GDPR-CARPA

GDPR-CERTIFIED ASSURANCE REPORT-BASED PROCESSING ACTIVITIES

Abstract

Document to the attention of organizations that want to obtain certification of processing activities under the GDPR-CARPA certification mechanism.

Commission nationale pour la protection des données

The Commission Nationale pour la protection des données ('CNPD') prepared this document in collaboration with representatives from the audit profession. It contains the criteria for the GDPR-CARPA certification mechanism as well as further information on the certification mechanism.

The certification criteria in this document constitute mandatory requirements that entities wishing to receive a GDPR-CARPA certification for one or several processing operations need to respect. The evaluation of organisational and technical data protection measures as well as reporting needs to follow the ISAE 3000 standard. Furthermore, only certification bodies accredited by the CNPD can grant a GDPR-CARPA certification.

About the 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 Management (ISQM1), Auditing, Review, Other Assurance and Related Services Pronouncements.

Versioning:

Version	Description	Date
V0.1	Initial version	11/04/2019
V1.0	Revised version	13/05/2022
V2.0	Revised version	06/07/2023

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 the GDPR is a voluntary process to assist controllers and / or processors in supporting their demonstration of compliance with the GDPR. This means that they can demonstrate the existence and implementation of appropriate measures defined by a GDPR certification mechanism that has been adopted by a supervisory authority in the case of a national certification mechanism or the European Data Protection Board ('EDPB') for European certification mechanism (EU seal). Once acquired, certification is a legally binding tool and entities commit to comply with the certification criteria throughout the validity period of the certificate. Furthermore, they agree to submit to regular evaluations undertaken by the accredited certification body.

Article 42(4) of the 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.

1.2 ROLE OF THE CNPD

Article 57(1)(q) of the GDPR provides that the supervisory authority shall conduct the accreditation of a certification body pursuant to Article 43 as a 'supervisory authority task'. Article 58(3)(e) provides that the supervisory authority has the authorisation and advisory power to accredit certification bodies pursuant to Article 43.

In Luxembourg, the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework has stipulated that certification bodies are to be accredited by the CNPD. The GDPR-CARPA certification mechanism is linked to the accreditation criteria "Luxembourg accreditation requirements of certification bodies (art 43(1)(a)) – Set Alpha" which contain the mandatory requirements that a certification body needs to fulfil in order to be eligible for an accreditation by the CNPD.

GDPR-CARPA certification can only be granted by certification bodies that have been accredited by the CNPD. The list of accredited certification bodies is published on the CNPD website and the GDPR-CARPA accreditation requirements are available on request (email: certification@cnpd.lu).

2 RELEVANT DEFINITIONS

2.1 GDPR (ARTICLE 4) – ISO 17065

- **'Accreditation'** means an attestation[1] by a national accreditation body and/or by a supervisory authority, that a certification body[2] is qualified to carry out certification pursuant to articles 42 and 43 of the GDPR, taking into account EN-ISO/IEC 17065/2012 and the additional requirements established by the supervisory authority and/or by the European Data Protection Board. In Luxembourg, article 43(1)(a) of the GDPR applies which means that accreditation is granted by the CNPD.
- **'Certification'** means the assessment[3]and impartial, third party attestation that the fulfilment of certification criteria has been demonstrated.
- **'Certification body'** means a third-party conformity assessment body[4]operating a certification mechanism[5].
- **'Certification mechanism'** means a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply.
- **'Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **'Criteria' or 'certification criteria'** means the criteria against which a certification (conformity assessment) is performed[6]. In the context of the GDPR-CARPA certification mechanism, this term refers to the criteria that are listed in this document.
- **'GDPR'** refers to Regulation (EU) 2016/679 of the European parliament and the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- **'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[1] Cf. article 2(10) Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products.

[2] Cf. with the definition of the term "accreditation" pursuant to ISO 17011.

[3] Third-party conformity assessment activity is performed by an organisation that is independent of the person or organization that provides the object, and of user interests in that object, cf. ISO 17000, 2.4.

[4] See ISO 17000, 2.5: "body that performs conformity assessment services"; ISO 17011: "body that performs conformity assessment services and that can be the object of accreditation"; ISO 17065, 3.12.

[5] Cf. article 42(1), 42(5) GDPR.

[6] Cf. article 42(5).

- '**Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **'Processor'** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

2.2 ISAE 3000 (A12)

- '**Assurance engagement**' means an engagement in which a practitioner aims to obtain sufficient appropriate evidence in order to express a conclusion designed to enhance the degree of confidence of intended users other than the responsible party about the subject matter information (i.e. the outcome of the measurement or evaluation of an underlying subject matter – here the target of evaluation – against the criteria). In the context of the GDPR-CARPA certification mechanism this term refers to the audit report / assurance report that underpins the certification decision.
- **'Criteria'** means the benchmarks used to measure or evaluate the underlying subject matter. The "applicable criteria" are the criteria used for the particular assurance engagement. In the context of the GDPR-CARPA certification mechanism, this term refers to the criteria that are listed in this document.
- **'Engagement partner'** means the partner or other person in the firm who is responsible for the engagement and its performance, and for the assurance report that is issued on behalf of the firm, and who, where required, has the appropriate authority from a professional, legal or regulatory body.
- **'Engaging party'** means the party(ies) that engage(s) the practitioner to perform the assurance engagement. In the context of the GDPR-CARPA certification mechanism those terms refers to either the data controller or the data processor who intends to obtain certification.
- **'Evidence'** means information used by the practitioner in arriving at the practitioner's conclusion. Evidence includes both information contained in relevant information systems, if any, and other information.
    - 'Sufficiency' of evidence is the measure of the quantity of evidence.
    - 'Appropriateness' of evidence is the measure of the quality of evidence.
- **'Practitioner'** means the individual(s) conducting the engagement (usually the engagement responsible or other members of the engagement team, or, as applicable, the certification body). Where this ISAE 3000 standard expressly intends that a requirement or responsibility be fulfilled by the engagement partner, the term "engagement partner" rather than "practitioner" is used. In the context of the GDPR-CARPA certification mechanism this term refers to the personnel employed by the certification body as well as personnel working under an individual contract / formal agreement placing them within the management control and systems / procedures of the certification body.

- **'Reasonable assurance engagement'** means an assurance engagement in which the practitioner reduces assurance engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the practitioner's conclusion. The practitioner's conclusion is expressed in a form that conveys the practitioner's opinion on the outcome of the measurement or evaluation of the underlying subject matter against criteria.

2.3 OTHER DEFINITIONS

- **'Contractual partner'** in the context of this certification mechanism is a term used in certification criteria applying to processors. The contractual partner can be:
  - the controller of the processing activities in scope of the certification for which the entity acts as a processor, or
  - a (sub-)processor for which the entity acts as a sub-processor.
- **'Management'** comprises the people that manage or direct an entity and that are responsible and accountable for the processing activity to be certified / certified (target of evaluation).

3 GENERAL CONSIDERATIONS

3.1 SCOPE OF THE GDPR-CARPA CERTIFICATION MECHANISM

The GDPR-CARPA certification is designed to provide data controllers and processors with a high level of reasonable assurance that they have set up and implemented technical and organisational measures helping them 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 this certification mechanism is to support controllers and processors in their obligation to implement appropriate technical 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.

3.1.1 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.

3.1.2 SCOPE LIMITATION & EXCLUSIONS

While information security elements have been integrated in the mechanism, 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 need to be considered.

In addition, only controllers and processors established in Luxembourg, under the supervision of the CNPD can apply for a GDPR-CARPA certification.

GDPR-CARPA is also not suitable:

- for certifying personal data processing specifically targeting minors under 16 years old;
- for the certification of processing activities in the context of a joint controllership;
- for processing activities in the context of article 10 GDPR, except those that are clearly defined and regulated by Luxembourgish or European Laws and for which the CNPD is the competent supervisory authority (e.g. Loi du 1er août 2018 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel en matière pénale ainsi qu’en matière de sécurité nationale);

- for entities that have not officially designated a DPO (article 37 GDPR). It should be noted that entities are free to officially designate a DPO regardless of whether they are required by the GDPR to do so or not.

3.2 GDPR - CARPA AND INTERNATIONAL STANDARDS

The GDPR-CARPA certification mechanism is the result of a proactive approach taken by the CNPD in order to provide data controllers and processors access to a flexible and highly professional certification mechanism, compliant with articles 42 and 43 of GDPR as well as the related guidance from the European Data Protection Board (EDPB).

The CNPD aims to provide a certification mechanism with the following characteristics:

- Certification must allow data controllers and processors to demonstrate a high degree of accountability – this should be underpinned by audit procedures that follow highest professional standards that do not only cover the design of controls but also their operational effectiveness over the validity period of the certificate.
- It is up to the applicant to make an initial choice of the processing operations included in the certification request submitted to the certification body. This flexibility aims to allow data controllers and processors to target those processing activities that are most relevant for them, the concerned data subjects or their professional clients – depending to whom they intend to demonstrate compliance. The target of evaluation (ToE) which comprises all processing operations to be certified has to be set up very carefully and needs to be assessed and validated by the certification body before the start of the evaluation.

The CNPD has chosen to include internationally recognized auditing and related quality control standards (see below) in its accreditation requirements in order to introduce a common method for all evaluation activities performed by the certification bodies. This allows for a coherent and consistent approach for certification activities performed by the different certification bodies, and adds value to the issued certificates.

- The assessment leading to the certification needs to be based on an assurance report that is executed according to the ISAE 3000 standard. This International Standard on Assurance Engagements (ISAE) has been developed by the International Auditing and Assurance Standards Board (IAASB)[7] and deals with assurance engagements other than audits or reviews of historical financial information. This standard is already well established in Luxembourg and allows the CNPD to leverage on best practices. In addition, an ISAE 3000 assurance report is in itself and independently of the GDPR-CARPA certification an internationally recognized

[7] The objective of the IAASB is to serve the public interest by setting high-quality auditing, assurance, and other related standards and by facilitating the convergence of international and national auditing and assurance standards, thereby enhancing the quality and consistency of practice throughout the world and strengthening public confidence in the global auditing and assurance profession (https://www.iaasb.org/about-iaasb).

report that can serve the data controller or processor in its relation with auditors or business clients.

