate that the processing in scope is performed in accordance with their responsibility obligation under the GDPR.

Non sector-specific criteria

The GDPR-CARPA certification criteria are designed to be sufficiently flexible to be relevant to a large panel of processing operations in multiple sectors. Each entity can define and implement the measures that best suit its specific situation and sector to comply with the criteria. The CNPD might issue additional sector specific elements in form of “focus points” or “guidance” for certification bodies.

Scope limitation of the certification scheme

- While information security elements have been integrated in the scheme, they do not constitute the focus of this certification mechanism. GDPR-CARPA does not certify the security of the processing in scope but rather focuses on the responsibility of controllers / processors who need to implement a governance system allowing them to define and implement measures to manage information security for the processing activity in scope. In order to have an assurance on implemented information security measures other appropriate information security certifications and frameworks should be considered.
- Only controllers and processors established in Luxembourg, under the supervision of the CNPD can apply for a GDPR-CARPA certification.

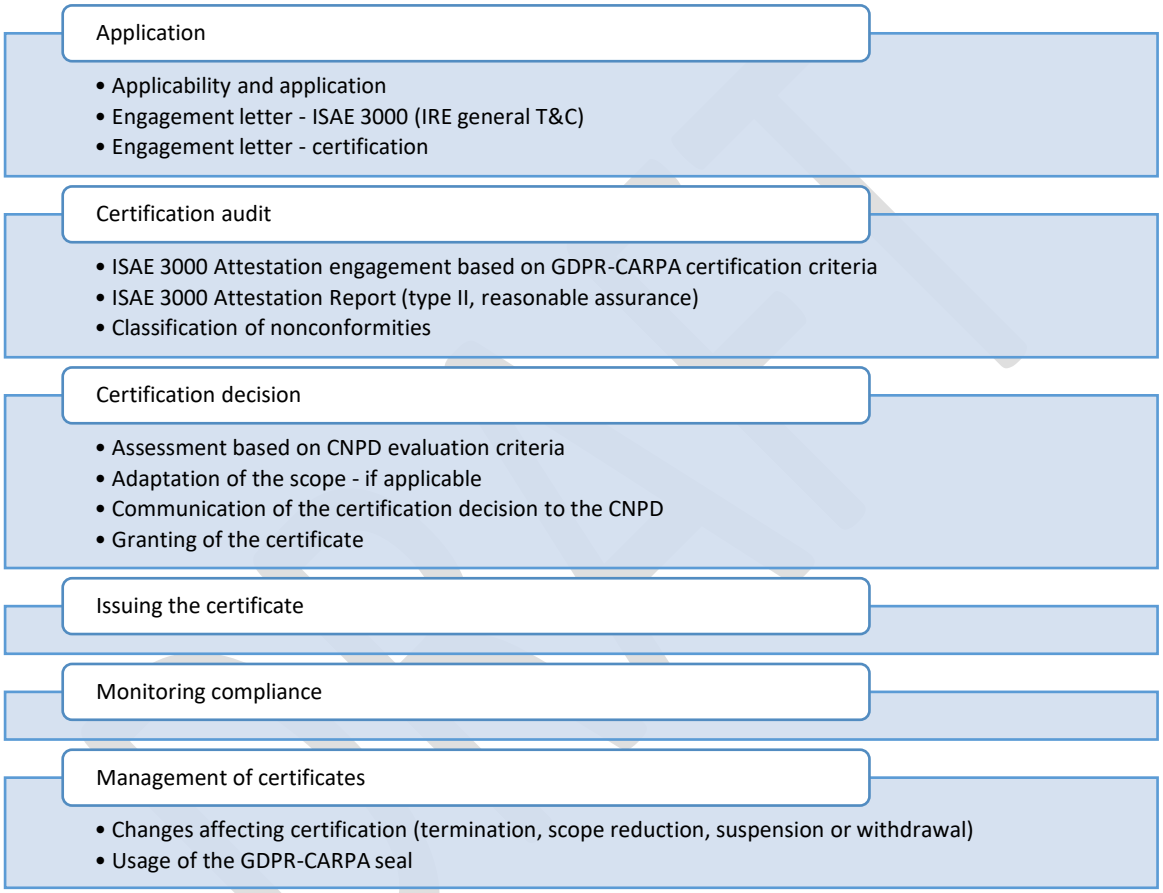
Exclusion from the scope of the certification

GDPR-CARPA is not suitable:

- for certifying personal data processing specifically targeting minors under 16 years old;
- for the certifications of processing activities in the context of a joint controllership;
- for processing activities in the context of article 10 GDPR.

3 CERTIFICATION PROCEDURE

The following diagram illustrates the different steps of the certification process:



The certification procedure is guided by ISO/IEC 17065:2012[1] requirements which have been combined with the ISAE 3000 and other relevant standards[2] in order to form the GDPR-CARPA accreditation requirements (for procedural requirements for accredited certification bodies in the context of certification activities, please refer to the CNPD's documentation regarding the GDPR-CARPA accreditation procedure).

[1] ISO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, processes and services

[2] Other relevant standards:

- International Standards on Quality Control 1 (ISQC1) – Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements, defined by the International Auditing and Assurance Standards Board (IAASB);
- Handbook of the International Code of Ethics for Professional Accountants, defined by the International Ethics Standards Board for Accountants (IESBA), especially parts 1 and 4B;
- International Standard on Assurance Engagements – Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000), defined by the IAASB.

The ISAE 3000 assurance report is an important element of the certification process. It follows that all relevant standards, codes of conducts and other regulatory texts need to be respected by the certification body performing the assurance engagement.

According to the attestation standards, the criteria used in an attestation engagement shall be suitable and available to report users. Attributes of suitable criteria are as follows:

- Relevance: Relevant criteria result in subject matter information that assists decision-making by the intended users.
- Completeness: Criteria are complete when subject matter information prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter information. Complete criteria include, where relevant, benchmarks for presentation and disclosure.
- Reliability: Reliable criteria allow reasonably consistent measurement or evaluation of the underlying subject matter including, where relevant, presentation and disclosure, when used in similar circumstances by different practitioners.
- Neutrality: Neutral criteria result in subject matter information that is free from bias as appropriate in the engagement circumstances.
- Understandability: Understandable criteria result in subject matter information that can be understood by the intended users.

In addition to being suitable, ISAE 3000 standard indicates that the criteria used in an attestation engagement must be available to intended users. The publication of the GDPR-CARPA certification criteria by the CNPD makes the criteria publicly available.

4 CERTIFICATION CRITERIA

4.1 ORGANISATION OF THE CRITERIA

The GDPR sets the ground for the development of certification criteria. While Articles 42 and 43 address fundamental requirements for certification procedures, the basis for certification criteria must be derived from the principles and rules set out by the GDPR in such a manner as to provide assurance that those principles and rules are complied with.

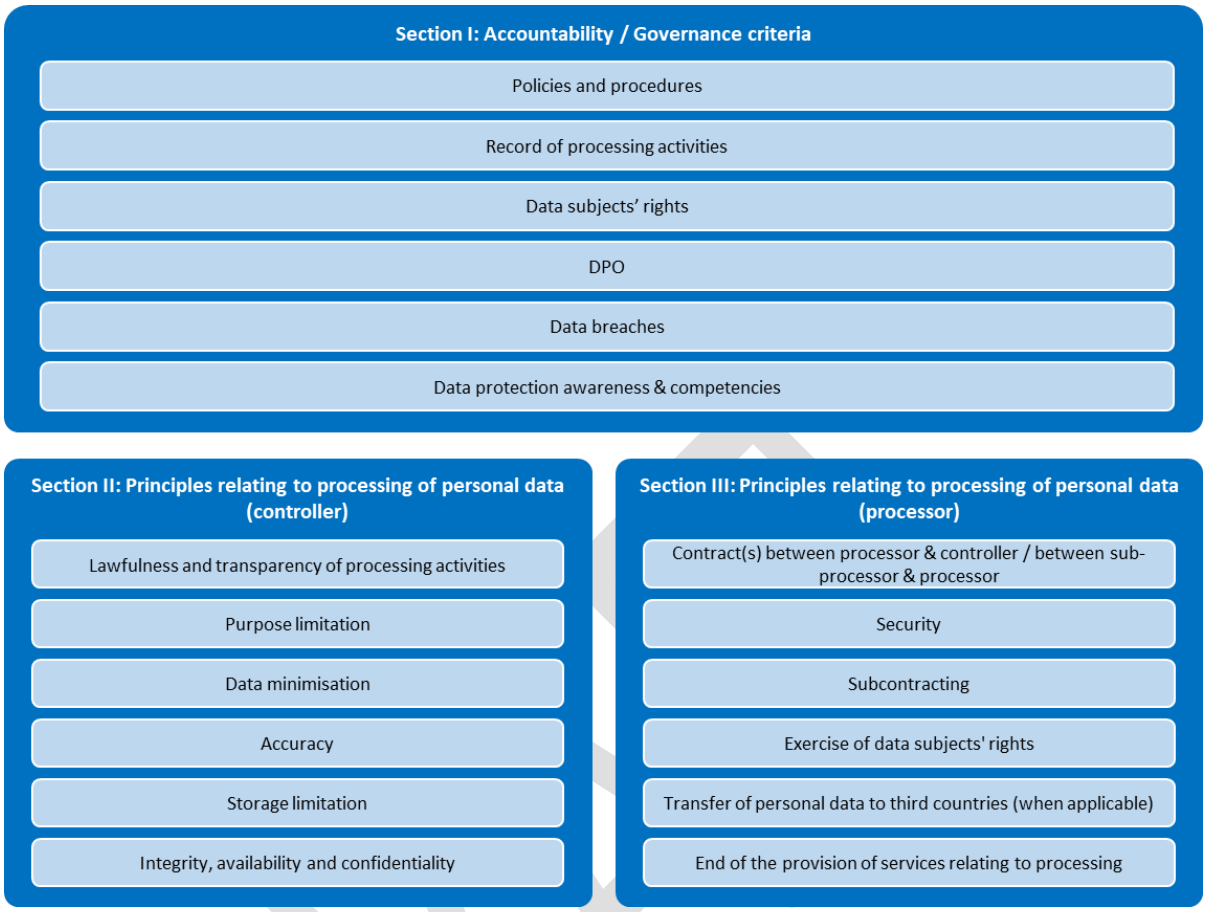
The criteria of a certification mechanism shall be applicable to the individual certification engagements. They should be able to cover all relevant aspects of data processing.

Depending on the area (e.g. health sector) and scope of certification (multiple or single processing operations) certification criteria shall always address, inter alia, the following compliance aspects in support of the assessment of the processing operation:

- the lawfulness of data processing pursuant to Article 6,
- the principles of data processing pursuant to Article 5,
- the data subjects' rights pursuant to Articles 12-23,
- the obligation to notify data breaches pursuant to article 33,
- data protection by design and by default, pursuant to article 25,
- whether a data protection impact assessment, pursuant to article 35.7(d) has been conducted, if applicable,
- technical and organisational measures put in place pursuant to Articles 32.

Taking the above into account, the GDPR-CARPA certification criteria for controllers have been aligned to the "Principles relating to processing of personal data" as defined under article 5 of GDPR, and complemented by the other requirements as set out above.

The criteria are organised in three sections:



Section I: Accountability Criteria

This section contains the criteria relevant to how an entity manages personal data protection concerns from a governance point of view to ensure its management can assume accountability. Criteria within this section contain a flag that indicates if they apply to entities that request certification as data controller or as data processor – if entities act as controller or as processor for at least one processing activity within the scope of the certification, they need to comply with all of the criteria set out in this section.

