GDPR-CERTIFIED ASSURANCE REPORT BASED PROCESSING ACTIVITIES

CERTIFICATION MECHANISM

Working draft for public consultation - 29 May 2018

Abstract

Document to the attention of organizations that want to provide certification procedures under the GDPR-CARPA certification mechanism.

Commission Nationale pour la Protection des Données

alain.herrmann@cnpd.lu

This document was prepared by the Commission Nationale Pour la Protection des Données ('CNPD') in collaboration with representatives from the assurance profession. It contains the description of the "GDPR-CARPA" certification mechanism. This document should be read in conjunction with the "GDPR-CARPA" certification criteria document that describes the content of the ISAE3000 report that underpins the certification decision. This document describes the additional steps that need to be taken based on the ISAE3000 report as well as the requirements that certification bodies have to fulfil in order to be granted the accreditation from CNPD to provide certification services according to the "GDPR-CARPA" certification mechanism.

About CNPD:

The National Commission for Data Protection (Commission Nationale pour la Protection des Données – CNPD) is an independent authority created by the Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data. It verifies the legality 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 draft bill 7184, CNPD will be the independent public authority responsible for monitoring the application of 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 the criteria. International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements other than Audits or Reviews of Historical Financial Information, should be read in conjunction with the Preface to the International Standards on Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements.

Versioning

Version	Description	Date	Author
V0.1	Initial version for public consultation	29/05/2018	CNPD

TABLE OF CONTENTS

INTRODUCTION

GENERAL

The General Data Protection Regulation (Regulation 2016/279) ('the GDPR'), which came into effect on 25 May 2018, provides a modernised, accountability and fundamental rights compliance framework for data protection in Europe. Ranges of measures 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.

As part of establishing certification mechanisms and data protection seals and marks, Article 43(1) of the GDPR requires Member States to ensure that certification bodies issuing certification under Article 42(1) are accredited by either or both, the competent supervisory authority or the national accreditation body. The Luxembourg legislator provides to the national supervisory authority (CNPD) the competence, on the basis of clear and transparent requirements to be set out by itself, to accredit certification bodies.

Meaningful certification mechanisms can enhance compliance with the GDPR and transparency for data subjects and in B2B relations, for example between controllers and processors. Data controllers and processors will benefit from an independent third-party attestation for the purpose of demonstrating compliance of their processing operations.

In this context, the Article 29 Working Party provides guidelines in relation to accreditation. The particular value and purpose of accreditation lies in the fact that it provides an authoritative statement of the competence of certification bodies that allows the generation of trust in the certification mechanism.

The guidelines provide guidance on how to interpret and implement the provisions of Article 43 of the GDPR. In particular, they aim to help Member States, supervisory authorities and national accreditation bodies to establish a consistent and harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR.

NOTICE TO READERS

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

If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority – which is the case for Luxembourg- , the supervisory authority should establish accreditation requirements including, but not limited to the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides less instruction about the requirements/criteria for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The Working Party notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.

Article 43(6) provides that "[t]he requirements referred to in paragraph 3 of this Article shall be made public by the supervisory authority in an easily accessible form". Therefore, to ensure transparency, all criteria or requirements approved by a supervisory authority should be published. In terms of quality and trust in the certification bodies, it would be desirable, if all the requirements for accreditation were readily available to the public.

The GDPR - CARPA certification mechanism describes the mandatory requirements that a certification body needs to fulfil in order to be eligible for an accreditation by CNPD under the mechanism. Furthermore, it describes the certification procedure as well as the way the certificate needs to be managed during its lifetime.

Certification can only be granted by certification bodies that have been accredited by CNPD. The list of accredited certification bodies, as well as the accreditation requirements will be published on the CNPD website.

GDPR - CARPA CERTIFICATION MECHANISM AND CRITERIA

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 Article 29 Working Party.