- The certification body issuing the ISAE 3000 report needs to be subject to the International Standard on Quality Management (ISQM – former ISQC)[8], or other professional requirements, or requirements on law or regulation, regarding the firm's responsibility for its system of quality control, that are at least as demanding. This deals with a firm's responsibilities for its system and management of quality control for audits or reviews of financial statements, or other assurance or related services engagements. It applies to all firms of professional accountants in respect of audits and reviews of financial statements, and other assurance and related services engagements.

The CNPD attaches great importance to the quality of the audit procedures that underpin its certification mechanism. The CNPD has created this certification mechanism and entrusts accredited certification bodies with the certification procedure to issue the certificate (article 15 of the act of 1st August 2018 on the organisation of the National Data Protection Commission and the general data protection framework). This approach allows data controllers and processors to have access to certification independently of the availability of the CNPD's internal resources. The CNPD will ensure continuous and thorough monitoring of accredited certification bodies.

As the owner of the certification mechanism, the CNPD ensures a continuous surveillance of the adequacy of the certification criteria compared to the current state of the art in the data protection domain as well as the European and Luxembourgish legislation.

3.3 RESPONSIBILITY OF CERTIFIED ENTITIES

The GDPR states that controllers and processors can rely on certification to demonstrate their compliance in regards of certain elements of the GDPR. However, it is also stated that certification pursuant to article 42 does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities that are competent pursuant to Article 55 or 56.

3.4 IMPACT OF CERTIFICATION AND ADMINISTRATIVE FINES

In case an administrative fine is to be imposed on an entity, article 83(2)(j) obliges the CNPD to give due regard to the adherence of the entity to approved certification mechanisms. It is however to be noted that a certification can either have a mitigating or an aggravating impact. It would in particular have an aggravating impact if the entity has misused its certificate. The GDPR-CARPA certification mechanism mitigates this risk because the certificate is based on an ISAE 3000 assurance report that covers a past period. This does not eliminate all inherent risks that exist for evaluation activities, namely the risk of not detecting a nonconformity; however, those risks can be reduced as the

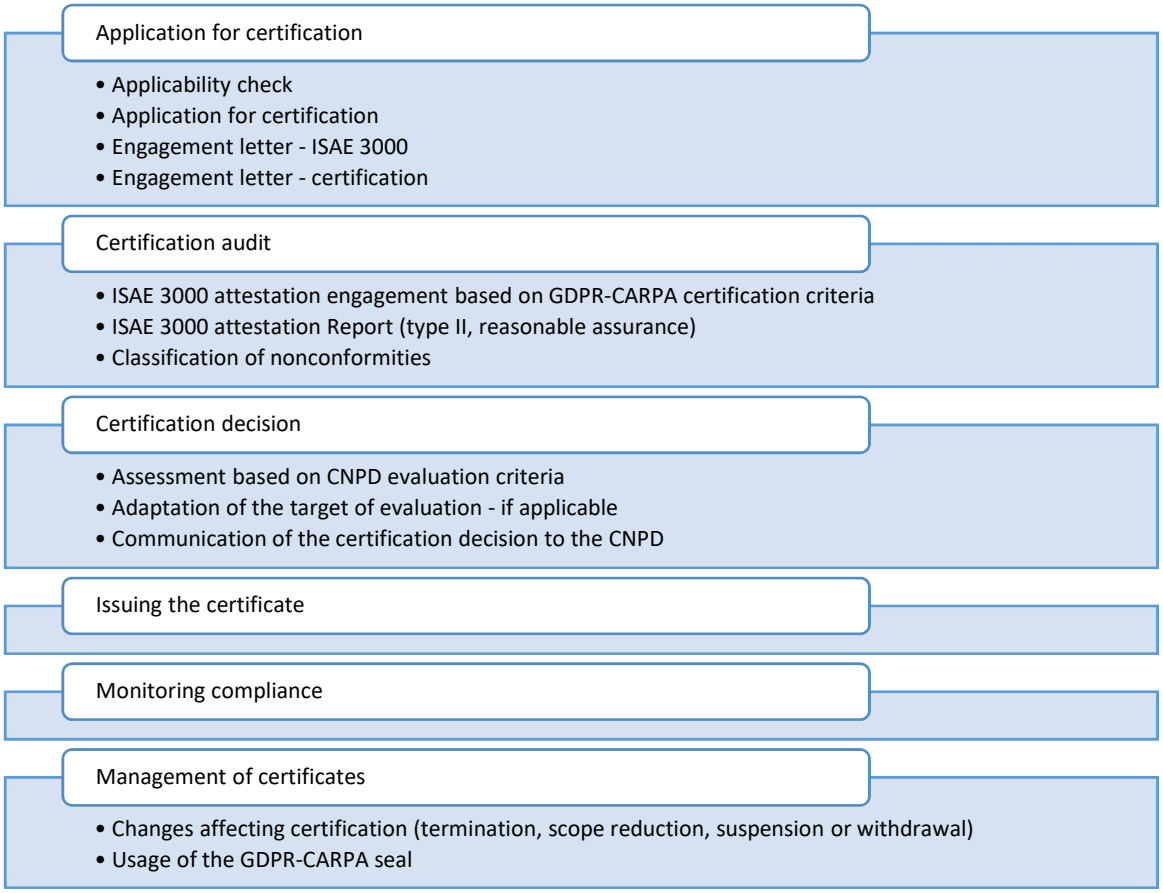
[8] International Standards on Quality Management (ISQM) – Quality Management for Firms that Perform Audits and Reviews of Financial Statements, or Other Assurance or Related Services Engagements, defined by the International Auditing and Assurance Standards Board (IAASB)

evaluation performed by the certification body is not limited to a short timeframe but covers the whole validity period of the certificate.

4 GDPR-CARPA CERTIFICATION PROCEDURE

The following diagram illustrates the different high-level steps of the certification process as established in the accreditation requirements for certification bodies[9] and the different applicable standards. Those steps are explained in more detail in the following sections.

In order to obtain more detailed information, please contact an accredited certification body (please refer to the CNPD website for a list of accredited certification bodies).



The certification procedure is guided by ISO/IEC 17065:2012[10] requirements which have been enriched with the ISAE 3000 and other relevant standards (see above) in order to form the GDPR-CARPA accreditation requirements (please refer to the CNPD's GDPR-CARPA accreditation procedure

[9] Luxembourg accreditation requirements of certification bodies (art 43(1)(a)) – Set Alpha)

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

for more information regarding the steps to follow to obtain and maintain an accreditation as a GDPR-CARPA certification body[11]).

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 pre-cited standards, the criteria used in an attestation engagement shall be suitable and available to report users. The following are attributes of suitable criteria:

- 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, the 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.

4.1 APPLICATION FOR CERTIFICATION

4.1.1 APPLICABILITY CHECK

The material and the territorial scopes as defined by the GDPR in articles 2 and 3 apply in the context of this certification mechanism.

Only processing activities involving personal data can be subject to the GDPR-CARPA certification. Furthermore, the scope and its limitations as defined in section 3.1 need to be respected.

[11] Please note: Only certification bodies that have received an accreditation by the CNPD can certify an entity's processing activities in the context of this certification mechanism. Such a certification body needs to respect the relevant accreditation requirements, which govern the way the certification body performs its work. As also noted in requirement 1.1.1.1 of these accreditation requirements, those requirements cannot be overridden by any external standard, such as ISAE 3000, ISQM or the IESBA Code.

4.1.2 MATURITY ASSESSMENT

It is highly recommended that an entity wishing to have one or more processing activity(ies) certified has familiarized itself with the relevant certification criteria upfront. Before submitting an official application for certification to an accredited certification body, the entity should perform a self-assessment to estimate if it has an adequate level of maturity with regard to the GDPR-CARPA certification criteria.

The different official guidelines published by the EDPB[12] can serve as support in order to better understand specific GDPR requirements and provide guidance with regard to the implementation of those GDPR requirements. Those guidelines can for example provide support for the design and practical implementation of organisational and technical measures but it should be noted that in the context of the GDPR-CARPA certification, entities need to strictly comply with the certification criteria in order to obtain certification.

For instance, when the terms “formal” and / or “formally” are mentioned in a criterion, a written documentation is required. For example, in the case of a required formal assessment, the entity shall perform said assessment according to the requirements laid out in the criteria and document in detail all its aspects (including also any objections raised) as well as the reached conclusion and validation of this assessment.

This self-assessment does not pre-empt any decision that a certification body will make within the certification process.

4.1.3 TARGET OF EVALUATION

Upon receipt of the application, the certification body will assess the target of evaluation (the ToE). The GDPR provides a broad scope for what can be certified, as long as the focus is to “demonstrat[e] compliance with GDPR of processing operations by controllers and processors” (Article 42(1) of the GDPR).

The target of evaluation under the GDPR-CARPA certification mechanism is a processing or a set of processing operations as defined in article 4(2) of the GDPR[13]. It is up to the entity applying for certification to propose the processing activities it intends to include in the target of evaluation. This approach adds flexibility to the mechanism as entities can start with a limited ToE and extend it over time. 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.

[12] https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

[13] Article 4(2) of the GDPR: ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

As the certification decision relies upon the ISAE 3000 assurance report, it is clear that the scope of this report must cover the whole ToE. Therefore, the certification body needs to validate the ToE chosen by the entity to ensure its meaningfulness.

It is important that the ToE of the certification remain **meaningful** and take into account all important aspects of a data processing activity, such as nature, content and risk. As an example, a target of evaluation focussing only on specific aspects of processing such as the collection of data but not on the further processing (e.g. creating advertising profiles) or the management of data subjects' rights is not meaningful for those addressed by the certification (e.g. the data subject).