Section II: Principles Relating to Processing of Personal Data (Controller)

This section contains the criteria relevant to how an entity manages personal data protection requirements for a given processing activity in scope, where it acts as controller. This section is composed of sub-sections, which respectively relate to the principles of processing of personal data as defined under GDPR, and complemented by additional relevant elements, namely:

- Subsection II-a: Lawfulness and transparency of processing activities
- Subsection II-b: Purpose limitation
- Subsection II-c: Data minimisation
- Subsection II-d: Accuracy
- Subsection II-e: Storage limitation
- Subsection II-f: Integrity, availability and confidentiality

Section III: Principles Relating to Processing of Personal Data (Processor)

This section contains the criteria relevant to how an entity manages personal data protection requirements for a given data processing activity in scope, where it acts as data processor.

4.2 APPLICATION OF CRITERIA

The GDPR-CARPA certification can only be issued if all the criteria are addressed by the certification engagement. In addition to the criteria in section I, which apply to all, data controllers need to meet all criteria set out in section II, and data processors need to meet all criteria set out in section III.

The certification body must report on all GDPR-CARPA certification criteria. However, in limited circumstances and depending on the context and the target of evaluation, one or more criteria of sections II and III may not be applicable to the processing activity of the entity. In those cases, the certification body does not evaluate the relevant criterion during the engagement. It shall be noted that every (partial) exclusion of a criterion and the reasons for doing so must be documented in detail in the assurance report with the reasoning for doing so.

However, the common criteria of section I must be applied regardless of which processing activities are included within the target of evaluation of the engagement. This means that all governance criteria need to be addressed during the certification engagement.

4.3 TARGET OF EVALUATION

The GDPR provides a broad scope for what can be certified (also known as "the object of certification" or "Target of Evaluation" (ToE)), as long as the focus is to "demonstrat[e] compliance with GDPR of processing operations by controllers and processors" (Article 42.1).

The "object of certification" under the GDPR-CARPA certification mechanism is a processing or a set of "processing activities" as defined by the GDPR. It is up to the entity to be certified to propose the processing activities it wants to include in the certification scope – this approach adds flexibility to the mechanism. Entities can start with a limited scope and extend it over the years; they can focus on key processing activities – or those that are most relevant in regards to demonstrating compliance. An entity can select processing activities for which it acts as controller or as a processor.

As the certification decision relies upon the ISAE 3000 assurance report, it is clear that the scope of this report must cover at least all processing activities that are in scope of the certification as well as all relevant governance-related criteria (see section I below).

The concept of processing is defined in Article 4.2 of the GDPR. It shall cover all the relevant components of a processing in such a way as to make them available for assessment for the purpose of certification, which is to demonstrate compliance with the GDPR. In order to fully understand processing operations, it has proven useful to distinguish at least five different levels of significant influencing factors or components for the evaluation of processing operations.

- The first level comprises the organisation of the controller or processor, e.g. a private or public organisation and its specific legal ecosystem.
- The second level addresses the organisational circumstances and the purpose(s) for which the processing operation is performed, e.g. the department and the people in charge of the operation.
- On a third level, the functional application is assessed that is used to implement the purpose.
- The fourth level, considers the entire IT respectively IT infrastructure, any filing systems and the functions provided. This level includes operating systems, virtual systems, databases, authentication

and authorisation systems, routers and firewalls, storage systems such as SAN or NAS, an organisation's communication infrastructure or Internet access, as well as the technical measures which must be implemented.

- The fifth level addresses the detailed processed of the processing activities.

The following table is an illustrative example of how the target of evaluation for a given entity can be defined:

Processing activity (as per the register)	Role	Level 1 Organisation	Level 2 Circumstances / purpose	Level 3 Functional application	Level 4 IT infrastructure / filing system	Level 5 Processes
Recruitment	Controller	Financial institution	HR department	SAP-HR	Windows server farm, Oracle DB	Application process & management Job offer process Administrative hiring process
Newsletter	Controller	Financial institution	Marketing	CRM	Cloud solution-SAAS	Send weekly newsletter Handle newsletter Subscription / unsubscription

5 GDPR-CARPA CERTIFICATION CRITERIA

The following certification criteria contain the rules to be followed by the entities applying for the CARPA-certification. Those entities need to ensure that their internal measures be designed, implemented and operated to allow them to reach the requirements set out in these certification criteria. When performing their certification audit, certification bodies will check whether the design, implementation and operation of these measures comply with the requirements defined by the certification criteria.

The certification body structures its evaluation tasks as follows:

- Design and implementation: The auditor will look at the documented design / description of a measure (for example in the form of a procedure) and verify if it will work in theory as required by the certification criteria: The auditor will try to determine if it is designed to comply with the certification criteria.
- Operating effectiveness: After having reviewed the design and implementation of a measure, the auditor will test the operating effectiveness of this measure: He / she will check if the control or measure works in practice as it should and as documented, through observation, walkthrough, sampling, interviews, interaction, e.g. with an interface, etc.

If a criterion is not applicable to a specific context at the entity, the certification body will document this accordingly indicating the reasons why it is not applicable.

Furthermore, the official guidelines published by the EDPB[3] can serve as support in order to better understand GDPR requirements and provide guidance with regard to the implementation of those GDPR requirements.

When the terms “formal” and / or “formally” are mentioned in a criteria, a documentation is required.

[3] https://edpb.europa.eu/

Overview of Section I: Accountability criteria / Governance criteria						
Subject	Criteria for controllers			Criteria for processors		
	Ref.	Page	Title	Ref.	Page	Title
Policies and procedures	I-1	18	Accountability	I-1	18	Accountability
	I-2	18	Policies and procedures	I-2	18	Policies and procedures
	I-3	19	Review and update of policies and procedures	I-3	19	Review and update of policies and procedures
Record of processing activities	I-4	19	Record of processing activities	I-5	20	Record of processing activities
	I-6	20	Management of the record of processing activities	I-7	21	Management of the record of processing activities
Data Subjects' Rights	I-8	21	Facilitate the exercise of data subjects' rights	I-9	22	Facilitate the exercise of data subjects' rights
DPO	I-10	23	Designation	I-10	23	Designation
	I-11	23	Competencies	I-11	23	Competencies
	I-12	24	Position	I-12	24	Position
	I-13	25	Tasks	I-13	25	Tasks
Data breaches	I-14	26	Data breaches	I-15	27	Notification of data breaches towards the controller
Data Protection Awareness & Competencies	I-16	28	Awareness trainings & competencies of staff	I-17	28	Awareness trainings & competencies of staff

	Transfer of personal data to third countries (when applicable)	II-a-18	43	Third country transfers
Subsection II – b: Purpose limitation		II-b-1	45	Quality of purpose definition
		II-b-2	45	Purpose compatibility
Subsection II – c: Data minimisation		II-c-1	47	Process to ensure data minimisation
		II-c-2	47	Alternative means
Subsection II – d: Accuracy		II-d-1	48	Reliability of the data source
		II-d-2	48	Accuracy of data
		II-d-3	48	Right to rectification
Subsection II – e: Storage limitation		II-e-1	50	Defined retention period
		II-e-2	50	Deletion or anonymization of data
		II-e-3	51	Right to erasure ('right to be forgotten')
Subsection II – f: Integrity, availability and confidentiality	Security	II-f-1	53	Inventory and data flow diagram
		II-f-2	53	Risk analysis
		II-f-3	54	Risk treatment
		II-f-4	54	Documented implementation of organisational and technical measures
		II-f-5	54	Audit
		II-f-6	55	Follow-up on audits
	Data protection impact assessment (DPIA)	II-f-7	55	DPIA

		II-f-8	56	DPIA - Prior consultation
	Outsourcing	II-f-9	56	Assessment of sufficiency
		II-f-10	56	Contract / legal act under Union or Member State law
		II-f-11	57	Policies and procedures (outsourcing relationship)
		II-f-12	58	Monitoring

SECTION I: ACCOUNTABILITY CRITERIA / GOVERNANCE CRITERIA

Ref.	Label	Description	C	P
		Policies and procedures		
I-1	Accountability (GDPR Article 24) (Recitals 74, 75, 76, 77, 84)	The entity has implemented organisational measures that ensure authorised management is informed of, involved in and accountable of personal data processing activities. Measures include at least: • the design of appropriate data protection policies and procedures as required by the criteria of this certification mechanism; • the formal allocation of roles and responsibilities regarding data protection topics; • the implementation of formal reporting lines to the entity's management; • a mechanism to formally report any incidents related to data protection and any infringement of the GDPR. The entity's management has formally validated those measures.	X	X
I-2	Policies and procedures (GDPR Article 24) (Recitals 74, 75, 76, 77, 84)	The entity has designed policies and procedures that shall cover at least the following topics: • the record of processing activities (I-4 to I-7); • data subject's rights (I-8, I-9, section II); • data protection principles (sections II & III); • the DPO's roles and responsibilities (I-10 to I-13, among others); • data protection by design and by default; • data protection impact assessment, if applicable (II-f-7, II-f-8); • data transfers, if applicable (II-a-18, III-13); • use and management of processors, if applicable (II-f-9 to II-f-12); • relationships with controllers, if applicable (e.g. communication with the controller/contractual partner, common procedures, etc.) (section III); • internal and external reporting and handling of incidents related to data protection, including data breaches. The entity has taken into account the formal opinion of its DPO on those policies and procedures.	X	X

Ref.	Label	Description	C	P
		The entity's management has formally validated those policies and procedures. In case the entity chooses not to follow the opinion of its DPO it documents this decision as well as all the reasons for doing so and the entity's management formally validate this decision.		
I-3	Review and update of policies and procedures (GDPR Article 24) (Recitals 74, 75, 76, 77, 84)	The entity reviews on a regular basis and at least annually or when significant changes in the data privacy landscape of the entity occur, the operating effectiveness of its data protection governance policies and procedures. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the content of its policies and procedures. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. The review is documented. The reviewer: • checks whether the policies and procedures include all necessary information (cf. individual subsequent criteria); • identifies all changes; • checks whether the policies and procedures need to be updated with regard to any potential changes (see above). Based on this, the reviewer formulates a formal conclusion containing propositions for changes as well as the reason for those changes. The entity's management formally validates the review and its conclusions. Based on the conclusions reached during the review phase, the entity adapts its policies and procedures if deemed necessary and documents all changes. At the end of the review process, the entity's management formally validates all policies and procedures (indicating their role / title, signature and signature date). This includes policies and procedures that were not affected by any changes.	X	X
Record of processing activities				
I-4	Record of processing activities (GDPR Article 30) (Recitals 13, 82)	The entity has implemented a written record (in electronic form) of processing activities under its responsibility that contains for each processing activity in scope at least the following information: • the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; • the purposes of the processing; • the legal basis of the processing • a description of the categories of data subjects and of the categories of personal data;	X	

Ref.	Label	Description	C	P
		• the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; • where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in absence of an EU Commission adequacy decision, the documentation of safeguards; • the envisaged time limits for erasure of the different categories of data; • a general description of the technical and organisational security measures to ensure a level of security the entity deems appropriate to the risk of the processing, including the reasoning why the entity thinks those measures appropriate. The entity has taken into account the formal opinion of its DPO on the content of this record of processing activities and the entity's management has formally validated this record of processing activities.		
I-5	Record of processing activities (GDPR Article 30) (Recitals 13, 82)	The entity has implemented a written record (in electronic form) of all categories of processing activities in scope carried out on behalf of a controller / contractual partner that contains at least the following information: • the name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; • the categories of processing carried out on behalf of each controller; • where possible, a general description of the technical and organisational security measures to ensure a level of security the entity deems appropriate to the risk of the processing, including the reasoning why the entity thinks those measures appropriate; • where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in absence of an EU Commission adequacy decision, the documentation of safeguards. The entity has taken into account the formal opinion of its DPO on the content of this record of processing activities and the entity's management has formally validated this record of processing activities.		X
I-6	Management of the record of processing activities (GDPR Article 30) (Recitals 13, 82)	The entity's management reviews and approves on a regular basis and at least annually, or when significant changes occur, the record of the personal data processing activities under its responsibility to ensure completeness and accuracy of the record. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the content of its record of processing activities. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. The review is documented and the reviewer checks for each processing activity in scope whether all required information (please refer to I-4) is correct, up-to-date and complete.	X	