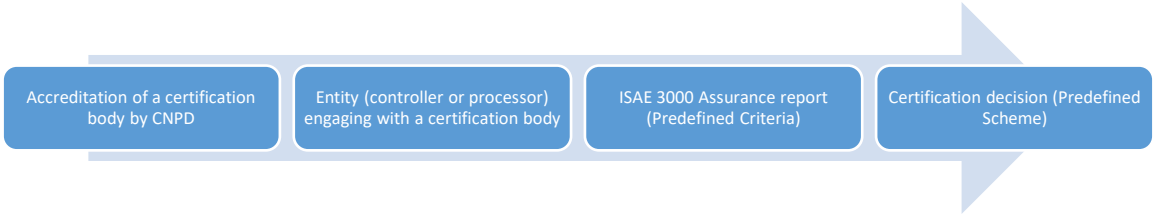
The CNPD aims to provide for a certification mechanism with the following characteristics:

- 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 a period of time;
- It is up to the entities to define the processes subject to the certification request. This flexibility aims allowing data controllers and processors to target those processing activities that are most relevant for them, data subjects or their clients – depending on whom they intend to demonstrate compliance to;
- Certification should have clear focus on data protection – other considerations are covered to the extent that they are relevant for data protection.

Considering these objectives, CNPD decided upon the following requirements:

- The assessment leading to the certification needs to be based on an assurance report that is to be executed according to the ISAE 3000 standard. The International Standard on Assurance Engagements (ISAE) deals with assurance engagements other than audits or reviews of historical financial information. This standard is already well established and allows CNPD to leverage on best practice. Furthermore an ISAE 3000 assurance report is in itself – and independently of GDPR certification - an internationally recognized report that can serve the data controller or processor in its relation with auditors or business clients.
- CNPD is focused on the quality of the audit procedures that will underpin its certification mechanism. CNPD creates the certification mechanism and entrusts accredited certification bodies with the certification procedure to issue the certificate. This approach allows data controllers and processors to have access to certification independently of the availability of CNPD's internal resources. CNPD will ensure continuous and thorough monitoring of accredited certification bodies.

The GDPR - CARPA certification process is composed of multiple steps – first the assurance audit, based on the GDPR - CARPA certification criteria, needs to be issued by an accredited certification body. This audit report is the basis of the formal certification decision, which is further described in the "GDPR Governance" Certification Mechanism.



CONTINUOUS IMPROVEMENT OF THE CERTIFICATION CRITERIA

The CNPD is owner of the certification mechanism and it ensures a continuous surveillance of the adequacy of the certification criteria to the current state of the art in the data protection domain.

DEFINITIONS

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 article 42 and 43 GDPR, taking into account EN-ISO/IEC 17065/2012 and the additional requirements established by the supervisory authority and or by the Board.
- **'Additional (accreditation) requirements'** means the requirements established by the supervisory authority which is competent and against which an accreditation is performed[3]
- **'Certification'** shall mean the assessment [4] and impartial, third party attestation that the fulfilment of certification criteria has been demonstrated;
- **'Certification body'** shall mean a third –party conformity assessment body [5] operating a certification mechanisms[6];
- **'Certification scheme / mechanism'** shall mean 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

[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] Article 43(1)(b), (3), (6).

[4] 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.

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

[6] Article 42.1, 42.5 GDPR.

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 shall mean the criteria against which a certification (conformity assessment)is performed[7]
- **'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);
- '**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;

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 (that is, the outcome of the measurement or evaluation of an underlying subject matter against criteria). In the context of the GDPR – CARPA certification scheme 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 engagement. In the context of the GDPR – CARPA certification scheme this term refers to the criteria that are listed in this document.
- '**Engaging party'** means the part(ies) that engages the practitioner to perform the assurance engagement.In the context of the GDPR – CARPA certification scheme this terms refers to either the data controller or the data processor who intends to obtain certification.
- '**Practitioner**' means the individual(s) conducting the engagement (usually the engagement partner or other members of the engagement team, or, as applicable, the firm). Where this ISAE 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 scheme this term refers to the staff/personnel employed or occupied by the accredited certification body that executes the certification audit / assurance engagement field work.

[7] See Article 42(5).

ORGANISATION OF THE CERTIFICATION MECHANISM

The certification mechanism is organized in two sections, that are either relevant to the certification bodies or that contain a functional description of the mechanism as listed below:

Aspects relevant to certification bodies	• **Accreditation requirements:** Description of the reuirements that needs to fulfil a certification body in order to be eligible for an accreditation as a certification body under this Certification Scheme. • **Accreditation process:** Description of the process that an organization that wished to act as certification body under this scheme needs to follow.
Functional description of the certification process and certificate management	• **Certification process:** Description of the certification process and how it relates to the certification criteria. This section also describes how the evaluation to determine certification based on the presence of a compliant ISAE3000 assurance report needs to be drawn.