A **clear and transparent** ToE description needs to include as much details as possible. Criterion I-0 'Target of Evaluation' of the certification criteria (please refer to section 5) needs to be complied with when defining the ToE. Further to this, it is useful to take into account the following four levels of factors / components when defining and describing a ToE:

1. The circumstances / context / nature of the controller or processor (public / private sector, etc.) influencing its activities and governance (e.g. financial sector with its specific legal ecosystem, etc.);
2. The function the processing activity performs within the entity and the people / functions / departments involved (e.g. HR department carrying out the recruitment process involving different functions, etc.);
3. The functional application(s) that is / are used to implement the purpose (e.g. SAP-HR, etc.);
4. The IT infrastructure, any filing systems and the functions they provide. This includes operating systems, virtual systems, databases, authentication and authorisation systems, routers and firewalls, storage systems such as SAN or NAS, an entity's communication infrastructure or Internet access, as well as the technical measures which must be implemented (e.g. Windows server farm, Oracle DB, etc.).

4.1.4 CERTIFICATION AGREEMENT

By signing the certification agreement with the certification body, the applying entity commits to comply with the requirements set out by this certification mechanism[14].

4.2 CERTIFICATION AUDIT

4.2.1 APPLICABILITY OF GDPR-CARPA CERTIFICATION CRITERIA

The GDPR-CARPA certification criteria are structured in three sections, which are described more in detail in section 5.1 of this document:

- Section I on accountability and governance applies to all entities, controllers and processors.

[14] Please refer to the accreditation requirements for GDPR-CARPA certification bodies for more information.

- Section II contains criteria on principles related to processors of personal data and applies only to controllers.
- Section III contains criteria on principles related to processors of personal data and applies only to processors.

An entity needs to comply with all criteria of the sections that are applicable to its status as a controller or processor.

The certification body must report on all GDPR-CARPA certification criteria. 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.

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 / criteria during the engagement. However, the certification body needs to document in detail every (partial) exclusion of a criterion and the reasons for doing so in the assurance report.

4.2.2 ISAE 3000 ASSURANCE REPORT

The certification body will perform an ISAE 3000 attestation engagement based on the GDPR-CARPA certification criteria listed in this document. The resulting ISAE 3000 type 2 assurance report constitutes the basis for the certification decision. A type 2 engagement provides assurance over

- the fairness of the presentation of the description of the entity's system, and
- the suitability of design, implementation and operating effectiveness of the controls throughout a period.

A type 1 engagement provides assurance over the fairness of the presentation of the description of the service entity's system and the suitability of design and implementation of the controls as at a specific date but it does not provide assurance over the operating effectiveness of the controls throughout a period, as a type 2 engagement would. Type 1 reports might be used in a preparatory phase but they cannot effectively support a certificate.

The ISAE 3000 assurance report on which the certification decision is based must provide "reasonable assurance" (as opposed to "limited assurance").

4.2.3 EVALUATION ACTIVITIES

The GDPR-CARPA certification criteria contain the rules to be followed by the entities applying for the certification. Those entities need to ensure that their internal measures be designed, implemented and operated in a way that allows them to comply with the requirements set out in these certification criteria. During the certification audit, the certification body 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 evaluates if the organisational or technical measure is designed to allow for effective compliance to the certification criteria by consulting among others available documentation (procedures, etc.).
- Operating effectiveness: After having reviewed the design and implementation of a measure, the auditor will test its operating effectiveness by checking if it works in practice as designed, 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 as indicated in section 4.2.1.

4.2.4 CATEGORIZATION OF NONCONFORMITIES

Any identified nonconformities falling within the scope of the certification shall be classified according to the following rules:

Major nonconformities: Nonconformities are classified as major when one of the following elements applies:

- Certification criteria are not implemented (e.g. systematic nonconformity linked to the processing operation as defined under article 30 of the GDPR, inexistent procedure for determining the lawfulness of a processing, etc.);
- Systematic problem at governance level (e.g. missing or incomplete policies / procedures, no systematic involvement of adequate / competent staff for data protection control activities that need to be executed by the controller / processor, several minor nonconformities that are related to a same process / domain indicating that there is a more serious underlying governance issue, etc.);
- A nonconformity that could have a major impact on data subjects' fundamental rights and freedoms;
- Nonconformities that have been identified during a previous audit and that have not been resolved within the set deadline.

Minor nonconformities: Nonconformities are classified as minor when one of the following elements applies:

- Isolated exception that has no impact on the rights and freedoms of the concerned data subjects (e.g. an isolated exception in the execution of a procedure, etc.);
- Policies and / or procedures are insufficiently formalized but the relevant criteria are met in practice underpinned by sufficient evidence (except when the procedure for determining the lawfulness of a processing activity is missing or weak) – there should be sufficient and conclusive evidence that criteria are indeed met in practice.

The certification body informs the applicant of all identified nonconformities.

4.3 CERTIFICATION DECISION

The certification decision is based on the evaluation activities documented in the ISAE 3000 assurance report. Depending on the nonconformity and the affected certification criteria different rules apply.

Section I of the certification criteria on the accountability and governance[15]: The following rules apply:

- A major nonconformity is cause to reject certification (see above).
- A high number of minor nonconformities (also taking into account minor nonconformities of the criteria in section II or III of the certification criteria) that indicate that there is a wider governance problem is cause to reject certification.
- A nonconformity posing a high risk to the fundamental rights and freedoms of data subjects is cause to reject certification.

Sections II and III of the certification criteria regarding the principles relating to processing of personal data by controllers and processors respectively[16]: For each processing activity in the ToE, the certification body needs to evaluate the impact of minor / major nonconformities on the certification decision.

- A major nonconformity for a specific processing activity leads to the exclusion of this processing activity from the certification scope (the certification can still be granted for the other processing activities in the ToE provided there is no further cause for rejection).
- If a minor nonconformity for a specific processing activity is identified, the certification body has to assess the impact on the fundamental rights and freedoms of the data subjects potentially caused by the identified nonconformity:
    - If there is a risk of an impact on the fundamental rights and freedoms of data subjects, the processing activity in question has to be excluded from the ToE of certification;
    - If there is no risk of an impact on the fundamental rights and freedoms of data subjects, the processing activity can remain in the ToE of certification.

The certification body can thus not give a positive certification decision for a specific target of evaluation if there are any open major nonconformities relevant to that target of evaluation. The certification body will issue an instruction to solve / mitigate any minor nonconformities that might still be open when the certificate is issued within a suitable period of time.

In case of a certification status change, the certification body will communicate its certification decision and relevant supporting documentation to the CNPD according to the accreditation requirements. This documentation contains among others for each identified nonconformity the reasoning behind its classification into either minor or major.

[15] Please refer to section **Error! Reference source not found.** of this document containing the **Error! Reference source not found.**.

[16] Please refer to section **Error! Reference source not found.** of this document containing the **Error! Reference source not found.**.

4.4 ISSUING THE CERTIFICATE

The certification body will provide formal certification documentation that conveys, or permits identification of the following:

- the name and address of the certification body;
- the name and address of the entity applying for certification;
- the name of the certification mechanism used for the certification (here GDPR-CARPA), including the version of the certification criteria;
- the GDPR-CARPA logo and the related rules of use;
- the description of the target of evaluation including all certified processing operations – This description needs to be as clear and detailed as possible to be easily understood by all stakeholders, including data subjects. It shall also indicate for each processing operation the entity's role (processor or controller);
- the date certification is granted (starting the first day following the period under review);
- the period of validity of the certification (including start and expiration date);
- the unique certification ID provided by the CNPD;
- a mention of the possibility to access the certification decision documentation on request;
- the reference to the accreditation that the certification body holds.

The issued certificate is valid during 3 years provided all conditions are met (please refer to section 4.5).

The certification body maintains a public register containing the information listed above as well as the status of the certificate (e.g. active, expired, withdrawn).

4.5 MONITORING COMPLIANCE

By default, the validity of a GDPR-CARPA certificate is as long as the period covered by the ISAE 3000 assurance report (usually 1 year). If the validity of the certificate is intended to be longer than one year, a new ISAE assurance evaluation is required for each period.

In the context of the GDPR-CARPA certification mechanism, the ISAE 3000 assurance engagement must cover a period of at least 6 months and at most 12 months. The certificate is valid for a period that corresponds to the period covered by the ISAE 3000 assurance engagement. This means that a certificate based on an engagement covering 12 months (in the past) is valid for 12 months (in the future) starting on the first day following the period covered by the report.

The validity of a certificate can be extended to a period of maximum 3 years. In this case a new audit covering the whole scope will be performed at each ISAE engagement anniversary. The rules concerning the period covered by the audit as well as the validity period set out above continue to apply.

Example:

- Total validity period of the certificate: 3 years (year 1 – year Y3)
- Period covered by each ISAE 3000 assurance engagement: 12 months
- Target of evaluation remains unchanged

Period	Activities during that period and their result
Year 0	From 01/01/Y0 to 31/12/Y0, processing activities in the ToE exist and measures are in place in compliance with the GDPR-CARPA certification criteria.
Year 1	The ISAE 3000 assurance report covers year 0 (01/01/Y0 – 31/12/Y0). In case of a positive certification decision, the certification body issues a certificate for year 1 with a certificate validity from 01/01/Y1 to 31/12/Y1.
Year 2	The ISAE 3000 assurance report covers year 1 (01/01/Y1 – 31/12/Y1). In case the certification decision remains positive, the certificate remains valid for year 2.
Year 3	The ISAE 3000 assurance report covers year 2 (01/01/Y2 – 31/12/Y2). In case the certification decision remains positive, the certificate remains valid for year 3. The entity can continue to use its certificate for the third and final year.

As seen above, the ISAE 3000 assurance report covers a past period. In order for the entity to receive a positive certification decision, it needs to ensure that it was compliant to the GDPR-CARPA certification criteria during this entire past period.

The certificate validity depends on the conclusions of each new ISAE 3000 assurance engagement report. Depending on the outcome of the assessment based on the GDPR-CARPA certification criteria, the certification body needs to decide whether the certificate remains valid, withdrawn or whether the ToE needs to be reduced.

Should the entity decide to continue the certification after the validity period of 3 years, it can do so. In this case, CNPD will issue a new certificate upon notification of a new positive certification decision by the certification body.

Please refer to 'Annex 1 – Certification validity' for more details.