Ref.	Label	Description	C	P
		Based on this assessment, the reviewer formulates a formal conclusion containing, if applicable, the information to be updated as well as the reason for those changes. The entity's management formally validates the review and its conclusions. Based on the conclusions reached during the review phase, the entity adapts its record of processing activities if deemed necessary and documents all changes. At the end of the review process, the entity's management formally validates the record of processing activities (indicating their role / title, signature and signature date).		
I-7	Management of the record of processing activities (GDPR Article 30) (Recitals 13, 82)	The entity's management reviews and approves on a regular basis and at least annually, or when significant changes occur, the record of all categories of processing activities carried out on behalf of a controller to ensure completeness and accuracy of the record. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the content of its record of processing activities. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. The review is documented and the reviewer checks for each processing activity in scope whether all required information (please refer to I-5) is correct, up-to-date and complete. Based on this assessment, the reviewer formulates a formal conclusion containing, if applicable, the information to be updated as well as the reason for those changes. The entity's management shall formally validate the review and its conclusions. Based on the conclusions reached during the review phase, the entity adapts its record of processing activities if deemed necessary and documents all changes. At the end of the review process, the entity's management formally validates the record of processing activities (indicating their role / title, signature and signature date).		X
Data Subjects' Rights				
I-8	Facilitate the exercise of data subjects' rights (GDPR Article 12) (Recitals 58, 59)	The entity has implemented measures to ensure that a contact point has been appointed that is easily accessible by the data subjects and that is responsible for receiving data subjects' request for exercising their rights referred to in Articles 15 to 22 of the GDPR. The entity's staff is informed of this contact point and its role so that it can redirect any requests from data subjects to it if necessary. The entity has defined and implemented a procedure regarding the handling of data subjects' requests. This procedure is communicated to the data subjects according to the rules set out in II-a-13 / II-a-14 as well as II-a-15 and contains at least the following:	X	

Ref.	Label	Description	C	P

		• The entity formally assesses the request and attributes one or more categories to the request depending on the right(s) of which the data subject makes use (please refer to articles 15 to 22 and to section II).
		• The entity records all requests and documents each step of their conducted execution in compliance with the requirements of the GDPR as well as the requirements set out in certification criteria (please refer to articles 15 to 22 and to section II).
		• The entity has formally established the responsibilities for the processing of such requests.
		• The entity formally assesses the received requests. During this assessment, the entity:
		  ○ analyses if it can clearly identify the data subject:
		  ▪ The entity assesses whether the data subject needs to provide additional information because of reasonable doubts concerning the identity of the data subject (this does not apply to the cases referred to in article 22 / II-a-12).
		  ▪ If the entity decides to request additional information from the data subject, it complies with the principle of data minimisation (please refer to subsection II-c).
		  ▪ With regard to articles 11 and 15 to 20 of the GDPR, in case the entity can demonstrate that it is not in a position to identify the data subject it shall inform the data subject accordingly, if possible, except where the data subject provides additional information enabling his / her identification.
		  ○ defines cases where a request can be considered appropriate or not (e.g. “is the request about personal data?”, “is the request excessive or manifestly unfounded?”, “is there a restriction by national legislation?”);
		  ○ estimates the complexity of the request as well as the expected time necessary to answer the request.
		• If the entity concludes that it cannot comply with the request within one month of receipt of the request, it documents in detail the reasons for this and informs the data subject of any extension within one month of receipt of the request, together with the reasons for the delay. In this case, the entity shall ensure that it complies with the request as soon as possible and at the very latest within 3 months after initial receipt of the request.
		For rejected or partly rejected requests, the entity documents the justification for not taking action and communicates this to the data subject without delay and at the latest within one month of receipt of the request. At the same time, the entity informs the data subject about the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.		

I-9	Facilitate the exercise of data subjects’ rights (GDPR Article 28) (Recitals 81)	The entity has defined and implemented a procedure regarding the handling of data subjects requests, including at least the following: The entity has implemented measures to ensure that a contact point has been appointed that is easily accessible by the contractual partner and / or the controller and that is responsible for receiving and answering the data subjects’ request for exercising their rights forwarded by the controller. • The entity records all received requests and documents each step of their conducted execution. • The entity and the contractual partner have established a clear division of roles and tasks to be performed taking into account the different types of requests likely to occur. In case a request does not correspond to an established procedure, the entity shall contact the contractual partner in order to receive clear instructions. If deemed necessary by the contractual partner and / or the controller, the formal procedure shall be adapted accordingly.		X

Ref.	Label	Description	C	P
		• The procedure includes information on when and how to communicate with the parties involved. This communication includes among others regular status updates to the contractual partner and / or controller. The entity formally analyses the information regarding the request provided by the controller to determine its nature, the estimated complexity and the expected time necessary to answer the request. It then communicates this information without undue delay to the contractual partner and / or the controller so that the controller can comply with the requirements set out in I-8. • If the entity concludes that it cannot comply with the request within the deadline set by the controller, it documents in detail the reasons for this as well as the estimated time to comply with the request and informs the contractual partner and / or the controller accordingly without undue delay. • If the entity concludes that it cannot comply with the request, it documents in detail the reasons for this and informs the contractual partner and / or the controller accordingly without undue delay. Those procedures and all subsequent changes are subject to the opinion of the DPO and are validated by the contractual partner as well as the controller in case the contractual partner is not the controller.		
		DPO		
I-10	Designation (GDPR Article 37) (Recital 97)	The entity has formally appointed a DPO, published the contact details of the DPO and communicated his or her contact details to the supervisory authority. In case the position of the DPO is held by a person who is not an internal staff member of the entity, the DPO is easily accessible from the entity. Similarly, if the position of the DPO is centralized for several entities, the DPO is easily accessible from each entity.	X	X
I-11	Competencies (GDPR Article 37) (Recital 97)	The entity has assessed the DPO's professional qualifications and in particular: • His / her expert knowledge of as well as experience in applying data protection legislation and practices including the following: ○ The DPO has a minimum of 3 years of recent professional experience in the data protection field. In case the DPO does not have at least 3 years of professional experience in data protection, one of the following conditions shall be respected: ▪ The DPO has two years of legal expertise and has followed comprehensive trainings on data protection. This mitigating element is only applicable if the DPO is 100% assigned to the function. ▪ The DPO has access to legal assistance internally, or via a non-limiting service contract with an external firm, covering all GDPR subjects. ○ The DPO has a good understanding of the processing activities carried out by the entity, as well as the corresponding information systems through: ▪ a former professional experience of at least 2 years in the same sector as the entity (optional); ▪ the regular attendance to trainings on business operations and IT / data security (mandatory);	X	X

Ref.	Label	Description	C	P
		▪ free access to and formal communication with the persons responsible for the processing activities as well as the person(s) responsible for information / IT security (e.g. CISO) (mandatory). ○ In case the DPO function is exercised within a team and the person designated as DPO has not all required competencies and experience, collegial skills can be taken into account provided that the team and its composition are formally defined (job descriptions defining tasks and responsibilities, inclusion in the organizational chart) and that the work is effectively carried out by the team (joint participation in discussions impacting data protection, communication and regular exchanges, etc.). The DPO shall maintain his / her knowledge in technical and legal skills through continuous professional development by attending data protection training sessions on at least a yearly basis. • His / her ability to fulfil the tasks mentioned in I-13. These abilities are regularly reviewed together with the entity's management to whom the DPO reports and at least on an annual basis. This review shall also cover the appropriateness of the resources at the disposal of the DPO (e.g. availability, competencies, experiences, etc. of the internal / external support team, training opportunities, collaboration with other teams, etc.). The documentation of this review as well as the conclusions will be formally validated by the DPO as well as the entity's management.		
I-12	Position (GDPR Article 38) (Recital 97)	The entity has implemented measures that: • ensure that the DPO is involved in a timely manner, in all topics which relate to the protection of personal data: ○ The entity has formally identified the topics that require the involvement of the DPO (e.g. data breaches, DPIA, register of processing activities, outsourcing of processing activities, changes in processing activities, etc.). ○ The DPO's consultation and / or involvement is formalized via procedures that are communicated to all concerned personnel. The DPO's job description contains a reference to these procedures and also includes information regarding the participation of the DPO in meetings such as management committees, project coordination committees, new products committees, safety committees or any other committee deemed useful in the data protection framework. ○ The DPO's involvement (based on the procedures cited above as well as other involvements) is documented (e.g. date of involvement, issued opinions, meeting minutes, participation in audits, etc.). • ensure that the DPO is supported by the entity's management in performing his / her tasks. The entity shall provide the DPO with time and resources necessary to carry out those tasks as well as to maintain his / her expert knowledge. The entity shall also provide access to personal data and to processing activities; • ensure that the DPO does not receive any instructions regarding the exercise of his / her tasks. He or she shall not be dismissed or penalised for performing his / her tasks and preferably be employed based on a long-term contract. The DPO shall directly report to the highest management level of the entity. This is among others formalized in the entity's organisational chart. • ensure that data subjects can contact the DPO with regard to all issues related to the processing of their personal data and to the exercise of their rights under the GDPR. The entity communicates the name and contact details to all employees and makes his or her contact details easily accessible on its website or via any other communication channel usually used to communicate with its data subjects.	X	X

Ref.	Label	Description	C	P
		• ensure that the DPO is bound by secrecy or confidentiality concerning the performance of his / her tasks, in accordance with Union or Member State law; • ensure that the DPO is not involved in tasks and duties that could result in a conflict of interests: ○ The entity has formally identified functions that are incompatible with that of DPO and situations that might cause a conflict of interest for the DPO (internal or external). The entity has formally established internal rules to avoid any conflicts of interest for the DPO. ○ In case the DPO (and / or one of his / her team members if applicable) was involved in the design / execution / implementation of a data processing activity at the entity, he / she cannot act as DPO / data protection team member for this processing activity during a transition period of 2 years. This period starts running when the involvement of this person in the processing activity ends. ○ In case the DPO identifies a situation that might constitute a conflict of interest, he / she reports this to the entity's management. In those cases, this conflict of interest is documented.		
I-13	Tasks (GDPR Article 39)	The entity has mandated the DPO to execute at least the following tasks: • To inform and advise the entity and its employees who carry out processing activities, of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions (e.g. through information sessions, awareness campaigns, opinions on data protection topics, data protection trainings etc.). • To monitor and formally report towards management on compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the entity in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. In order to do this, the DPO shall be involved in the drawing up and implementation of an audit plan covering 3 years. The audit plan shall be based on a documented method which shall include elements such as a detailed information about planning requirements, responsibilities and reporting lines, sampling methods used, testing frequency over the year, reporting, audit scope definition, the definition of audit criteria, documentation and audit report as well as the follow-up on nonconformities. The results of these audits shall be communicated in the form of a report to the highest level of management. • To provide advice where requested as regards the data protection impact assessment and monitor its performance. The entity (controller) receives formal advice from the DPO among others on: ○ the necessity to carry out a data protection impact assessment (DPIA); ○ the methodology to be followed when carrying out a DPIA; ○ the decision to perform the DPIA internally or to subcontract it; ○ the measures (including technical and organizational measures) to be implemented to mitigate any risks to the rights and interests of the persons concerned; ○ whether the DPIA has been correctly carried out in compliance with the GDPR and the present certification criteria.	X	X