ACCREDITATION REQUIREMENTS

A certification body, in order to be eligible for accreditation by the CNPD, needs to fulfil all "accreditation requirements" under this certification mechanism. Accreditation requirements have to be classified as either "general requirements" or "additional supervisory authority requirements".

GENERAL CRITERIA

The general requirements are aligned with ISO 17065 (the mapping / gap analysis between ISO 17065 and ISAE 3000 has been documented).

The certification body has to be authorized to issue ISAE3000 reports. Therefore as the certification body has to apply all requirements for performing an ISAE 3000 attestation engagement. An ISAE 3000 template report can be found in "Annex I – ISAE3000 Template report".

All aspects linked to the procedures of the attestation engagement are covered in the document: "International Standard on Assurance Engagements 3000 (Revised) – Assurance engagements other than audits or reviews of historical financial information" Link: http://www.ire.lu/fileadmin/media/Env_normatif_international_non_ISA/201312_ISAE_3000_Revised_20150618_IRE_adoption.pdf

In addition to the ISAE3000 requirements, the certification body needs to fulfil the following general requirements.

General requirements (ISO 4)	
Legal and contractual matters (ISO 4-1)	
ISO-4-1-1	The certification body shall ensure its certification agreement requires that the client comply at least with the following: • the client always fulfils the certification requirements, including implementing appropriate changes when they are communicated by the certification body; • the client makes claims regarding certification consistent with the scope of certification; • the client does not use its product certification in such a manner as to bring the certification body into disrepute and does not make any statement regarding its product certification that certification body may consider misleading or unauthorized; • upon suspension, withdrawal, or termination of certification, the client discontinues its use of all advertising matter that contains any reference thereto and take actions as required by the certification scheme and takes any other required measure; • if the client provides copies of the certification documents to others, the documents shall be reproduced in their entirely; • in making reference to its product certification in communication media such as documents, brochures or advertising, the client complies with the requirements specified by the certification scheme • the client keeps a record of all complaints made known to it relating to compliance with certification requirements and makes these records available to the certification body when requested, and

	○ takes appropriate action with respect to such complaints and any deficiencies found in products that affect compliance with the requirements for certification; ○ documents the actions taken; • the client informs the certification body, without delay, of changes that may affect its ability to conform with the certification requirements.
ISO-4-1-2	The certification body shall exercise the control as specified by the certification scheme over ownership, use and display of licenses, certificates, marks of conformity, and any other mechanisms for indicating a product is certified.
ISO-4-1-3	Incorrect references to the certification scheme, or misleading use of licenses, certificates, marks, or any other mechanism for indicating a product is certified, found in documentation or other publicity, shall be dealt with by suitable action.
Legal and contractual matters (ISO 4-2) –requirements covered by ISAE3000	
Liability and financing (ISO 4-3)	
ISO-4-3-1	The certification body shall have adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations.
ISO-4-3-2	The certification body shall have the financial stability and resources required for its operations.
Non-discriminatory conditions (ISO 4-4)	
ISO-4-4-1	The policies and procedures under which the certification body operates, and the administration of them, shall be non-discriminatory. Procedures shall not be used to impede or inhibit access by applicants, other than those duly documented in the certification body's internal risk management criteria. Note: A certification body can decline to accept an application or maintain a contract for certification from a client when fundamental or demonstrated reasons exist, such as the client participating in illegal activities, having a history of repeated non-compliances with certification/product requirements, or similar client-related issues.
Confidentiality (ISO 4-5) –requirements covered by ISAE3000	
Publicly available information (ISO 4-6)	
ISO-4-6-1	The certification body shall maintain (through publications, electronic media or other means), and make available upon request, the following: a) information about (or reference to) the certification scheme(s), including evaluation procedures, rules and procedures for granting, for maintaining, for extending or reducing the scope of, for suspending, for withdrawing or for refusing certification; b) a description of the means by which the certification body obtains financial support and general information on the fees charged to applicants and to clients; c) a description of the rights and duties of applicants and clients, including requirements, restrictions or limitations on the use of the certification body's name and certification mark and on the ways of referring to the certification granted; d) information about procedures for handling complaints and appeals.
Structural requirements (ISO 5)	
Organizational structure and top management (ISO 5-1)	