4.6 MANAGEMENT OF CERTIFICATES

4.6.1 CHANGES AFFECTING CERTIFICATION

Changes affecting GDPR-CARPA certification can originate from two sources:

- Changes initiated by the CNPD: The CNPD will publish any changes to the certification mechanism and will communicate to the certification bodies the conditions under which those changes shall be implemented including a transition phase at the end of which the

implementation needs to be finalized. In case those changes affect as well a certification body's clients, the certification body will then contact its clients in order to elaborate a corresponding action plan to ensure future compliance with the certification mechanism.

- Changes initiated by other factors: The certification body shall consider other changes affecting certification, including changes initiated by the certification body's client, and shall decide upon the appropriate action. In case the entity implements any changes affecting one or more certification criteria or processing activities in the target of evaluation, it shall inform the certification body without undue delay.

If a nonconformity with certification criteria is substantiated, either as a result of an audit or otherwise, the certification body shall consider and decide upon the appropriate action, which can include:

- Continuation of certification under conditions specified by the certification body and approved by the CNPD (e.g. increased monitoring);
- Reduction of the ToE by removing nonconforming processing activities (in this case, a new certificate ID will be issued by the CNPD, but the validity period of the original certificate remains applicable);
- Withdrawal of certification.

The decisions to reduce or to withdraw a certification are based on the rules set out in this document, and more specifically in section 4.3 'Certification decision'.

The certification body shall inform the CNPD of its decisions to change an entity's certification status or ToE and provide all relevant documentation to the CNPD for review.

In case of a change in the certification status and / or ToE, the certification body as well as its client shall make all necessary modifications to formal documents, public information, authorizations for use of marks, etc. in order to ensure that this status change is clearly specified. Furthermore, this change needs to be communicated to all relevant stakeholders.

4.6.2 USAGE OF THE GDPR-CARPA SEAL

The GDPR-CARPA certificates, seals or marks shall be used in a clear and transparent manner preventing any confusion or misleading communication about the scope of the certified processing activities. Incorrect references to the certification mechanism, or misleading use of certificates, seals or marks, or any other mechanism for indicating a processing activity is certified, found in documentation or other publicity, is subject to suitable action by the certification body, such as:

- Taking any action to stop the misleading / wrong communication and thus removing the visibility of the data protection certificate, mark and seal;
- Informing the public about the misuse;
- Immediately informing the Data Protection Supervisory Authority about the misuse;
- Suspension of the authorization to use the data protection certificate, mark and seal for the process in question.

The type of corrective action to be taken will be influenced by the nature of the misuse and its subsequent consequences.

The notification to the misuser by the certification body is always confirmed in writing by registered letter (or equivalent) with a copy sent to the CNPD. This notification contains:

- the reason(s) for corrective action,
- the action(s) to be taken by the misuser to resolve the issue, and
- a request for a statement from the misuser formalizing his engagement to perform the action(s) to be taken to ensure that the data protection certificate, mark or seal is not applied to any ineligible processes.

When the data protection certificate, mark and seal has not been used in compliance with established rules of use, legal proceedings might result in a court of law deciding what the corrective action will be.

Please refer to the dedicated document under the certification section on the CNPD website for more detailed information about the rules of usage of the registered and protected GDPR-CARPA seal.

5 GDPR-CARPA CERTIFICATION CRITERIA

5.1 ORGANISATION OF THE CERTIFICATION 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.

Depending on the area (e.g. health sector) and the target of evaluation (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[17]:

- 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.

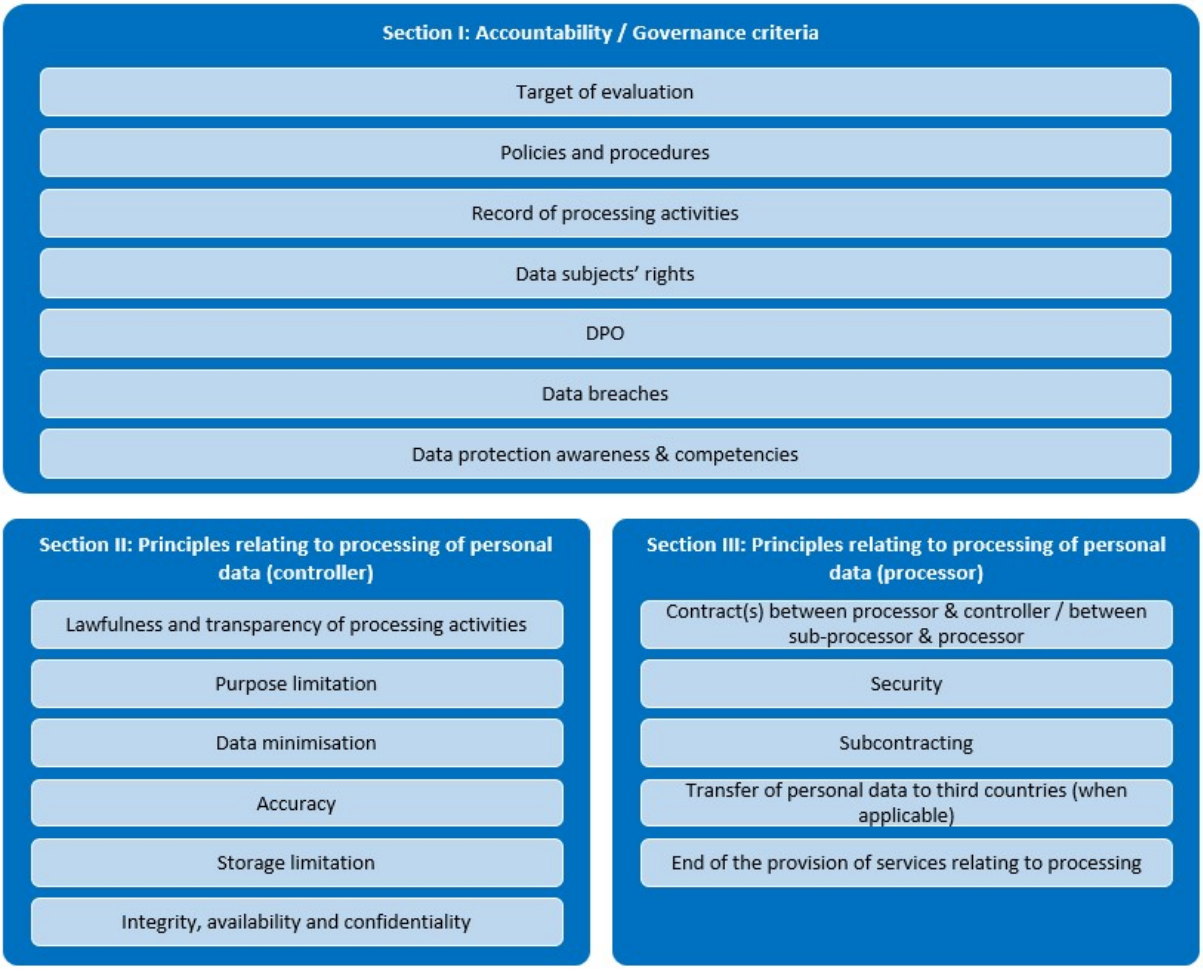
Taking the above into account, the structure of the GDPR-CARPA certification criteria for controllers has been aligned to the "Principles relating to processing of personal data" as defined under article 5 of the GDPR, and complemented by the other requirements as set out above (please refer to 'Annex 2 – Mapping of GDPR-CARPA certification criteria' for more details).

The certification criteria in this document have been adopted by the CNPD on 13th of May 2022[18] and officially constitute the first version of the GDPR-CARPA criteria.

[17] Please refer i.a. to paragraph 48 of the guidelines 1/2018 on certification and identifying certification criteria in accordance with articles 42 and 43 of the regulation (Version 3.0, 4th of June 2019)

[18] Décision N° 15/2022 du 13 mai 2022 de la Commission nationale pour la protection des données portant exécution de l'article 15 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données

The GDPR-CARPA certification criteria are organised in three sections:



Section I: Accountability Criteria

This section contains the criteria relevant to the way 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 the ToE, 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 the ToE, where it acts as data processor.

5.2 TABLE OF CONTENTS

Subsection II – d: Accuracy		II-d-1	63	Reliability of the data source
		II-d-2	63	Accuracy of data
		II-d-3	63	Right to rectification
Subsection II – e: Storage limitation		II-e-1	65	Defined retention period
		II-e-2	65	Deletion or anonymization of data
		II-e-3	65	Right to erasure ('right to be forgotten')
Subsection II – f: Integrity, availability and confidentiality	Security	II-f-1	68	Risk analysis
		II-f-2	69	Risk treatment
		II-f-3	70	Documented implementation of organisational and technical measures
		II-f-4	71	Audit
		II-f-5	71	Follow-up on audits
	Data protection impact assessment (DPIA)	II-f-6	71	DPIA
		II-f-7	72	DPIA - Prior consultation
	Outsourcing	II-f-8	72	Assessment of sufficiency
		II-f-9	73	Contract / legal act under Union or Member State law
		II-f-10	73	Policies and procedures (outsourcing relationship)
		II-f-11	74	Monitoring

Overview of Section III: Principles relating to processing of personal data (processor)			
Subject	Ref.	Page	Title
Contracts between processor and controller / between sub-processor and processor	III-1	75	Contract / legal act under Union or Member State law
	III-2	76	Policies and procedures (outsourcing relationship)
	III-3	76	Limitation of processing to documented instructions
	III-4	77	Processing without instructions
Security	III-5	77	Risk analysis
	III-6	78	Risk treatment
	III-7	80	Documented implementation of organisational and technical measures
	III-8	80	Audit
	III-9	80	Follow-up on audits
Subcontracting	III-10	81	Assessment of sufficiency
	III-11	81	Subcontracting
Transfer of personal data to third countries (when applicable)	III-12	81	Third countries
End of the provision of services relating to processing	III-13	83	Return / deletion of data