Ref.	Label	Description	C	P
		If the controller does not follow the opinion provided by the DPO, the written documentation of the DPIA should explicitly justify the reason why the opinion was not taken into consideration. • To cooperate with the supervisory authority; • To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation for DPIAs, and to consult, where appropriate, with regard to any other matter.		
		Data breaches		
I-14	Data breaches (GDPR Articles 12, 33, 34) (Recitals 85, 86, 87, 88)	The entity has implemented technical and organisational measures to identify, manage and if applicable notify personal data breaches to the competent supervisory data protection authority and the data subjects within the timeframes defined by the GDPR. Those measures cover at least: • the formal nomination of one or multiple contact point(s) in charge of collecting and assessing potential data breach events; • the degree of involvement of the DPO. The DPO shall always be informed of each data breach as well as its assessment and handling including the communication to the supervisory data protection authority and / or the data subjects, if applicable; • the awareness raising of all internal and external stakeholders regarding their responsibility to know the procedure and to report data breach events as quickly as possible to the designated point of contact; • the implementation of a methodology to assess whether an event qualifies as a personal data breach as well as to systematically assess the potential risks to the rights and freedoms of natural persons caused by a data breach; • the setup and management of a record of all personal data breaches. The record of personal data breaches must contain for each data breach at least a description of the event, the impact of the event including the risk analysis for data subjects, the root cause, the remediation action taken and the evidence of notification, if applicable; • the communication with the supervisory data protection authority using, if applicable, the competent supervisory authority's notification form or service. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay; • the ability to communicate with data subjects, if required or decided upon on a voluntary basis. This communication is given to the data subjects free of charge and in an easily accessible way and is written in a clear and plain language adapted to the target audience. It shall include at least the following information: o a description of the nature of the personal data breach; o the name and contact details of the data protection officer or other contact point where more information can be obtained; o a description of the likely consequences of the personal data breach; and o a description of 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. This message shall be individual and dedicated only to this breach. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. Furthermore, the entity shall perform a	X	

Ref.	Label	Description	C	P
		formal assessment which is reviewed by the DPO. This assessment shall take into account among other things the nature, circumstances, scope and context of the data breach that occurred as well as the target audience and the type of personal data concerned. Furthermore, it shall include: ○ an analysis evaluating the best approach / format to communicate with the data subjects; ○ an analysis to determine the best structure of such information; ○ an analysis of the language used ensuring it is easily understood by the data subject.		
I-15	Notification of data breaches towards the controller (GDPR Article 33) (Recitals 85, 86, 87, 88)	The entity has implemented technical and organisational measures to detect, manage and notify personal data breaches towards the contractual partner(s) and / or controller(s) within a timeframe allowing the controller to notify the supervisory authority within 72 hours after becoming aware of a personal data breach, should the controller identify a risk to the rights and freedoms of natural persons caused by the data breach. Those measures must cover at least: • the formal nomination of one or multiple contact point(s) in charge of collecting and assessing potential data breach events; • the degree of involvement of the DPO. The DPO shall always be informed of each data breach as well as its assessment and handling; • the awareness raising of all internal and external stakeholders regarding their responsibility to know the procedure and to report data breach events as quickly as possible to the designated point of contact; • the implementation of a methodology (validated by the contractual partner/controller) to assess whether an event qualifies as a personal data breach; • the setup and management of a record of all personal data breaches. The record of personal data breaches must contain for each data breach at least a description of the event, the impact of the event including the risk analysis for data subjects if possible, the root cause, the remediation action taken and the evidence of notification; The notification to the contractual partner / controller shall at least: • describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; • communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; • describe the likely consequences of the personal data breach, if possible; • describe 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. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.		X
Data Protection Awareness & Competencies				

Ref.	Label	Description	C	P
I-16	Awareness trainings & competencies of staff (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope, the entity shall define and document the competencies and experience required of personnel to be able to carry out this processing activity in a secure manner. This includes the competencies and experience of all persons involved directly or indirectly in this processing activity who potentially have an impact on the confidentiality, integrity, availability and resilience of the personal data processed. For this assessment, the entity takes into account among others the record of processing activities (I-4), the data flow diagram (II-f-1), the risk analysis (II-f-2) as well as the risk treatment plan (II-f-3). Based on this assessment, the entity establishes together with its DPO a security and data protection training and awareness programme which is validated by management and which corresponds to the competency requirements defined for each role / position. New employees and external staff shall participate in those sessions at the beginning of their work with the entity. The entity ensures that each employee and external staff follows these sessions at least once a year and documents their participation accordingly. The entity shall assess the competencies and experience of the above-mentioned persons to ensure that they meet the requirements for their specific role. This assessment shall be carried out on an annual basis and shall be documented.	X	
I-17	Awareness trainings & competencies of staff (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope, the entity shall define and document the competencies and experience required of personnel to be able to carry out this processing activity in a secure manner. This includes the competencies and experience of all persons involved directly or indirectly in this processing activity who potentially have an impact on the confidentiality, integrity, availability and resilience of the personal data processed. For this assessment, the entity takes into account among others the record of processing activities (I-5), the data flow diagram (III-5), the risk analysis (III-6) as well as the risk treatment plan (III-7). Based on this assessment, the entity establishes together with its DPO a security and data protection training and awareness programme which is validated by management as well as the contractual partner and which corresponds to the competency requirements defined for each role/position. New employees and external staff shall participate in those sessions at the beginning of their work at the entity. The entity ensures that each employee and external staff follows these sessions at least once a year and documents their participation accordingly. The entity shall assess the competencies and experience of the above-mentioned persons to ensure that they meet the requirements for their specific role. This assessment shall be carried out on an annual basis and shall be documented.		X

SECTION II: PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (CONTROLLER)

SUBSECTION II – A: LAWFULNESS AND TRANSPARENCY OF PROCESSING ACTIVITIES

Ref.	Label	Description
		Lawfulness
II-a-1	Identification of a valid legal basis (GDPR Article 6) (Recitals 39 - 50, 171)	The entity has implemented measures to ensure that a valid legal basis has been identified and validated for each processing activity in scope. The entity has assessed the validity of the identified legal basis in detail –taking into account among others the purpose of the processing - together with all stakeholders and has documented this assessment. The entity has taken into account the formal opinion of its DPO. The entity's management has formally validated this assessment. In case the entity chooses not to follow the opinion of its DPO, it shall document this decision as well as all the reasons for doing so. The entity's management shall formally validate this decision.
II-a-2	Review of the conformity of the identified legal basis (GDPR Article 6) (Recitals 39 - 50, 171)	The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, the identified legal bases of the processing activities in scope. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the legal basis of the processing activities in scope. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. Applying the above-mentioned methodology the reviewer checks whether the chosen legal bases for the processing activities in scope are still valid. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.

II-a-3	Processing based on consent
	(GDPR Article 4, 7, 8)
	(Recitals 38, 40, 42, 43)
		For each processing activity in scope, where processing is based on the data subject's consent, the entity has implemented measures to ensure that the conditions for a valid consent are respected.
		Valid consent is :
		• freely given: The entity has analysed the necessity of consent
		  ○ in case of an imbalance of power (public authorities, employers, etc.);
		  ○ in the context of the provision of a contract or service for which these personal data are not necessary.

Ref.	Label	Description
		• given for a specific purpose: In case of multiple processing purposes, the entity has implemented measures ensuring that the data subject can chose which one to consent to. The entity ensures that consent is presented in a manner that is clearly distinguishable from other matters. • informed; • an unambiguous indication of wishes. The entity has implemented measures ensuring: • consent is obtained before the entity starts processing personal data for which consent is needed; • it keeps a record of consent to demonstrate consent for a defined processing activity exists; • it stored this record of consent in an unaltered manner; • in the context of information society services offered directly to a child below the age of 16 years, the entity has implemented a mechanism to collect consent / authorization from the holder of parental responsibility over the child. The entity has implemented measures ensuring data subjects can withdraw their consent as easily as they gave it and at any given time without detriment. The entity implemented measures to stop the processing activity for which consent is needed in case data subjects withdraw their consent.
II-a-4	Processing based on a contract (GDPR Article 6) (Recital 44)	For each processing activity in scope, where processing is necessary: • for the performance of a contract to which the data subject is party, or • in order to take steps at the request of the data subject prior to entering into a contract, the entity has implemented measures to ensure that personal data and / or contracts are collected and stored in an unaltered manner.
II-a-5	Processing based on a legal obligation (GDPR Article 6) (Recital 45)	For each processing activity in scope, where processing is necessary for compliance with a legal obligation with which the entity is required by law to comply, the entity has for this processing identified and formally assessed the applicable legal obligation.
II-a-6	Processing based on vital interest (GDPR Article 6) (Recital 46)	For each processing activity in scope, where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the entity has assessed the presence of the vital interest at the moment the processing takes place and formally documented this assessment.

Ref.	Label	Description
		Note: This lawfulness basis is only relevant in situations where processing is vital to an individual's survival and where the processing cannot be based on another legal basis.
II-a-7	Processing based on public interest (GDPR Article 6) (Recital 50)	For each processing activity in scope, where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the entity, the entity has: • identified and formally assessed the Union law or Member State law laying down the basis for this processing activity; • if applicable, obtained from the relevant authority a formal document stating that it has vested an official authority in the entity for this processing activity; • implemented measures to be able to suspend the processing activity in case data subjects execute their right to object (article 21 GDPR).
II-a-8	Processing based on legitimate interest (GDPR Article 6) (Recitals 47, 48)	For each processing activity in scope, where processing is necessary for the purposes of the legitimate interests pursued by the entity or by a third party, the entity has implemented the following measures: • The entity implemented a methodology to formally and objectively assess that the entity's interests are not overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child; • The entity implemented measures to ensure that data subject's interests have been expressed and taken into consideration during the assessment; • The entity implemented measures to be able to suspend the processing in case a data subject has executed his right of opposition (article 21 GDPR). *Note: The legislator provides by law for the legal basis for public authorities to process personal data. Consequently, this legal basis should not apply to the processing by public authorities in the performance of their tasks.*

II-a-9	Processing of special categories of personal data
	(GDPR Article 9)
	(Recitals 33, 35, 46, 51, 52, 53, 54, 55, 56, 75)
		For each processing activity in scope, the entity has implemented measures to ensure that processing of special categories of data is strictly prohibited unless a valid legal basis as required by the GDPR is identified and applies (see also II-a-1, II-a-2).
		Depending on the legal basis chosen, the entity has namely addressed the following in addition to the requirements stated in II-a-1 as well as the criteria linked to article 6 GDPR:
		• Data subject's explicit consent (Article 9(2)(a)): In addition to the conditions stated in II-a-3:
		  ○ The entity has assessed whether data subjects are authorised by law to lift the prohibition to process sensitive data by giving their explicit consent for this processing activity.
		  ○ The entity has implemented measures allowing data subjects to give their explicit consent.