ISO-5-1-1	The management of the certification body shall identify the board, group of persons, or person having overall authority and responsibility for supervision of the finances of the certification body;
Mechanism for safeguarding impartiality (ISO 5-2) –requirements covered by ISAE3000	
Resource requirements (ISO 6)	
Certification body personnel (ISO 6-1)	
ISO-6-1-1	The certification body maintains records on the personnel involved in the certification process. The record contains: • Name and address; • Employer(s) and position held; • Educational qualification and professional status; • Experience and training; • The assessment of competence; • Performance monitoring; • Authorizations held within the certification body; • Date of the most recent updating of each record; Record have to be retained until 3 years after the last certificate the person has been involved in has expired.
Resources for evaluation (ISO 6-2)	
ISO-6-2-1	The certification body shall not outsource certification activities.
Process requirements (ISO 7)	
General (ISO 7-1)- –requirements covered by ISAE3000	
Application (ISO 7-2) –requirements covered by ISAE3000	
Application review (ISO 7-3) –requirements covered by ISAE3000	
Evaluation (ISO 7-4) –requirements covered by ISAE3000	
Review (ISO 7-5)	
ISO-7-5-1	The certification body shall assign at least one person to review all information and results related to the evaluation. The review shall be carried out by person(s) who have not been involved in the evaluation process.
ISO-7-5-2	Recommendations for a certification decision based on the review shall be documented, unless the review and the certification decision are completed concurrently by the same person.
Certification decision (ISO 7-6)	
ISO-7-6-1	The certification body shall be responsible for, and shall retain authority for, its decisions relating to certification.
ISO-7-6-2	The certification body shall assign at least one person to make the certification decision based on all information related to the evaluation, its review, and any other relevant information. The certification decision shall be carried out by a person or group of persons that has not been involved in the process for evaluation Note: The review and the certification decision can be completed concurrently by the same person or group of persons.

ISO-7-6-3	The person(s) [excluding members of committees] assigned by the certification body to make a certification decision shall be employed by, or shall be under contract with the certification body;
ISO-7-6-4	The certification body shall notify the client of a decision not to grant certification, and shall identify the reasons for the decision.
Certification documentation (ISO 7-7)	

ISO-7-7-1	The certification body has to provide to the client formal certification documentation the cleary convey, or permits identification of:
	• The name and address of the certification body
	• The date certification is granted; the date shall not precede the date the certification decision was completed;
	• The name and address of the client;
	• The scope of certification
	  ○ List of the processing certified
	  ○ Covered period
	• The term or expiration date of certification
	• Conclusion of the ISAE audit associated to the certification (assurance statement)

ISO-7-7-2	The certification documentation has to include the signature or other defined authorization of the person(s) of the certification body assigned such responsibility;
ISO-7-7-3	The formal certification documentation can only be issued after or concurrent with: • The decision to grant or extend the scope of certification has been made • Certification requirements being fulfilled; and • The certification agreement has been completed / signed.
Directory of certified "products" (ISO 7-8)	
ISO-7-8-1	The certification body shall maintain information on certified organisations which contains at least the following: a) identification of the client. b) identification of the scope b) identification of the period covered.
Surveillance (ISO 7-9) - Note – surveillance is to be executed under ISAE3000 rules	
Changes affecting certification (ISO 7-10)- Note – changes affecting certification have to be assessed under ISAE3000 rules	
Termination, reduction, suspension or withdrawal of certification (ISO 7-11)	
ISO-7-11-1	If certification is terminated (by request of the client), suspended or withdrawn, the certification body shall take actions specified by the certification scheme and shall make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure it provides no indication that the processing activity continues to be certified.
ISO-7-11-2	If certification is suspended, the certification body shall assign one or more persons to formulate and communicate the following to the client: • actions needed to end suspension and restore certification for the processing activity(ies) in accordance with the certification scheme; • any other actions required by the certification scheme.