5.3 CERTIFICATION CRITERIA

SECTION I: ACCOUNTABILITY CRITERIA / GOVERNANCE CRITERIA

C = applies to controller / P = applies to processor

Ref.	Label	Description	C	P
		Target of Evaluation		
I-0	Definition of the target of evaluation	The entity shall define the target of evaluation including all processing activities in scope of this certification. 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 any manual steps, transformation(s) and manipulation(s) of data, physical printouts, location(s) of the task performed, and the position(s) / function(s), department(s) 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 documented 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.	X	X
		Policies and procedures		
I-1	Accountability (GDPR Article 24) (Recitals 74, 75, 76, 77, 84)	The entity has implemented organisational measures that ensure management is informed of, involved in and accountable of personal data processing activities. Measures include at least: • the design of 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-6, II-f-7); • data transfers, if applicable (II-a-18, III-12); • use and management of processors, if applicable (II-f-8 to II-f-11); • 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 (i.a. I-14 & I-15). The entity has taken into account the formal opinion of its DPO on those policies and procedures. The entity's management has formally validated those policies and procedures and communicated them to its personnel. 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.	X	X
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 documented 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. Then the management communicates the updated policies and procedures to its personnel including a mention of what has changed.	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 for the processing; • a description of the categories of data subjects and of the categories of personal data; • 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.	X	
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 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 documented 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. 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).	X	
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 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 documented 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)	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.	X	

	(Recitals 58, 59)	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: • 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: o 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. o 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?"); o 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.		X

		• 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. • 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 at all, 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: o 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. ▪ The DPO has 2 years of data protection / data security-related experience (e.g. IT security, etc.) and has followed comprehensive trainings on data protection. In any case, the DPO shall have free and easy access to legal assistance internally, or via a non-limiting service contract with an external firm covering all GDPR subjects when deemed necessary by the DPO. o The DPO has a good understanding of the processing activities carried out by the entity, as well as the corresponding information systems through:	X	X

		▪ 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); ▪ 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). o 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: o 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.). o 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. o 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 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	X	X

		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. • ensure that the DPO is bound by secrecy or confidentiality concerning the performance of his / her tasks, in accordance with Union or Luxembourgish law; • ensure that the DPO is not involved in tasks and duties that could result in a conflict of interests: o 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. o 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. o 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. Furthermore, the entity has formally established a procedure on how to resolve a conflict of interest. Note: Even if the DPO has a significant role for the compliance monitoring of the entity's processing activities according to Article 39 of the GDPR, he / she is not the one responsible to assess the implementation of the measures designed to ensure such compliance. The entity remains responsible for the measures it implements and the way those measures are implemented.		
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 provisions in Union or Luxembourgish data protection law (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 Luxembourgish 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: o the necessity to carry out a data protection impact assessment (DPIA); o the method to be followed when carrying out a DPIA; o the decision to perform the DPIA internally or to subcontract it;	X	X

		○ the measures (including technical and organizational measures) to be implemented to mitigate any risks to the rights and interests of the data subjects; ○ whether the DPIA has been correctly carried out in compliance with the GDPR and the present certification criteria. 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, its assessment and handling including the communication to the supervisory data protection authority and / or the data subjects, if applicable. A formal procedure validated by the DPO shall define at what point in time the DPO needs to be informed and what this information shall include; • 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 documented method 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 data subjects caused by a data breach. This assessment shall take into account at least the following factors: ○ the context, nature, scope and purposes of the processing activity, including also elements such as the type / nature of data breached, the volume of data (potentially) concerned by the breach, etc.; ○ the context and nature of the entity (e.g. sector, market, etc.); ○ the ease of identification of any concerned or potentially concerned data subject as well as any potential impact of the data breach to the rights and freedoms of any concerned or potentially concerned person; ○ the circumstances of the breach (e.g. malicious / non-malicious intent, concerns about confidentiality / integrity / availability / resilience of data, etc.); • 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 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	X	

		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: ○ a description of the nature of the personal data breach; ○ the name and contact details of the data protection officer or other contact point where more information can be obtained; ○ a description of the likely consequences of the personal data breach; and ○ 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 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 and without undue delay after becoming aware of a personal data breach, should the controller identify a risk to the rights and freedoms of data subjects 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, its assessment and handling including the communication to the supervisory data protection authority and / or the data subjects, if applicable. A formal procedure validated by the DPO shall define at what point in time the DPO needs to be informed and what this information shall include; • 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 documented method (validated by the contractual partner/controller) to assess whether an event qualifies as a personal data breach. This assessment shall take into account at least the following factors (in so far as the entity disposes of this information as per its contract with the contractual partner / controller): ○ the context, nature, scope and purposes of the processing activity, including also elements such as the type / nature of data breached, the volume of data (potentially) concerned by the breach, etc.; ○ the context and nature of the controller as well as the entity (e.g. sector, market, etc.);		X

		○ the ease of identification of any concerned or potentially concerned data subject as well as any potential impact of the data breach to the rights and freedoms of any concerned or potentially concerned person; ○ the circumstances of the breach (e.g. malicious / non-malicious intent, concerns about confidentiality / integrity / availability / resilience of data, etc.); • 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.		
Data protection awareness & competencies				
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 (I-0), the risk analysis (II-f-1) as well as the risk treatment plan (II-f-2) as well as defined policies and procedures. 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. Furthermore, the entity shall inform its internal / external personnel of any change in its data protection governance, including among others data protection relevant changes in policies and procedures, changes in roles / responsibilities (DPO, CISO, etc.) and reporting lines, etc. as soon as possible. The entity has formally established in what situations such a communication is necessary and when, how and to whom it will communicate should those situations arise. Finally, the entity has a written agreement with its internal / external personnel according to which personnel commits itself to respect data protection obligations.	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 (I-0), the risk analysis (III-5) as well as the risk treatment plan (III-6) as well as defined policies and procedures. 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. Furthermore, the entity shall inform its internal / external personnel of any change in its data protection governance, including among others data protection relevant changes in policies and procedures, changes in roles / responsibilities (DPO, CISO, etc.) and reporting lines, etc. as soon as possible. The entity has formally established in what situations such a communication is necessary and when, how and to whom it will communicate should those situations arise. Finally, the entity has a written agreement with its internal / external personnel according to which personnel commits itself to respect data protection obligations.		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 formally validated for each processing activity in scope. The entity has assessed the validity of the identified legal basis in detail. This assessment shall be documented and shall take into account: • the necessity of the processing activity in relation to the purpose(s) pursued according to articles 6.1(b) to (f) of the GDPR; • the nature, context, scope and purposes of the processing activity. The assessment of the applicable legal basis shall also include: • an analysis of any processing limitations defined by law and their applicability to the processing activity in scope; • an analysis of any conditions defined by law, under which the processing activity can be performed and their applicability to the processing activity in scope (this can include specific safeguards, certain types of personal data, specific circumstances, etc.); • an analysis of any additional organisational and / or technical measures required by law to be implemented by the entity (e.g. measures indicated in articles 85 to 89 of the GDPR). In case the law requires the implementation of such additional measures and / or processing limitations, the entity shall define, implement and control them according to the requirements set out in the criteria on Security (Subsection II – f: Integrity, availability and confidentiality). 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 documented 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 method 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.

Ref.	Label	Description

II-a-3	Processing based on consent
	
	(GDPR Article 4, 7, 8)
	
	(Recitals 32, 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 all of the following conditions for a valid consent are respected.
		
		Valid consent is :
		
		• freely given: The data subject needs to have a genuine choice and be able to refuse or withdraw consent without detriment. It is very unlikely that a consent be freely given
		  ○ 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.
		  In case the entity choses nevertheless to use consent as a legal basis in this kind of situation, it shall be able to prove that data subjects have a genuine choice with regard to accepting or declining the terms offered or declining them without detriment.
		• 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: the entity shall provide the data subject at least with the following information:
		  ○ the identity of the controller;
		  ○ the purpose of each of the processing activities for which consent is sought;
		  ○ the (type of) data that will be collected and used;
		  ○ the existence of the right to withdraw consent;
		  ○ information about the use of the data for automated decision-making in accordance with article 22.2(c) where relevant;
		  ○ information on the possible risks of data transfers due to an absence of an adequacy decision and of appropriate safeguards as described in article 46.
		• an unambiguous indication of wishes: Consent requires a statement from the data subject or a clear affirmative act (i.e. an active motion or declaration). The entity shall collect explicit consent (i.e. an express statement of consent):
		  ○ when processing special categories of data;
		  ○ in the context of data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49;
		  ○ in the context of automated individual decision-making, including profiling (article 22).
		
		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.

Ref.	Label	Description
		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 formally: • identified the applicable legal obligation; • assessed the applicability of this legal obligation with regard to the processing activity in scope.
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. *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 applicability of the Union law or Luxembourgish 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 has formally identified and described its legitimate interest in this processing activity. • The entity implemented a documented method 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).

Ref.	Label	Description
		Note: The legislator provides by law for the legal basis for public authorities to process personal data. Consequently, this legal basis shall 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 (criteria II-a-1 and II-a-2) and additional measures to safeguard the rights and freedoms of data subjects stipulated by law have been assessed and implemented (criteria II-a-1 and criteria on Security in Subsection II – f: Integrity, availability and confidentiality), in particular regarding article 9.4 of the GDPR regarding further conditions / limitations defined by law regarding the processing of genetic data, biometric data or data concerning health. 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: o 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 identified the applicable legal obligation and formally assessed the applicability of this legal obligation with regard to the processing activity in scope. o The entity has implemented measures allowing data subjects to give their explicit consent. • Controller's obligations / specific rights in the field of employment, social security, social protection law (Article 9(2)(b)): The entity has identified the applicable legal basis and formally assessed its applicability with regard to this processing activity. Based on the identified Union or Luxembourgish law or collective agreement pursuant to Luxembourgish law, the entity has ensured that safeguards are in place in order to respect the fundamental rights and interests of data subjects as also required by criterion II-a-1. • 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. *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.* • 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.