Ref.	Label	Description
		• Controller's obligations / specific rights in the field of employment, social security, social protection law (Article 9(2)(b)): The entity has identified and formally assessed the applicable legal basis for this processing activity. • Vital interest when data subject is physically or legally incapable of giving consent (Article 9(2)(c)): The entity has assessed the presence of the vital interest at the moment the processing takes place and formally documented this assessment. • Legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim (Article 9(2)(d)): o The entity has included in its formal assessment whether it fulfils the conditions with regard to its legal form and aim as required in Article 9(2) point d. Furthermore, the entity has assessed whether the processing takes place in the course of its legitimate activities. o The entity has formally assessed whether the processing of special categories of data relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes. o The entity has established and implemented a procedure to prevent that personal data are disclosed outside that body without the explicit consent of the data subjects. • Public data (Article 9(2)(e)): The entity has formally defined and implemented a procedure to check whether the sensitive data to be processed has already been manifestly made public by the data subject. For the processing activity in scope, the entity has documented all steps of this procedure. • Establishment, exercise or defence of legal claims (Article 9(2)(f)): The entity has established that there is a substantial connection between the processing of the sensitive data and the purpose. • Substantial public interest (Article 9(2)(g)): The entity has identified the Union or Member State law(s), which constitute(s) the basis for the processing of sensitive data. • Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (Article 9(2)(h)): o The entity has formally assessed whether it fulfils the conditions with regard to the purpose as required in Article 9(2)(h). o If the processing is based on Union or Member State law, the entity has formally identified the law(s) in question. o If the processing is based on a contract with a health professional, the entity has formally documented this. o Furthermore, the entity has ensured that the person that will be processing the sensitive data is either subject to the obligation of professional secrecy (under Union or Member State law or rules established by national competent bodies) or subject to an obligation of secrecy (under Union or Member State law or rules established by national competent bodies). The entity has included the relevant law(s) or rule(s) in its documentation. • Public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (Article 9(2)(i)): The

Ref.	Label	Description
		entity has identified the Union or Member State law(s), which constitute(s) the legal basis for the processing of sensitive data in scope. • Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 9(2)(j)): The entity has identified the Union or Member State law(s), which constitute(s) the legal basis for the processing of sensitive data in scope.
II-a-10	Right to object (GDPR Articles 12, 21) (Recitals 65, 69, 70, 73)	For each processing activity in scope, the entity has implemented measures to ensure that the "right to object" of a data subject is effectively implemented. The entity has established a procedure explaining how data subjects can exercise their right to object and has communicated it to the data subjects (see below). In particular, the right to object to processing shall be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and is presented clearly and separately from any other information. The entity has assessed whether the data subject has a right to object for the processing activity in scope. The data subject shall have a right to object: • at any time when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, including profiling based on this provision; • at any time when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, including profiling based on this provision; • at any time when personal data are processed for direct marketing purposes, including profiling to the extend that it is related to such direct marketing; • when personal data are processed for scientific or historical research purposes or statistical purposes (unless the processing is necessary for the performance of a task carried out for reasons of public interest). The entity has established and formally implemented a procedure for the assessment of claims of data subjects making use of their right to object, including the following elements: • For processing necessary for the performance of a task carried out in the public interest / in the exercise of official authority vested in the controller or for the purposes of the legitimate interests pursued by the controller / by a third party, the entity shall analyse whether it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. • For personal data processed for scientific or historical research purposes or statistical purposes, the entity shall verify whether the processing is necessary for the performance of a task carried out or reasons of public interest.

Ref.	Label	Description
		This assessment includes a formal opinion of the DPO and has been validated by the entity's management. If the entity concludes in its assessment that processing is still necessary, it will inform the data subject of this and will provide the reasons for doing so. Should the entity's analyses conclude that none of the two above-mentioned points is applicable the entity shall no longer process the personal data of the data subject in question. In this case, the entity has established and implemented a procedure to stop the processing of this data. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.
II-a-11	Right to restriction of processing (GDPR Articles Articles 12, 18, 19) (Recitals 67, 156)	For each processing activity in scope, the entity has implemented measures to ensure that the right to restriction of processing of a data subject is effectively implemented. The entity has established and formally implemented a procedure for the assessment of claims of data subjects making use of their right to restriction of processing. This procedure shall require that the entity assess whether the right to restriction of the processing activity is applicable in a specific situation. The data subject has a right to restriction of processing when: • the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

Ref.	Label	Description
		• the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; • the controller no longer needs the personal data for the purposes of the processing but they are required by the data subject for the establishment, exercise or defence of legal claims; • the data subject has objected to processing pursuant to GDPR Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. Furthermore, the procedure includes also the following: • The entity has defined and implemented technical and organisational measures to restrict the processing of data when the conditions are met (see above). Restriction of processing does not include storage of said data. • The entity has defined and implemented technical and organisational controls to ensure that personal data whose processing is restricted can only be processed: o with the data subject's consent; o for the establishment, exercise or defence of legal claims; o for the protection of the rights of another natural or legal person; o for reasons of important public interest of the Union or of a Member State. In such cases, the entity has formally assessed the reasons to process the data. This assessment includes a formal opinion of the DPO. • The entity shall inform the data subject before lifting the restriction of processing and document this notification. The entity has established an inventory of recipients to whom the personal data have been disclosed. The entity shall communicate any restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. In such cases, the entity has formally assessed the reasons not to communicate the restriction of processing. This assessment includes a formal opinion of the DPO and has been validated by the entity's management. The controller shall inform the data subject about those recipients if the data subject requests it. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include:

Ref.	Label	Description
		• an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.
II-a-12	Automated individual decision-making, including profiling (GDPR Articles 12, 22) (Recitals 71, 72, 91)	For each processing activity in scope, the entity has implemented measures to ensure that data subjects can contest a decision based solely on automated processing which produces legal effect concerning him/her or similarly significantly affects him / her. The entity performs a formal assessment regarding such a processing activity and reviews this assessment on a regular basis, but at least annually. This assessment includes the following: • The entity has formally assessed the necessity to use automated decision-making, including profiling with regard to this processing activity. • The entity has assessed and formally documented whether the decision solely based on automated decision-making / profiling is authorized by law (article 22(2)(b)), is necessary for entering into / performance of a contract between the data subject and the entity, and / or is based on the data subject's explicit consent. • The entity has formally assessed whether this processing activity processes special categories of data and whether article 9(2)(a) & (g) apply (please refer to article 22(4)). The entity has taken into account the formal opinion of its DPO on the content of this record of processing activities and the entity's management has formally validated this assessment. Based on this assessment the entity implements measures to safeguard the data subject's rights and freedoms and legitimate interests which shall include at least the implementation of measures that allow data subjects to make use of their right not to be subject solely to automated decision-making, including profiling, which produces legal effects concerning them or significantly affects them. Such measures shall include at least the provision of information to the data subjects regarding the nature of the processing (please refer to II-a-13, II-a-14, II-a-15) and the implementation of a procedure to follow when data subjects make use of their right (including the requirement to document such cases). In case the automated decision-making, including profiling, is authorized by law (article 22(2)(b)), is necessary for entering into / performance of a contract between the data subject and the entity, and / or is based on the data subject's explicit consent,

Ref.	Label	Description
		the entity shall implement measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain qualified human intervention on the part of the entity, to express his or her point of view and to contest the decision. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.
Transparency		
II-a-13	Availability of information (direct collection) (GDPR Articles 12, 13) (Recitals 39, 58, 59, 60, 61, 62, 63)	For each processing activity in scope, where personal data are collected from the data subject, the entity has implemented measures to ensure that the data subject is provided with the following information at the time when personal data are obtained / collected and free of charge: • the identity and the contact details of the entity and, where applicable, of the entity's representative; • the contact details of the DPO, if a DPO has been designated; • the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; • where the processing is based on the legitimate interest of the entity, the legitimate interests pursued by the entity or by a third party; • the recipients or categories of recipients of the personal data, if any;

Ref.	Label	Description
		• where applicable, the fact that the entity intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; • the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; • the existence of the right to request from the entity access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; • where the processing is based on point data subjects consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; • the right to lodge a complaint with a supervisory authority; • 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; • the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The entity has defined and implemented a procedure outlining the process of the provision / publication of such an information to the data subject. The entity has implemented for each processing activity in scope measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. To ensure transparency, completeness and accuracy, these measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment before providing the information to the data subjects.

Ref.	Label	Description
		Furthermore, the entity shall document the date and time of the information provision / publication as well as the content of the information.
II-a-14	Availability of information (indirect collection) (GDPR Articles 12, 14) (Recital 57, 60, 61, 62)	For each processing activity in scope, where personal data have not been obtained from the data subject, the entity has implemented measures to ensure that the data subject is provided with the following information and free of charge: • the identity and the contact details of the entity and, where applicable, of the entity's representative; • the contact details of the DPO, if a DPO has been designated; • the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; • the categories of personal data concerned; • the recipients or categories of recipients of the personal data, if any; • where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49.1, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available; • the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; • where the processing is based on legitimate interest, the legitimate interests pursued by the entity or by a third party; • the existence of the right to request from the entity access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; • where processing is based on data subjects consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; • the right to lodge a complaint with a supervisory authority; • from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; • the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. The entity has defined and implemented a procedure outlining the process of the provision of such an information to the data subject. The entity has implemented for each processing activity in scope measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand.

Ref.	Label	Description
		To ensure transparency, completeness and accuracy, these measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment before providing the information to the data subjects. Furthermore, the entity shall document the date and time of the information provision as well as the content of the information. The entity has formally assessed at what point in time it provides the data subject with the above-cited information and has documented the reasons for their choice. The data subject shall be informed as soon as possible after the entity has obtained the data, but at the latest within one month. If the personal data are to be used for communication with the data subject, the entity has implemented measures to ensure the data subject be informed at the latest at the time of the first communication. Furthermore, if a disclosure to another recipient is envisaged, the entity has implemented measures to ensure the data subject be informed at the latest when the personal data are first disclosed. In case the entity does not provide the data subject with the above-mentioned information, it has performed a detailed formal assessment of the applicable exception, including evidence supporting the decision not to inform the data subject. The entity does not need to inform the data subject in the following cases: • The provision of such information: ○ proves impossible: The entity has implemented measures ensuring that the information is provided to data subjects as soon as the factors rendering such information impossible no longer exist. ○ would involve a disproportionate effort: The entity has carried out a balancing exercise in its documentation to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. ○ in so far as the obligation referred to in paragraph 1 of Article 14 is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the entity shall take measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Ref.	Label	Description
		• Obtainment or disclosure of personal data is expressly laid down by Union or Member State law to which the entity is subject and which provides measures to protect the data subject's legitimate interests. The entity shall include in its assessment a demonstration on how the law in question applies to them and requires them to either obtain or disclose the personal data in question. • The personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy. The entity shall include in its assessment the law in question as well as a demonstration on how the professional secrecy obligation directly addresses the entity. These assessments have been formally reviewed by the DPO and have been approved by the entity's management.
II-a-15	Information obligation - up to date information (GDPR Articles 12, 13, 14) (Recitals 58, 61, 73)	For each processing activity in scope, the entity has implemented measures to ensure that changes to the processing activity impacting information to be provided as per GDPR Articles 13 and 14 are identified by the entity and communicated in a timely manner to the data subjects. The entity has defined and implemented procedures for identifying and formally assessing such changes including an analysis of its impact on the data subjects and a methodology for determining the timing and the modalities of the communication of this change as well as the identification of the data subjects to be notified. In this context, the entity shall perform a review of the processing activities in scope at least on an annual basis. This review as well as its results shall be documented and shall include a formal opinion of the DPO.
II-a-16	Right of access by the data subjects (GDPR Articles 12, 15) (Recitals 63, 64, 73)	For each processing activity in scope, the entity has implemented measures to ensure that it can implement the "right of access" by the data subjects. In addition to the measures outlined in I-8 the entity has defined and implemented a structured process: • to clearly identify the requested information and the location where it can be found; • for collecting the requested data by involving the relevant systems, services and entities; and • for clearly structuring the data. Furthermore, the entity shall perform a completeness, accuracy and format review prior to sending the information to the data subject. This review shall take into account the formal opinion of the DPO. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand.

Ref.	Label	Description
		These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.
II-a-17	Right to data portability (GDPR Articles 12, 20) (Recitals 68)	For each processing activity in scope where processing is carried out by automated means and is either based on consent or on a contract, the entity has implemented measures to ensure that it can effectively implement the "right to data portability" of a data subject. In addition to the measures outlined in I-8 the entity has formally assessed: • which structured, commonly used and machine-readable format corresponds best to the needs of the data subjects; • how to transmit the data to the data subjects in case they want to receive it themselves; • the technical feasibility of transmitting the data to another controller in case the data subjects request this. Furthermore, the entity shall perform a completeness, accuracy and format review prior to sending the information to the data subject or to another controller. This review shall take into account the formal opinion of the DPO. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject;

Ref.	Label	Description
		• an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.
Transfer of personal data to third countries (when applicable)		
II-a-18	Third country transfers (GDPR Article 46) (Recitals 105, 108, 109, 110, 114)	For each processing activity in scope that involves a transfer of personal data to third countries, the entity has formally assessed whether mechanisms are in place or need to be implemented to ensure compliance with the GDPR (see mechanisms below). The entity has taken into account the formal opinion of its DPO on the content of this assessment and the entity's management has formally validated this assessment. In case this assessment concludes that a mechanism needs to be implemented, the entity's authorized management shall supervise this implementation supported by its DPO. Mechanisms not requiring any specific authorisation from a supervisory authority: • an adequacy decision from the Commission; • a legally binding and enforceable instrument between public authorities or bodies; • binding corporate rules in accordance with Article 47 of the GDPR; • standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR; • standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) of the GDPR; • an approved code of conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or • an approved certification mechanism pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Ref.	Label	Description
		Mechanisms subject to the authorisation from a competent supervisory authority: • contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or • provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. The entity reviews on a regular basis and at least annually or when significant changes in the data privacy landscape of the entity occur, the validity of the mechanism chosen for the data processing activities in scope. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the validity of the chosen mechanism. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. Applying the above-mentioned methodology the reviewer checks whether the chosen mechanism is still valid. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.

SUBSECTION II – B: PURPOSE LIMITATION

Ref.	Label	Description
II-b-1	Quality of purpose definition (GDPR Article 5) (Recitals 39, 58)	For each processing activity in scope, the entity has implemented measures to ensure that: • the purpose for the processing activity in scope is clearly defined and documented; • the entity has formally assessed whether this purpose description is specific, detailed, explicit and legitimate and to ensure that it does not process the data in a manner that is incompatible with this purpose as well as the corresponding legal basis; • the entity has formally reviewed the design of the processing activity to ensure it processes the data according to the defined purpose. The entity has taken into account the formal opinion of its DPO and the entity's management has formally validated the above assessments. The entity shall ensure that the purpose of the data processing activity is described in a way that allows data subjects to understand and assess the impact on their privacy (please refer to II-a-13, II-a-14, II-a-15). The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, these assessments. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the processing activity in scope and its defined purpose. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. Applying the above-mentioned methodology the reviewer checks whether the defined purpose of the processing activity in scope is still valid. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-b-2	Purpose compatibility (GDPR Articles 5, 6) (Recitals 39, 50, 58)	For each processing activity in scope, and where processing is using data collected for another purpose, the entity has implemented measures to ensure it has formally assessed that the processing activity's purpose is compatible with the initial purpose for which the data has been collected. The entity has taken into account the formal opinion of its DPO. The assessment is then formally validated by the management of the entity. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the purpose compatibility. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. Applying the above-mentioned methodology the reviewer checks whether the purpose compatibility is still valid.

		This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.

SUBSECTION II – C: DATA MINIMISATION

Ref.	Label	Description
II-c-1	Process to ensure data minimisation (GDPR Articles 5 and 25) (Recitals 39, 78)	For each processing activity in scope, the entity has implemented measures to ensure that the collection of personal data is adequate, relevant and strictly limited to what is necessary in relation to the purposes for which they are processed. In particular, the entity has formally assessed that it: • cannot achieve the purpose of its processing activity with less (privacy invasive) data (e.g. working with less granular data); • has documented the necessity for each data field (electronic or paper based) in relation to the purpose. The entity has taken into account the formal opinion of its DPO. The assessment is then formally validated by the management of the entity. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the purpose compatibility. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-c-2	Alternative means (GDPR Articles 5 and 25) (Recitals 39, 78)	For each processing activity in scope, the entity has formally assessed the impossibility to reach the purpose(s) in implementing a less intrusive process (i.e. using less intrusive means to collect data). The entity has taken into account the formal opinion of its DPO. The assessment is then formally validated by the management of the entity. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the possible means to collect data. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.

SUBSECTION II – D: ACCURACY

Ref.	Label	Description
II-d-1	Reliability of the data source (GDPR Article 5) (Recital 39)	For each processing activity in scope, the entity has formally assessed that data sources used to collect personal data are relevant and reliable, taking into account the following: • The assessment is based on an up-to-date record kept by the entity containing all used sources to collect personal data for the processing activity in scope. • The entity assesses those data sources with regard to their relevance and reliability using a method defined by the entity. This method shall take into account among others whether data is collected directly or indirectly from the data subjects. In case data subjects did not provide their data directly to the entity, the entity takes into account in its assessment how, when and by whom the data was initially collected and what and how many entities were involved from the time of initial collection until the moment the entity received the data. The entity shall only process personal data coming from sources deemed relevant and reliable based on this assessment. With regard to the method used for this assessment, the entity has taken into account the formal opinion of its DPO. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the reliability of the data source. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-d-2	Accuracy of data (GDPR Article 5) (Recital 39)	For each processing activity in scope, the entity has implemented measures to ensure that personal data is accurate and kept up to date. The entity has defined and implemented a procedure to verify on a regular basis and at least annually the personal data it received, either by directly contacting the data subject, or by contacting the source from which it received the data. The entity documents this verification of data accuracy and has implemented a procedure to update data if necessary.
II-d-3	Right to rectification (GDPR Articles 12, 16 and 19) (Recitals 39, 59, 65, 156)	For each processing activity in scope, the entity has implemented measures to ensure that it can effectively implement the "right to rectification" of a data subject to rectify inaccurate personal data concerning him or her or to complete incomplete personal data. The entity has established a procedure explaining how data subjects can exercise their right to rectification and has communicated it to the data subjects (see also **I-8**). Furthermore, the entity has established and formally implemented a procedure to ensure personal data is rectified / completed in a timely manner after reception of the request. For the processing activities in scope, the entity has set a maximum delay for the completion of this request taking into account elements such as the type of data, the type of data subjects, the sensitivity of the processing activity etc. in order to avoid any negative consequences for the data subjects if their data is not corrected in time.

		The entity has established an inventory of recipients to whom the personal data have been disclosed. The entity shall communicate any rectification of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. In such cases, the entity has formally assessed the reasons not to communicate the rectification of personal data. This assessment includes a formal opinion of the DPO and has been validated by the entity's management. The controller shall inform the data subject about those recipients if the data subject requests it. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.

SUBSECTION II – E: STORAGE LIMITATION

Ref.	Label	Description
II-e-1	Defined retention period (GDPR Article 5) (Recitals 39)	For each processing activity in scope, the entity has implemented measures to ensure that retention periods are defined, communicated and reviewed. To determine retention periods for personal data, the entity has performed a detailed formal assessment which includes an analysis of the applicable legal requirements regarding data retention for each defined processing purpose. Based on this, the entity determines and documents the data retention periods for the personal data processed, including backups and logs. The entity has taken into account the formal opinion of its DPO on the assessment and the entity's management has formally validated this record of processing activities. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the retention periods. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-e-2	Deletion or anonymization of data (GDPR Article 5) (Recitals 39)	For each processing activity in scope, the entity has implemented measures to ensure that data is effectively deleted or anonymised: • at the end of the retention period defined in II-e-1; • where personal data is not, or no longer necessary for the purpose of the processing; • when it no longer needs the data; or • when the conditions for the right to erasure are met (please refer to II-e-3). The entity has defined and implemented a procedure that includes the following: • Based on the record of processing activities as well as the inventory referred to in II-f-1, the entity has performed a detailed formal assessment to determine the effectiveness of the mechanism used to identify and delete / anonymise personal data, including backups and logs, to ensure anonymised data cannot be re-identified and deleted data cannot be restored. This assessment includes a formal opinion of the DPO. • The entity performs tests on a regular basis, and at least once a year to determine whether the mechanism used to anonymise or delete personal data, including backups and logs, is working as defined. Any deviations are documented and corrected in a timely fashion according to a procedure defined by the entity. The DPO is informed of any exception identified.

Ref.	Label	Description

II-e-3	Right to erasure ('right to be forgotten')
	
	(GDPR Articles 12, 17 and 19)
	
	(Recitals 65, 66, 156)
		For each processing activity in scope, the entity has implemented measures to ensure that it can effectively implement the right to erasure of a data subject.
		
		The entity has established a procedure explaining how data subjects can exercise their right to erasure and has communicated it to the data subjects (see also I-8).
		
		The entity has established and formally implemented a procedure for the assessment of data subjects' claims making use of their right to erasure of personal data.
		
		This procedure shall require that the entity assess whether the right to erasure is applicable in a specific situation. The data subject shall have a right to erasure in the following cases:
		
		• the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
		• the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
		• the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
		• the personal data have been unlawfully processed;
		• the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
		• the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
		
		Furthermore, the procedure also includes the following:
		
		• The entity performs a formal and detailed assessment of data subjects' requests for erasure and analyses if processing is still necessary:
		  ○ for exercising the right of freedom of expression and information;
		  ○ for compliance with a legal obligation which requires processing by Union or Member State law to which the entity is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the entity;
		  ○ for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
		  ○ for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
		  ○ for the establishment, exercise or defence of legal claims.
		
		This assessment includes a formal opinion of the DPO and has been validated by the entity's management.
		
		If the entity concludes in its assessment that processing is still necessary and data cannot be erased, it will inform the data subject accordingly and will provide the reasons for doing so.

Ref.	Label	Description
		• The entity has defined and implemented technical and organisational measures to effectively erase the personal data in a timely manner after reception of the request when the conditions are met (see above). The entity has established an inventory of recipients to whom the personal data have been disclosed. The entity shall communicate any erasure of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. In such cases, the entity has formally assessed the reasons not to communicate the erasure of personal data. This assessment includes a formal opinion of the DPO and has been validated by the entity's management. The controller shall inform the data subject about those recipients if the data subject requests it. In case the entity has made the personal data public, it informs controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. The entity formally assesses how it informs these controllers, taking account of available technology and the cost of implementation. Regarding the communication with the data subject, the entity has implemented measures to ensure that: • clear and written plain language is used; • information is given to the data subjects in an easily accessible way before the processing takes place; • where the entity communicates with children, such information is addressed in a clear and plain language that the child can easily understand. These measures shall include a formal assessment that shall at least take into account the nature, circumstances, scope and context of the processing activity as well as the target audience and the type of personal data concerned. Furthermore, this assessment shall include: • an analysis evaluating the best approach / format to communicate with / provide information to the data subject; • an analysis to determine the best structure of such information; • an analysis of the language used ensuring it is easily understood by the data subject. The entity has taken into account the formal opinion of its DPO regarding this assessment and the entity's management has formally validated this assessment. The entity shall provide the information free of charge. In case the entity charges a fee for providing the requested information, it shall have documented evidence regarding the manifestly unfounded or excessive character of the request. Furthermore, the entity shall document how it justifies the amount of the charged fees.

SUBSECTION II – F: INTEGRITY, AVAILABILITY AND CONFIDENTIALITY

Ref.	Label	Description
		Security
II-f-1	Inventory and data flow diagram (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope and in addition to the record of processing activities (I-4), the entity has formally established a complete inventory of all systems, interfaces (internal and external, if applicable) and filing systems (electronic and / or physical) used to carry out this processing activity. In addition, the entity has an up-to-date, detailed and clearly structured data flow diagram containing all steps necessary to carry out this processing activity, including manual steps, transformation and manipulation of data, physical printouts, location of the task performed, and the position / function of the people involved. The entity has taken into account the formal opinion of its DPO and the entity's management has formally validated this inventory and data flow diagram. The entity reviews them on a regular basis and at least annually or when significant changes impacting the processing activity occur. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence this inventory and data flow diagram. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-f-2	Risk analysis (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope, the entity has defined and implemented measures to identify, to analyse and to categorise risks to confidentiality, integrity, availability and resilience of personal data (e.g. accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed). This formal assessment includes an analysis of the potential impact and probability of each identified risk and is based on a method chosen or established by the entity to ensure consistent and meaningful results. For this assessment, the entity shall take into account among others the record of processing activities (I-4), the inventory and the data flow diagram (II-f-1) of the processing activities in scope. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the risk analysis. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc.