Ref.	Label	Description
		○ The entity has ensured that safeguards are in place in order to respect the fundamental rights and interests of data subjects as also required by criterion II-a-1. • 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 Luxembourgish law(s), which constitute(s) the basis for the processing of sensitive data. Furthermore, the entity has ensured that safeguards are in place in order to respect the fundamental rights and interests of data subjects as also required by criterion II-a-1. • 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)): ○ The entity has formally assessed whether it fulfils the conditions with regard to the purpose as required in Article 9(2)(h). ○ If the processing is based on Union or Luxembourgish law, the entity has formally identified the law(s) in question. ○ If the processing is based on a contract with a health professional, the entity has formally documented this. ○ 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 Luxembourgish law or rules established by national competent bodies) or subject to an obligation of secrecy (under Union or Luxembourgish law or rules established by national competent bodies). The entity has included the relevant law(s) or rule(s) in its documentation and has ensured that safeguards are in place in order to respect the fundamental rights and interests of data subjects as also required by criterion II-a-1. • 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 entity has identified the Union or Luxembourgish law(s), which constitute(s) the legal basis for the processing of sensitive data in scope. Based on the identified law(s), the entity has ensured that safeguards are in place in order to respect the fundamental rights and interests of data subjects, in particular professional secrecy, as also required by criterion II-a-1. • 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 Luxembourgish law(s), which constitute(s) the legal basis for the processing of sensitive data in scope. Furthermore and pursuant to article 89 of the GDPR, the entity has analysed the applicability of any derogations and has ensured that safeguards are in place in order to respect the fundamental rights and interests of data subjects as also required by criterion II-a-1.
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

Ref.	Label	Description
		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. 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;

Ref.	Label	Description
		• 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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.

II-a-11	Right to restriction of processing
	
	(GDPR 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;
		• 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:
		  ○ with the data subject's consent;
		  ○ for the establishment, exercise or defence of legal claims;
		  ○ for the protection of the rights of another natural or legal person;
		  ○ for reasons of important public interest of the Union or of a Member State (Luxembourg).
		  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 a complete inventory of recipients to whom the personal data have been disclosed. The entity has taken into account the formal opinion of its DPO regarding the completeness and accuracy of this inventory and the entity's management has formally validated this inventory. A formal review of the completeness and accuracy of this inventory is performed at least on an annual basis or when significant changes in the data privacy landscape of the entity occur. The entity takes into account the formal opinion of its DPO the review outcome is

Ref.	Label	Description
		validated by the entity's management. The entity shall communicate any restriction of processing to each recipient to whom the personal data have been disclosed. For this, the entity shall have defined and implemented measures to effectively communicate this restriction of processing to all relevant recipients. 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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.
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, including profiling, 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 authorised 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.

Ref.	Label	Description
		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. In case the automated decision-making, including profiling, is authorised 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 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. Measures mentioned in this criteria 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). 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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.
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;

Ref.	Label	Description
		• 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; • 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. Furthermore, the entity shall document the date and time of the information provision / publication as well as the content of the information.

Ref.	Label	Description
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. 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;

Ref.	Label	Description
		• 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: o proves impossible: This is the case when it is not possible for the entity to contact the concerned data subjects because it has no access to contact details of those data subjects (e.g. due to contractual agreements, etc.). In this case, the entity needs to be able to prove that it does not have access to those contact details. 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. o 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. The assessment in this situation shall take into account financial, human resource and other material factors as well as elements as the minimum time necessary to identity concerned data subjects, the means to contact concerned data subjects, etc. o 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. • Obtainment or disclosure of personal data is expressly laid down by Union or Luxembourgish 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 Luxembourgish law, including a statutory obligation of secrecy. The entity shall include in its assessment the law

Ref.	Label	Description
		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 documented method 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. The entity shall provide confirmation as to whether or not personal data concerning the data subject are being processed, and, where that is the case, access to the personal data and the following information: • the purposes of the processing; • the categories of personal data concerned; • the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; • where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; • the existence of the right to request from the entity rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; • the right to lodge a complaint with a supervisory authority; • where the personal data are not collected from the data subject, any available information as to their source; • the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) 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. 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.

Ref.	Label	Description
		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. The entity has implemented measures to ensure that when the data subject makes the request by electronic means, and unless otherwise requested, the information be provided in a commonly used electronic form. 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 upon the first request for access by the data subject. In case the entity charges a fee for providing the requested information anew after a first access request by the data subject, 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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.
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. The entity has formally assessed whether the requesting data subject's right does not adversely affect the rights and freedoms of others (e.g. the inclusion of personal data of other data subjects in the data to be provided might prevent other data subjects from exercising their rights, etc.). The assessment shall take into account at least the context and the purpose of the processing activity, the nature of the data and the intended recipient of the data (the requesting data subject or another controller) as well as the possible uses the recipient can make of the data. This assessment shall also establish if and how the entity can avoid adversely affecting the rights and freedoms of others (e.g. anonymising / deletion only of the data of other data subjects) when complying with the request of the data subject. In case the entity arrives to the conclusion that the effort involved to safeguard the rights and freedoms of others is disproportionate to the compliance with the request of the data subject, it shall communicate the reasons for not complying to the data subject's request according to the procedure outlined in criterion I-8. The assessment in this situation shall take into account at least financial, human resource and other material factors as well as the number of other data subjects (potentially) concerned. In addition to the measures outlined in I-8 the entity has formally assessed:

Ref.	Label	Description
		• 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; • 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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.
Transfer of personal data to third countries (when applicable)		
II-a-18	Third country transfers (GDPR Article 44 to 46) (Recitals 101 to 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 assessment shall include an analysis of all possible available transfer mechanisms and their suitability with regard to the processing activity in scope respecting the provisions of chapter V of the GDPR. During this assessment, at least the following factors need to be considered: • Taking into account the nature, scope, context and purpose of the processing activity in scope, the entity shall assess which of those mechanisms is best suited to protect the rights and freedoms of the data subjects whose data is concerned by a transfer (e.g. specific safeguards, level of protection of personal data, ease of the exercise of data subjects' rights, etc.); • The entity shall assess what the risks of using each of those mechanisms are and how they can be avoided / mitigated (e.g. mitigation of risks in case there are

Ref.	Label	Description
		any provisions in the law of the country of the data importer that might reduce the effectiveness of the organisational / technical measures to protect personal data transferred, etc.); • The entity shall take into account CJEU judgments regarding the topic of transfers and mechanisms as well as EDPB guidelines when analysing those mechanisms. 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 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 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 documented 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 method 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 documented 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 method 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. This assessment shall take into account: • whether Union or Luxembourgish law determines and specifies the tasks and purposes for which the further processing should be regarded as compatible and lawful (e.g. where 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 entity); • whether further processing is performed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and whether this can be considered to be a compatible lawful processing activity. Furthermore, in order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the entity, after having met all the requirements for the lawfulness of the original processing, shall for this assessment also take into account at least the following: • any link between those purposes and the purposes of the intended further processing; • the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;

		• the nature of the personal data; • the consequences of the intended further processing for data subjects; and • the existence of appropriate safeguards in both the original and intended further processing operations (please refer to criteria in the Security part in Subsection II – f: Integrity, availability and confidentiality). 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 documented 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 method 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 taking into account the amount, type and nature of the data collected and 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) by considering among others to collect less personal data, avoid the collection of special categories of data if possible, reduce the number of data subjects concerned, shorten retention periods, use a more adapted technology, avoid data transfers to third parties / countries, etc.; • 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 documented 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) by considering among others to collect less personal data, avoid the collection of special categories of data if possible, reduce the number of data subjects concerned, shorten retention periods, use a more adapted technology, avoid data transfers to third parties / countries, etc. 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 documented 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 documented 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 documented 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 / holds, 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, correct and / or deletes 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 a complete inventory of recipients to whom the personal data have been disclosed. The entity has taken into account the formal opinion of its DPO regarding the completeness and accuracy of this inventory and the entity's management has formally validated this inventory. A formal review of the completeness and accuracy of this inventory is performed

		at least on an annual basis or when significant changes in the data privacy landscape of the entity occur. The entity takes into account the formal opinion of its DPO the review outcome is validated by the entity's management. The entity shall communicate any rectification of personal data to each recipient to whom the personal data have been disclosed. For this, the entity shall have defined and implemented measures to effectively communicate this rectification to all relevant recipients. 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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.

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. In case the entity could not identify an applicable legal requirement governing data retention periods, the entity shall define maximum retention periods for the concerned data after having performed an assessment that shall take into account at least factors such as the nature, context, scope and purpose of the processing activity, the maximum time period the data is needed to perform the processing activity, sector-specific best practices, etc. 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 documented 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 the conditions for the right to erasure are met (please refer to II-e-3); or • when article 58.2(g) applies. 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 I-0, 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.
II-e-3	Right to erasure ('right to be forgotten') (GDPR Articles 12, 17 and 19)	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).

Ref.	Label	Description
	(Recitals 65, 66, 156)	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 Luxembourgish 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: o for exercising the right of freedom of expression and information; o for compliance with a legal obligation which requires processing by Union or Luxembourgish 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; o 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); o 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 o 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. • 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 a complete inventory of recipients to whom the personal data have been disclosed. The entity has taken into account the formal opinion of its DPO regarding the completeness and accuracy of this inventory and the entity's management has formally validated this inventory. A formal review of the completeness and accuracy of this inventory is performed at least on an annual basis or when significant changes in the data privacy landscape of the entity occur. The entity takes into account the formal opinion of its DPO the review outcome is validated by the entity's management. The entity shall communicate any erasure of personal data to each recipient to whom the personal data have been disclosed. For this, the entity shall have defined and implemented measures to effectively communicate this erasure of personal data to all relevant recipients. The entity formally assesses how it informs these controllers, taking account of available technology and the cost of implementation.

Ref.	Label	Description
		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 with regard to the administrative cost of providing the communication or taking the action requested by the data subject.

SUBSECTION II – F: INTEGRITY, AVAILABILITY AND CONFIDENTIALITY

Ref.	Label	Description
		Security

II-f-1	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). The entity pays particular attention to special categories of data when performing its risk analysis.
		
		This formal assessment includes an analysis of the potential impact(s) and probability of each identified risk to the rights and freedoms of the data subjects (e.g. physical, material, or non-material damage, loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy, significant economic or social disadvantage to concerned data subjects, etc.) and is based on a method chosen or established by the entity to ensure consistent and meaningful results. The entity has documented this method and the procedure to be followed when performing the risk analysis.
		
		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 (I-0) of the processing activities in scope.
		
		Furthermore, the entity considers at least the following elements when performing this risk analysis:
		• Organizational security elements:
		  ○ Security management: security policies and procedures for the protection of personal data, roles and responsibilities, access control policy, resource / asset management, change management, data processors
		  ○ Incident response and business continuity: handling of incidents / personal data breaches, business continuity / disaster recovery
		  ○ Human resources: confidentiality of personnel, training
		• Technical security elements:
		  ○ access control and authentication
		  ○ Logging and monitoring
		  ○ Security of data at rest: server / database security, workstation security
		  ○ Network / communication security
		  ○ Back-ups
		  ○ Mobile / portable devices
		  ○ Application lifecycle security
		  ○ Data deletion / disposal
		  ○ Physical security
		Furthermore, the entity takes also into account any additional requirements defined by law such as any processing limitations / conditions and specific organisational / technical measures to be implemented by the entity (please also refer to criterion II-a-1).
		
		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 documented 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-2	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 to personal data as well as for each identified risk to the rights and freedoms of the data subjects (II-f-1).
		This risk treatment plan shall be documented in detail and shall be established and carried out according to a documented 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 considers at least the following technical and organisational measures:
		• Organizational security elements:
		  ○ Security management:
		  ▪ Security policies and procedures for the protection of personal data (e.g. revision, communication, validation, etc.)
		  ▪ Roles and responsibilities (e.g. definition and allocation, avoidance of conflicts of interest, etc.)
		  ▪ Access control policy (e.g. role-based access, need to know principle, four-eyes-principle, etc.) – Furthermore, the entity shall ensure that any natural or legal person acting under its authority, who has access to personal data, does not process them except on instructions from the entity, unless he or she is required to do so under Union or Luxembourgish law.
		  ▪ Resource / asset management (e.g. inventory of software / hardware / networks, revision of these inventories, access, etc.)
		  ▪ Change management (e.g. monitoring of changes, separate testing environment, use of dummy data while testing, change policy, etc.)
		  ▪ Data processors (see also sections regarding the use of data processors)
		  ○ Incident response and business continuity:
		  ▪ Handling of incidents / personal data breaches (e.g. incident response plan, reporting of personal data breaches, documentation, etc.)
		  ▪ Business continuity / disaster recovery (e.g. detailed documentation, testing, roles & responsibilities, etc.)
		  ○ Human resources:
		  ▪ Confidentiality of personnel (e.g. confidentiality / non-disclosure agreements, etc.)
		  ▪ Training (e.g. training programmes / plans, etc.)
		• Technical security elements:
		  ○ Access control and authentication (e.g. user access management, password management, management of privileged users, review of user access rights, avoidance of generic users, etc.)
		  ○ Logging and monitoring (e.g. logging of view / modification / deletion, protection of log files, timestamps, logging of system administrator actions, logging of access to log files, etc.)

Ref.	Label	Description
		○ Security of data at rest: ▪ Server / database security (e.g. encryption, pseudonomization, etc.) ▪ Workstation security (e.g. anti-virus, session time-outs, installation of security updates, external storage devices, encryption, etc. ○ Network / communication security (e.g. encryption, remote access management, traffic monitoring, firewalls / Intrusion Detection Systems, etc.) ○ Back-ups (e.g. back-up strategy, monitoring, location of and access to back-up media, back-up media, back-up recovery testing, encryption, etc.) ○ Mobile / portable devices (e.g. access control procedures, encryption, secure software containers to separate private and business use, remote erasure, etc.) ○ Application lifecycle security (e.g. use of secure coding standards, vulnerability assessment / periodic penetration testing, software patching, etc.) ○ Data deletion / disposal (e.g. physical destruction, use of a data processor, etc.) ○ Physical security (e.g. IT system infrastructure, access controls, UPS, fire / water protection, etc.) 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. The entity shall define and implement procedures to assess the effectiveness of the risk treatment plan. This assessment shall take into account at least the following factors: ○ the results / conclusions of controls performed referenced in criteria II-f-3 to II-f-5; ○ lead indicators allowing the entity to measure the plan's effectiveness (e.g. including data on data breaches identified related to the processing activities in scope, on incidents detected during the controls performed, incidents handled vs. open incidents, etc.); Furthermore, the entity shall take into account any changes of the following factors when assessing the effectiveness of its risk treatment plan: ○ risk and risk level changes (II-f-1); ○ changes in the nature scope, context and purposes of the processing activity; ○ changes in the applicable regulatory framework; ○ changes in the entity's structure (internal as well as external in case of outsourcing etc.); ○ changes in the technology(ies) used for the processing activity; ○ changes concerning persons (e.g. responsibilities, functions, etc.) involved in the processing activity. • takes into account the formal opinion of the DPO. The entity's management formally validates the risk treatment plan.
II-f-3	Documented implementation of organisational and technical measures (GDPR Articles 5, 32)	For each processing activity in scope, the entity has implemented the operational and technical measures documented in the validated risk treatment plan (II-f-2). 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 persons within the entity that are involved in the processing activity and to the DPO and the entity's management.

Ref.	Label	Description
	(Recitals 29, 39, 75 – 79, 83, 116, 123)	
II-f-4	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. 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-5	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-6	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 based on the requirements set out in article 35 of the GDPR. In case the entity decides not to perform a DPIA, the decision together with the detailed 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

Ref.	Label	Description
		compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. The entity shall consider the opportunity to seek the views of data subjects or their representatives without prejudice to the protection of commercial or public interests or the security of processing operations (article 35.9 of the GDPR). Where the entity does not do so, it shall document the reasons for this in detail. The DPIA as well as all related assessments include a formal opinion of the DPO and have 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. For this review, the entity has implemented a documented 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 of the risk represented by the processing activity, 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-7	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-8	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; • assess whether the processor provides sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures allowing the entity to meet these certification criteria. • identify and analyse the risks related to the use of the processor according to II-f-1 and perform a DPIA according to II-f-6 and II-f-7, if applicable; • establish and put in place a risk treatment plan for each identified risk according to II-f-2; • ensure that the organisational and technical measures defined in the validated risk treatment plan are correctly implemented and documented according to II-f-3; • perform audits of the processor's activities in the context of the processing activities in scope as well as the follow-up on those audits according to II-f-4 and II-f-5.

Ref.	Label	Description
II-f-9	Contract / legal act under Union or Member State law (GDPR Article 28) (Recital 81)	For each processing activity in scope, where the entity uses a processor, it has a written (including in electronic form) contract / legal act under Union or Luxembourgish law in place that fulfils at least the following requirements for the processor: • The contract shall set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the entity. • 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 Luxembourgish law to which the processor is 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 Luxembourgish 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 pursuant to articles 32 to 36 of the GDPR 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 Luxembourgish 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-10	Policies and procedures (outsourcing relationship) (GDPR Article 28) (Recital 81)	The contractual provisions mentioned in II-f-9 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.

Ref.	Label	Description
		The entity has performed a detailed and documented assessment to ensure that those policies and procedures allow the entity to be compliant with 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.
II-f-11	Monitoring (GDPR Article 28) (Recital 81)	For each processing activity in scope, where the entity uses a processor, it has defined audit / monitoring 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 written (including in electronic form) contract or legal act under Union or Luxembourgish 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 Luxembourgish 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 Luxembourgish law, in particular providing guarantees to implement technical and organisational measures in such a manner that the processing will meet the requirements of GDPR; • 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 pursuant to articles 32 to 36 of the GDPR 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 Luxembourgish law requires storage of the personal data;

Ref.	Label	Description
		• 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 a detailed and documented assessment to ensure that those policies and procedures allow the entity to be compliant with 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, including with regard to transfers of personal data to a third country or an international organisation, unless required to do otherwise by Union or Luxembourgish law to which the entity is subject. In the latter case, the entity has documented this legal obligation and has informed the contractual partner of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. 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, 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).

Ref.	Label	Description
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	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). The entity pays particular attention to special categories of data when performing its risk analysis.
		
		This formal assessment includes an analysis of the potential impact and probability of each identified risk to the rights and freedoms of the data subjects (e.g. physical, material, or non-material damage, loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy, significant economic or social disadvantage to concerned data subjects, etc.) 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. The entity has documented this method and the procedure to be followed when performing the risk analysis.
		
		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 (I-0) of the processing activities in scope.
		
		Furthermore, the entity considers at least the following elements when performing this risk analysis:
		
		• Organizational security elements:
		  ○ Security management: security policies and procedures for the protection of personal data, roles and responsibilities, access control policy, resource / asset management, change management, data processors
		  ○ Incident response and business continuity: handling of incidents / personal data breaches, business continuity / disaster recovery
		  ○ Human resources: confidentiality of personnel, training
		• Technical security elements:
		  ○ access control and authentication
		  ○ Logging and monitoring
		  ○ Security of data at rest: server / database security, workstation security
		  ○ Network / communication security
		  ○ Back-ups

Ref.	Label	Description
		○ Mobile / portable devices ○ Application lifecycle security ○ Data deletion / disposal ○ Physical security 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 documented 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-6	Risk treatment (GDPR Article 32) (Recitals 39, 75 – 79, 83)	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 to personal data as well as for each identified risk to the rights and freedoms of the data subjects (please refer to III-5). This risk treatment plan shall be documented in detail and shall be established and carried out according to a documented 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 considers at least the following technical and organisational measures: • Organizational security elements: ○ Security management: ▪ Security policies and procedures for the protection of personal data (e.g. revision, communication, validation, etc.) ▪ Roles and responsibilities (e.g. definition and allocation, avoidance of conflicts of interest, etc.) ▪ Access control policy (e.g. role-based access, need to know principle, four-eyes-principle, etc.) – Furthermore, the entity shall ensure that any natural or legal person acting under its authority, who has access to personal data, does not process them except on instructions from the entity, unless he or she is required to do so under Union or Luxembourgish law. ▪ Resource / asset management (e.g. inventory of software / hardware / networks, revision of these inventories, access, etc.) ▪ Change management (e.g. monitoring of changes, separate testing environment, use of dummy data while testing, change policy, etc.)