Ref.	Label	Description
		This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-f-3	Risk treatment (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope, the entity has defined and implemented policies and procedures to establish and put in place a risk treatment plan for each identified risk (II-f-2). This risk treatment plan shall be documented in detail and shall be established and carried out according to a defined method. This method shall include risk treatment strategies allowing to mitigate, to reduce or to avoid the identified risks. In case the entity choses to accept a risk or a residual risk, it clearly documents this in the risk treatment plan and includes the reasons for doing so. The entity shall describe in detail what technical and organisational measures it implemented to address the identified risk(s) including elements such as frequency of controls, person / function carrying out / overseeing controls, target / threshold for the control to be successful, required documentation of the control, etc. The entity shall evaluate the effectiveness of the design of those measures. The entity: • defines this risk treatment plan before implementing new processing activities; • reviews the effectiveness of this plan at least on an annual basis or when changes impacting the risk evaluation occur and adapts the risk treatment plan if necessary; • takes into account the formal opinion of the DPO. The entity's management formally validates the risk treatment plan.
II-f-4	Documented implementation of organisational and technical measures (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope, the entity has implemented the operational and technical measures documented in the validated risk treatment plan (II-f-3). The entity ensures that the performance of the implemented measures is documented in detail. On a daily basis, reports on controls performed and security incidents related to the processing activities in scope are provided to the DPO and the entity's management.
II-f-5	Audit (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	For each processing activity in scope, the entity ensures that an independent audit of the effectiveness of the design and implementation of the technical and organisational measures ensuring secure processing of personal data take place. The DPO shall be involved in all stages of the audit planning and execution. These audits are performed by independent internal or external auditors, at least on an annual basis or when changes occur. The entity, together with the DPO has established rules to define the type of changes triggering an audit.

Ref.	Label	Description
		The auditors shall establish together with the DPO an audit plan covering 3 years and based among others on the record of processing activities, the inventory and the data flow diagram of processing activities, the risk analysis and the validated risk treatment plan as well as the precedent audits performed (including all discovered nonconformities). The audit plan shall be based on a documented method which shall include elements such as a detailed information about planning requirements, responsibilities and reporting lines, sampling methods used, testing frequency over the year, reporting, audit scope definition, the definition of audit criteria, documentation and audit report as well as the follow-up on nonconformities. The results of these audits shall be communicated in the form of a report to the highest level of management.
II-f-6	Follow-up on audits (GDPR Articles 5, 32) (Recitals 29, 39, 75 – 79, 83, 116, 123)	The entity shall perform an evaluation of the nonconformities discovered during the audit in order to identify their cause(s) and to assess their impact on the processing activities in scope (as well as the personal data concerned). The entity shall then correct those nonconformities in a timely manner and review the effectiveness of the corrective action taken. This process is documented in detail and the entity takes into account the formal opinion of its DPO. The entity's management shall validate the corrective actions taken.
Data protection impact assessment (DPIA)		
II-f-7	DPIA (GDPR Article 35) (Recitals 72, 75, 84, 89, 90, 91, 92, 93, 94, 95)	For each processing activity in scope, the entity has assessed and documented the decision to perform a DPIA prior to the processing. In case the entity decides not to perform a DPIA, the decision together with the assessment that leads to the decision is approved by the entity's management based on the opinion of the DPO. In case the entity decides to perform a DPIA, the DPIA is documented in detail and covers at least the following elements: • a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the entity; • an assessment of the necessity and proportionality of the processing operation in relation to the purposes (including elements such as data minimisation and minimisation of stored data, purpose compatibility, alternative means, etc.); • an assessment of the identified risks to the rights and freedoms of data subjects; • the measures envisaged to address these risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. The DPIA includes a formal opinion of the DPO and has been validated by the entity's management. The entity reviews the DPIA on a regular basis and at least annually or when significant changes impacting the DPIA occur. The entity takes into account the formal opinion of its DPO.

Ref.	Label	Description
		For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the DPIA. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. During this review, the entity: • shall reassess its decision not to perform a DPIA, in case it has decided not to perform one; • shall carry out a review to assess if processing is performed in accordance with the DPIA. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
II-f-8	DPIA - Prior consultation (GDPR Article 36) (Recitals 37, 84, 94, 95, 96)	For each processing activity in scope, where the DPIA indicates that the processing would result in a high risk for the rights and freedoms of the data subjects after measures have been taken by the entity to mitigate the risk, the entity has consulted the CNPD, the national the supervisory authority, prior to the implementation of the processing activity. In case the CNPD is of the opinion that the intended processing would infringe the GDPR, in particular where the entity has insufficiently identified or mitigated the risk, the entity documents how the written advice that has been provided by the CNPD has been fully addressed – prior to implementing the processing activity.
		Outsourcing
II-f-9	Assessment of sufficiency (GDPR Article 28) (Recital 81)	For each processing activity in scope where the entity uses a processor, the entity shall perform the following prior and during the engagement of that processor: • define and document the competencies and experience of personnel in contact with the processor according to I-16; • identify and analyse the risks related to the use of the processor according to II-f-2 and perform a DPIA according to II-f-7 and II-f-8, if applicable; • establish and put in place a risk treatment plan for each identified risk according to II-f-3; • ensure that the organisational and technical measures defined in the validated risk treatment plan are correctly implemented and documented according to II-f-4; • perform audits as well as the follow-up on those audits according to II-f-5 and II-f-6.
II-f-10	Contract / legal act under Union or Member State law	For each processing activity in scope, where the entity uses a processor, it has a contract in place that fulfils at least the following requirements for the processor: • The processor processes the personal data only on documented instructions from the entity, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is

Ref.	Label	Description
	(GDPR Article 28) (Recital 81)	subject. In such a case, the processor shall inform the entity of that legal requirement before starting the processing, unless that law prohibits such information on important grounds of public interest. • The processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. • The processor takes all measures required to ensure secure processing. Those measure shall at least ensure the same level of security that is required of the entity itself (please refer to the security requirements in subsection II-e). • The processor does not engage another processor without prior specific or general written authorisation of the entity. In case of general written authorisation, the processor shall inform the entity of any intended changes concerning the addition or replacement of other processors, thereby giving the entity the opportunity to object to such changes. Where a processor engages another processor for carrying out specific processing activities on behalf of the entity, the same data protection obligations as set out in the contract or other legal act between the entity and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing guarantees to implement technical and organisational measures in such a manner that the processing will meet the requirements of GDPR. • The processor, taking into account the nature of the processing, assists the entity by technical and organisational measures, insofar as this is possible, for the fulfilment of the entity's obligation to respond to requests for exercising the data subject's rights. • The processor assists the entity in ensuring compliance with his obligations taking into account the nature of processing and the information available to the processor. • At the choice of the entity the processor deletes or returns all the personal data to the entity after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data. • The processor makes available to the entity all information necessary to demonstrate compliance with the obligations and allows for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
II-f-11	Policies and procedures (outsourcing relationship) (GDPR Article 28) (Recital 81)	The contractual provisions mentioned in II-f-10 are supported by shared policies and procedures validated by both parties that establish in more detail how the contractual elements are implemented, executed and monitored in practice. In addition to the contractual points mentioned above, those policies and procedures shall also include at least the following elements in detail: • Distribution of roles and responsibilities on both sides, including contact information for specific situations; • Data subjects' rights request management; • Data breach management; • Data protection awareness training programmes; • Data retention periods. The entity has performed an assessment to ensure that those policies and procedures allow for compliance to these certification criteria. The entity has taken into account the formal opinion of its DPO on the content of these policies and procedures and the entity's management as well as the management of the processor has formally validated them. The review procedure follows the rules set out in I-3 with the addition that the policies and procedures are validated by both parties of the contract.

Ref.	Label	Description
II-f-12	Monitoring (GDPR Article 28) (Recital 81)	For each processing activity in scope, where the entity uses a processor, it has defined audit / monitoring and due diligences procedures that ensure at least annually that contractual arrangements regarding data protection are satisfied. For each processing activity in scope, the entity ensures that an independent audit of the correct implementation of the contractual obligations take place. These audits are performed by independent internal or external auditors, at least on an annual basis or when changes occur. The entity, together with the processor and the DPO, has established rules to define the type of changes triggering an audit. The auditors shall establish an audit plan covering 3 years. The method used shall be documented and shall include detailed information about planning requirements, responsibilities and reporting lines, sampling methods used, reporting, audit scope definition, the definition of audit criteria, documentation and audit report. The resulting audit report shall be communicated to the entities management as well as the DPO. The entity shall perform an evaluation of the nonconformities discovered during the audit in order to identify their cause(s) and to assess their impact on the processing activities in scope (as well as the personal data concerned) as well as on the contractual agreement. The entity shall then ensure that those nonconformities are corrected in a timely manner by the processor and review the effectiveness of the corrective action taken. This process is documented in detail and the entity takes into account the formal opinion of its DPO. The entity's management shall validate the corrective actions taken.

SECTION III: PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (PROCESSOR)

Ref.	Label	Description
	Contracts between processor and controller / between sub-processor and processor	
III-1	Contract / legal act under Union or Member State law (GDPR Articles 28, 29) (Recital 81)	The entity has a contract or legal act under Union or Member State law with each contractual partner (i.e. controller or processor) that is binding on the entity with regard to the contractual partner and that sets out: • the subject-matter and duration of the processing in scope, • the nature and purpose of this processing, • the type of personal data and categories of data subjects, and • the obligations and rights of the contractual partner as well as the controller. It stipulates that the entity: • processes the personal data only on documented instructions from the contractual partner (formally validated and authorised by the controller in case the contractual partner is not the controller), including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the entity is subject. In such a case, the entity shall inform the contractual partner of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; • ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; • takes all measures required to ensure secure processing; • does not engage another processor without prior specific or general written authorisation of the contractual partner and the controller. In the case of general written authorisation, the entity shall inform the contractual partner of any intended changes concerning the addition or replacement of other processors, thereby giving the contractual partner and the controller the opportunity to object to such changes. Where the entity engages another processor for carrying out specific processing activities on behalf of the contractual partner, the same data protection obligations as set out in the contract or other legal act between the contractual partner and the entity shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing guarantees to implement technical and organisational measures in such a manner that the processing will meet the requirements of GDPR;

Ref.	Label	Description
		• taking into account the nature of the processing, assists the contractual partner by technical and organisational 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; • assists the contractual partner and the controller in ensuring compliance with his obligations taking into account the nature of processing and the information available to the entity; • at the choice of the controller, deletes or returns all the personal data to the contractual partner or the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; • makes available to the contractual partner all information necessary to demonstrate compliance with the obligations and allows for and contribute to audits, including inspections, conducted by the contractual partner or the controller or another auditor mandated by either of them.
III-2	Policies and procedures (outsourcing relationship)	The contractual provisions mentioned in III-1 are supported by shared policies and procedures validated by both parties that establish in more detail how the contractual elements are implemented, executed and monitored in practice. In addition to the contractual points mentioned above, those policies and procedures shall also include at least the following elements in detail: • Distribution of roles and responsibilities on both sides, including contact information for specific situations; • Data subjects' rights request management; • Data breach management; • Data protection awareness training programmes; • Data retention periods. The entity has performed an assessment to ensure that those policies and procedures allow for compliance to these certification criteria. The entity has taken into account the formal opinion of its DPO on the content of these policies and procedures and the entity's management as well as the management of the processor has formally validated them. The review procedure follows the rules set out in requirement I-3 with the addition that the policies and procedures are validated by both parties of the contract.
III-3	Limitation of processing to documented instructions (GDPR Articles 28, 29) (Recital 81)	For each processing activity in scope, the entity has documented and implemented measures to ensure that processing of personal data for its contractual partner is limited to the processing activity defined in the documented instructions from the latter unless required to do otherwise by Union or Member State law to which the entity is subject. In the latter case, the entity has documented this legal obligation. The entity shall perform a review at least on an annual basis or when changes impacting the processing activity occur (e.g. changes in the documented instructions, changes in technology, changes in the legal framework, etc.). During this review,

Ref.	Label	Description
		the entity shall formally assess whether the processing performed corresponds to the documented instruction received by the controller or the contractual partner (authorised and validated by the controller). In case the processing performed by the entity does not match the documented instructions, the entity documents the reasons for this in detail (e.g. applicable law(s), etc.). In case the entity did not follow the documented instructions without a valid reason such as a legal requirement, the entity shall identify the cause of the infringement and correct it in a timely manner. The entity shall take into account the opinion of the DPO. The review has been formally validated by the entity's management. The entity shall provide the contractual partner with a report of this review (excluding exceptions mentioned in III-4, if applicable).
III-4	Processing without instructions (GDPR Articles 28, 29) (Recital 81)	For each processing activity in scope, the entity informs the contractual partner in case of a legal obligation to process, without prior instructions from the controller or the contractual partner, the controller's data (unless prohibited by law on important grounds of public interest). This information is provided to the contractual partner: • prior to the implementation of the processing activity; • at least on an annual basis; • prior to a change in the applicable legal framework. In case the entity does not inform the contractual partner, it has identified and assessed the applicable law on important grounds of public interest. The entity has taken into account the formal opinion of its DPO. The assessment has been formally validated by the management of the entity.
Security		
III-5	Inventory and data flow diagram (GDPR Article 32) (Recitals 39, 75 – 79, 83)	For each processing activity in scope and in addition to the record of processing activities (I-5), the entity has formally established a complete inventory of all systems, interfaces (internal and external, if applicable) and filing systems (electronic and / or physical) used to carry out this processing activity. In addition, the entity has an up-to-date, detailed and clearly structured data flow diagram containing all steps necessary to carry out this processing activity, including manual steps, transformation and manipulation of data, physical printouts, location of the task performed, and the position / function of the people involved.

Ref.	Label	Description
		The entity has taken into account the formal opinion of its DPO and the entity's management has formally validated this inventory and data flow diagram. The entity reviews them on a regular basis and at least annually or when significant changes impacting the processing activity occur. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence this inventory and data flow diagram. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review.
III-6	Risk analysis (GDPR Article 32) (Recitals 39, 75 – 79, 83)	For each processing activity in scope, the entity has defined and implemented measures to identify, to analyse and to categorise risks to confidentiality, integrity, availability and resilience of personal data (e.g. accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed). This formal assessment includes an analysis of the potential impact and probability of each identified risk and is based on a method chosen or established by the entity and validated by the contractual partner / controller to ensure consistent and meaningful results. For this assessment, the entity shall take into account among others the input of the contractual partner / controller, the record of processing activities (I-5), the inventory and the data flow diagram (III-5) of the processing activities in scope. The entity reviews on a regular basis and at least annually or when significant changes impacting the processing activity occur, this assessment. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the risk analysis. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. This review is documented and its outcome is validated by the entity's management. In case the entity chooses not to follow the opinion of its DPO it shall include its decision as well as the reasons for doing so in the documentation of the review. The entity will provide the contractual partner with this assessment at least on an annual basis.
III-7	Risk treatment	For each processing activity in scope, the entity has defined and implemented policies and procedures to establish and put in place a risk treatment plan for each identified risk (please refer to III-6).

Ref.	Label	Description
	(GDPR Article 32) (Recitals 39, 75 – 79, 83)	This risk treatment plan shall be documented in detail and shall be established and carried out according to a defined method. This method shall include risk treatment strategies allowing to mitigate, to reduce or to avoid the identified risks. In case the entity choses to accept a risk or a residual risk, it clearly documents this in the risk treatment plan and includes the reasons for doing so. This must be explicitly validated by the contractual partner. The entity shall describe in detail what technical and organisational measures it implemented to address the identified risk(s) including elements such as frequency of controls, person / function carrying out / overseeing controls, target / threshold for the control to be successful, required documentation of the control, etc. The entity shall evaluate the effectiveness of the design of those measures. The entity: • defines this risk treatment plan before implementing new processing activities; • reviews the effectiveness of this plan at least on an annual basis or when changes impacting the risk evaluation occur and adapts the risk treatment plan if necessary; • takes into account the formal opinion of the DPO. The entity's management as well as the contractual partner formally validate the risk treatment plan.
III-8	Documented implementation of organisational and technical measures (GDPR Article 32) (Recitals 39, 75 – 79, 83)	For each processing activity in scope, the entity has implemented the operational and technical measures documented in the validated risk treatment plan (please refer to III-7). The entity ensures that the performance of the implemented measures is documented in detail. On a daily basis, reports on controls performed and security incidents related to the processing activities in scope are provided to the DPO and the entity's management. The entity also provides the contractual partner with a report on a regular basis (as defined by the contract but at least on a weekly basis).
III-9	Audit (GDPR Article 32) (Recitals 39, 75 – 79, 83)	For each processing activity in scope, the entity ensures that an independent audit of the effectiveness of the design and implementation of the technical and organizational measures ensuring secure processing of personal data take place. The DPO shall be involved in all stages of the audit planning and execution. The entity decides together with the contractual partner the involvement of the latter in the different stages of this audit. These audits are performed by independent internal or external auditors, at least on an annual basis or when changes occur. The entity, together with the DPO has established rules to define the type of changes triggering an audit. The auditors shall establish together with the DPO an audit plan covering 3 years and based among others on the record of processing activities, the inventory and the data flow diagram of processing activities, the risk analysis and the validated risk treatment plan as well as the precedent audits performed (including all discovered nonconformities).

Ref.	Label	Description
		The audit plan shall be based on a documented method which shall include elements such as a detailed information about planning requirements, responsibilities and reporting lines, sampling methods used, testing frequency over the year, reporting, audit scope definition, the definition of audit criteria, documentation and audit report as well as the follow-up on nonconformities. The results of these audits shall be communicated in the form of a report to the highest level of management as well as to the contractual partner.
III-10	Follow-up on audits	The entity shall perform an evaluation of the nonconformities discovered during the audit in order to identify their cause(s) and to assess their impact on the processing activities in scope (as well as the personal data concerned). The entity shall then correct those nonconformities in a timely manner and review the effectiveness of the corrective action taken. This process is documented in detail and the entity takes into account the formal opinion of its DPO. The entity's management shall validate the corrective actions taken and provide a report to the contractual partner.
Subcontracting		
III-11	Assessment of sufficiency (GDPR Article 28) (Recital 81)	For each processing activity in scope where the entity uses a processor, the entity shall perform the following prior and during the engagement of that processor: • define and document the competencies and experience of personnel in contact with the processor according to I-17; • identify and analyse the risks related to the use of the processor according to III-6; • establish and put in place a risk treatment plan for each identified risk according to III-7; • ensure that the organisational and technical measures defined in the validated risk treatment plan are correctly implemented and documented according to III-8; • perform audits as well as the follow-up on those audits according to III-9 and III-10.
III-12	Subcontracting (GDPR Article 28) (Recital 81)	For each processing activity in scope for which the entity intends to subcontract the processing activity, entirely or partially, to another processor, the entity has formally assessed that the subcontracted processor offers the same level of guarantees that the entity provides to its contractual partner. This assessment takes into account the opinion of the DPO. The management has validated this assessment and provided it to the contractual partner of the entity. The entity has implemented measures to ensure that: • it obtains prior written authorisation from the contractual partner as well as the controller if the contractual partner is not the controller;

Ref.	Label	Description
		• in case a general authorisation is in place, it informs all contractual partners about the new subcontracting and provide them with opportunity to refuse it. The entity has put in place a contract that ensures the same obligations in regards to data protection requirements than with its initiating contractual partner.
		Transfer of personal data to third countries (when applicable)
III-13	Third countries (GDPR Article 46) (Recitals 105, 108, 109, 110, 114)	For each processing activity in scope that involves a transfer of personal data to third countries, the entity has formally assessed whether mechanisms are in place or need to be implemented to ensure compliance with the GDPR (see mechanisms below). The entity has taken into account the formal opinion of its DPO on the content of this assessment and the entity's management has formally validated this assessment. In case this assessment concludes that a mechanism needs to be implemented, the entity's authorized management shall supervise this implementation supported by its DPO. Mechanisms not requiring any specific authorisation from a supervisory authority: • an adequacy decision from the Commission; • a legally binding and enforceable instrument between public authorities or bodies; • binding corporate rules in accordance with Article 47 of the GDPR; • standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR; • standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) of the GDPR; • an approved code of conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or • an approved certification mechanism pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. Mechanisms subject to the authorisation from a competent supervisory authority: • contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or

Ref.	Label	Description
		• provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. The entity shall inform the data controller of this assessment before starting the processing activity. The choice of a mechanism shall be subject to the opinion of the DPO and shall be validated by the data controller before the processing activity starts. The entity reviews on a regular basis and at least annually or when significant changes in the data privacy landscape of the entity occur, the validity of the mechanism chosen for the data processing activities in scope. The entity takes into account the formal opinion of its DPO. For this review, the entity has implemented a method ensuring that it took into account all factors likely to influence the validity of the chosen mechanism. Such factors can be external or internal and include among others changes in the applicable regulatory framework, changes in the entity's structure such as outsourcing, organisational or technical changes, etc. Applying the above-mentioned methodology the reviewer checks whether the chosen mechanism is still valid. This review is documented and its outcome is validated by the entity's management as well as the controller.
End of the provision of services relating to processing		
III-14	Return / deletion of data (GDPR Article 28) (Recital 81)	The entity, together with the contractual partner, has established and implemented procedures to ensure, at the request of the controller, to delete or to return all the personal data to the controller after the end of the provision of services relating to processing, and to delete existing copies unless Union or Member State law requires storage of the personal data.

6 ANNEX

ANNEX 1: CERTIFICATE EXAMPLE

[…]

ANNEX 2: CERTIFICATION TIMELINES

[…]

ANNEX 3: MAPPING OF GDPR-CARPA CERTIFICATION CRITERIA

The below mapping table serves as a reference table to demonstrate that the GDPR-CARPA certification criteria meet the mandatory compliance aspects.

Mandatory compliance aspects	GDPR-CARPA Criteria
Lawfulness of data processing pursuant to Article 6	Section II: Principles relating to processing of personal data (controller): Subsection II - a: Lawfulness and transparency of processing activities
Principles of data processing pursuant to Article 5	Section II: Principles relating to processing of personal data (controller): Subsection II – a: Lawfulness and transparency of processing activities Subsection II – b: Purpose limitation Subsection II – c: Data minimisation Subsection II – d: Accuracy Subsection II – e: Storage limitation Subsection II – f: Integrity, availability and confidentiality
Data subjects' rights pursuant to Articles 12-23	Section I: Accountability criteria / Governance criteria (Data subjects' rights) Section II: Principles relating to processing of personal data (controller): Subsection II – a: Lawfulness and transparency of processing activities Subsection II – d: Accuracy Subsection II – e: Storage limitation Section III: Principles relating to processing of personal data (processor) (Exercise of rights of data subjects)
Obligation to notify data breaches pursuant to article 33	Section I: Accountability criteria / Governance criteria (Policies and procedures; Data breach)
Data protection by design and by default, pursuant to article 25	Section II: Principles relating to processing of personal data (controller): Subsection II – f: Integrity, availability and confidentiality Section III: Principles relating to processing of personal data (processor) (Security)
Data protection impact assessment, pursuant to article 35.7(d) has been conducted, if applicable	Section I: Accountability criteria / Governance criteria (DPO) Section II: Principles relating to processing of personal data (controller): Subsection II – f: Integrity, availability and confidentiality
Technical and organisational measures put in place pursuant to Articles 32	Section I: Accountability criteria / Governance criteria (Policies and procedures) Section II: Principles relating to processing of personal data (controller): Subsection II – f: Integrity, availability and confidentiality Section III: Principles relating to processing of personal data (processor) (Security)