Ref.	Label	Description
		▪ Data processors (see also sections regarding the use of data processors) ○ Incident response and business continuity: ▪ Handling of incidents / personal data breaches (e.g. incident response plan, reporting of personal data breaches, documentation, etc.) ▪ Business continuity / disaster recovery (e.g. detailed documentation, testing, roles & responsibilities, etc.) ○ Human resources: ▪ Confidentiality of personnel (e.g. confidentiality / non-disclosure agreements, etc.) ▪ Training (e.g. training programmes / plans, etc.) • Technical security elements: ○ Access control and authentication (e.g. user access management, password management, management of privileged users, review of user access rights, avoidance of generic users, etc.) ○ Logging and monitoring (e.g. logging of view / modification / deletion, protection of log files, timestamps, logging of system administrator actions, logging of access to log files, etc.) ○ Security of data at rest: ▪ Server / database security (e.g. encryption, pseudonomization, etc.) ▪ Workstation security (e.g. anti-virus, session time-outs, installation of security updates, external storage devices, encryption, etc. ○ Network / communication security (e.g. encryption, remote access management, traffic monitoring, firewalls / Intrusion Detection Systems, etc.) ○ Back-ups (e.g. back-up strategy, monitoring, location of and access to back-up media, back-up media, back-up recovery testing, encryption, etc.) ○ Mobile / portable devices (e.g. access control procedures, encryption, secure software containers to separate private and business use, remote erasure, etc.) ○ Application lifecycle security (e.g. use of secure coding standards, vulnerability assessment / periodic penetration testing, software patching, etc.) ○ Data deletion / disposal (e.g. physical destruction, use of a data processor, etc.) ○ Physical security (e.g. IT system infrastructure, access controls, UPS, fire / water protection, etc.) 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. The entity shall define and implement procedures to assess the effectiveness of the risk treatment plan. This assessment shall take into account at least the following factors: ○ the results / conclusions of controls performed referenced in criteria III-7 to III-9; ○ lead indicators allowing the entity to measure the plan's effectiveness (e.g. including data on data breaches identified related to the processing activities in scope, on incidents detected during the controls performed, incidents handled vs. open incidents, etc.); Furthermore, the entity shall take into account any changes of the following factors when assessing the effectiveness of its risk treatment plan:

Ref.	Label	Description
		○ risk and risk level changes (III-5); ○ changes in the nature scope, context and purposes of the processing activity; ○ changes in the applicable regulatory framework; ○ changes in the entity's structure (internal as well as external in case of outsourcing etc.); ○ changes in the technology(ies) used for the processing activity; ○ changes concerning persons (e.g. responsibilities, functions, etc.) involved in the processing activity. • 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-7	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-6). 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 persons within the entity that are involved in the processing activity and 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-8	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). 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-9	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.

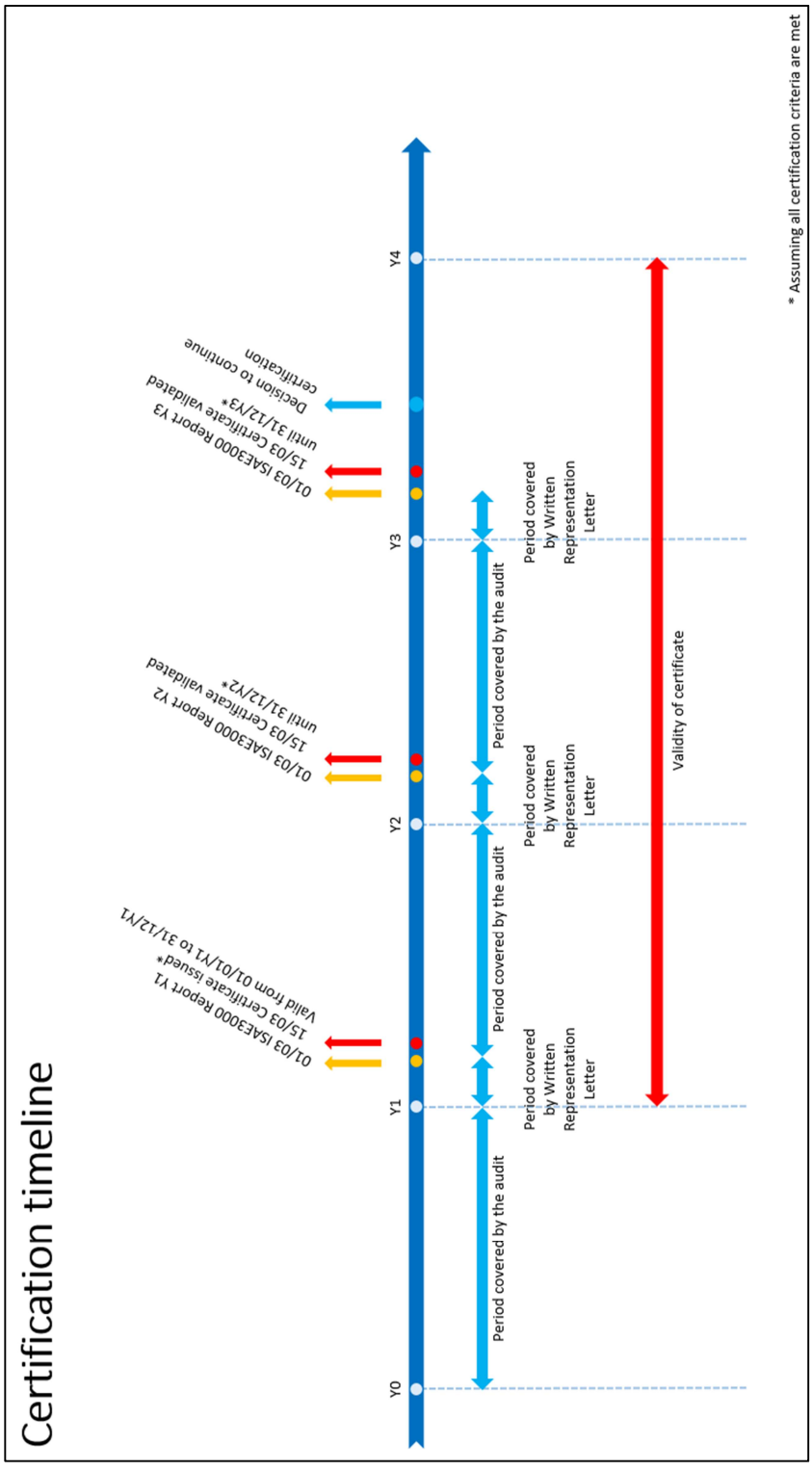
Ref.	Label	Description
		This process is documented in detail and the entity takes into account the formal opinion of its DPO. The entity's management shall validate the corrective actions taken and provide a report to the contractual partner.
		Subcontracting
III-10	Assessment of sufficiency (GDPR Article 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; • assess whether the processor provides sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures allowing the entity to meet these certification criteria. • identify and analyse the risks related to the use of the processor according to III-5; • establish and put in place a risk treatment plan for each identified risk according to III-6; • ensure that the organisational and technical measures defined in the validated risk treatment plan are correctly implemented and documented according to III-7; • perform audits of the processor's activities in the context of the processing activities in scope as well as the follow-up on those audits according to III-8 and III-9.
III-11	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, including information on the location(s) of the processor, the processing activities they will be carrying out and on any safeguards and measures to be implemented.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; • 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-12	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 assessment shall include an analysis of all possible available transfer mechanisms and their suitability with regard to the processing activity in scope respecting the provisions of chapter V of the GDPR. During this assessment, at least the following factors need to be considered: • Taking into account the nature, scope, context and purpose of the processing activity in scope, the entity shall assess which of those mechanisms is best suited to protect the rights and freedoms of the data subjects whose data is concerned by a transfer (e.g. specific safeguards, level of protection of personal data, ease of the exercise of data subjects' rights, etc.);

Ref.	Label	Description
		• The entity shall assess what the risks of using each of those mechanisms are and how they can be avoided / mitigated (e.g. mitigation of risks in case there are any provisions in the law of the country of the data importer that might reduce the effectiveness of the organisational / technical measures to protect personal data transferred, etc.); • The entity shall take into account CJEU judgments regarding the topic of transfers and mechanisms as well as EDPB guidelines when analysing those mechanisms. 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 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 • 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 documented 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 method the reviewer checks whether the chosen mechanism is still valid.

Ref.	Label	Description
		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-13	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 Luxembourgish law requires storage of the personal data.

6 ANNEX

ANNEX 1 – CERTIFICATION VALIDITY



ANNEX 2 – MAPPING OF GDPR-CARPA CERTIFICATION CRITERIA

The mapping table below serves as a reference table to demonstrate that the GDPR-CARPA certification criteria meet the mandatory compliance aspects[19].

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 Section III: Principles relating to processing of personal data (processor)
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 (right to object, right to restriction of processing, right of access, right to data portability) Subsection II – d: Accuracy (right to rectification) Subsection II – e: Storage limitation (right to erasure) Section III: Principles relating to processing of personal data (processor) (Contract / legal act under Union or Member State law, Policies and procedures (outsourcing relationship))
Obligation to notify data breaches pursuant to article 33	Section I: Accountability criteria / Governance criteria (Policies and procedures, Data breaches, Notification of data breaches towards the controller)
Data protection by design and by default, pursuant to article 25	Section I: Accountability criteria / Governance criteria (policies and procedures) Section II: Principles relating to processing of personal data (controller): Subsection II – a: Lawfulness and transparency of processing activities (Lawfulness, Transparency) 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 (Security, Outsourcing) Section III: Principles relating to processing of personal data (processor): Principles relating to processing of personal data (processor) (Security)

[19] Please refer i.a. to paragraph 48 of the guidelines 1/2018 on certification and identifying certification criteria in accordance with articles 42 and 43 of the regulation (Version 3.0, 4th of June 2019)

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 (DPIA)
Technical and organisational measures put in place pursuant to Articles 32	Section I: Accountability criteria / Governance criteria Section II: Principles relating to processing of personal data (controller) Section III: Principles relating to processing of personal data (processor)