	These persons shall be competent in their knowledge and understanding of all aspects of the handling of suspended certifications.
ISO-7-11-3	If a scope of certification is reduced, the certification body shall take actions specified by the certification scheme and shall make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.
ISO-7-11-4	If certification is reinstated after suspension, the certification body shall make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure all appropriate indications exist that the processing activity(ies) continu(es) to be certified.
ISO-7-11-5	If a decision to reduce the scope of certification is made as a condition of reinstatement, the certification body shall make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.
Records (ISO 7-12)	
ISO-7-12-1	The certification body retains records to demonstrate that all certification process requirements (those of this certification scheme) have been effectively fulfilled.
ISO-7-12-2	The certification body shall keep records confidential. Records shall be transported, transmitted and transferred in a way that ensures confidentiality is maintained.
ISO-7-12-3	The certification body defines a retention policy of these records.
Complaints and appeals (ISO 7-13)	
ISO-7-13-1	The certification body shall have a documented process to receive, evaluate and make decisions on complaints and appeals. The certification body shall record and track complaints and appeals, as well as actions undertaken to resolve them.
ISO-7-13-2	Upon receipt of a complaint or appeal, the certification body shall confirm whether the complaint or appeal relates to certification activities for which it is responsible and, if so, shall address it.
ISO-7-13-3	The certification body shall acknowledge receipt of a formal complaint or appeal.
ISO-7-13-4	The certification body shall be responsible for gathering and verifying all necessary information (as far as possible) to progress the complaint or appeal to a decision.
ISO-7-13-5	The decision resolving the complaint or appeal shall be made by, or reviewed and approved by, person(s) not involved in the certification activities related to the complaint or appeal.
ISO-7-13-6	To ensure that there is no conflict of interest, personnel (including those acting in a managerial capacity) who have provided consultancy for a client, or been employed by a client, shall not be used by the certification body to review or approve the resolution of a complaint or appeal for that client within two years following the end of the consultancy or employment.
ISO-7-13-7	Whenever possible, the certification body shall give formal notice of the outcome and the end of the complaint process to the complainant.
ISO-7-13-8	The certification body shall give formal notice of the outcome and the end of the appeal process to the appellant.

ISO-7-13-9	The certification body shall take any subsequent action needed to resolve the complaint or appeal.
Management system requirements (ISO 8)-Option A	
General management system documentation (Option A) (ISO 8-2)	
ISO-8-2-1	The certification body's top management shall establish, document, and maintain policies and objectives for fulfilment of this certification scheme and shall ensure the policies and objectives are acknowledged and implemented at all levels of the certification body's organization.
ISO-8-2-2	The certification body's top management shall provide evidence of its commitment to the development and implementation of the management system and its effectiveness in achieving consistent fulfilment of this certification scheme.
ISO-8-2-3	The certification body's top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that include the following: • ensuring that processes and procedures needed for the management system are established, implemented and maintained; • reporting to top management on the performance of the management system and any need for improvement.
ISO-8-2-4	All documentation, processes, systems, records, etc. related to the fulfilment of the requirements of this certification scheme shall be included, referenced, or linked to documentation of the management system.
ISO-8-2-5	All personnel involved in certification activities shall have access to the parts of the management system documentation and related information that are applicable to their responsibilities.
Control of documents (Option A) (ISO 8-3)	
ISO-8-3-1	The certification body shall establish procedures to control the documents (internal and external) that relate to the fulfilment of this certification scheme.
ISO-8-3-2	The procedures shall define the controls needed to: • approve documents for adequacy prior to issue; • review and update (as necessary) and re-approve documents; • ensure that changes and the current revision status of documents are identified; • ensure that relevant versions of applicable documents are available at points of use; • ensure that documents remain legible and readily identifiable; • ensure that documents of external origin are identified and their distribution controlled; • prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.
Control of records (Option A) (ISO 8-4)	
ISO-8-4-1	The certification body shall establish procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfilment of this certification scheme.
ISO-8-4-2	The certification body shall establish procedures for retaining records for a period consistent with its contractual and legal obligations. Access to these records shall be consistent with the confidentiality arrangements.
Management review (Option A) (ISO 8-5)	

ISO-8-5-1	The certification body's top management shall establish procedures to review its management system at planned intervals, in order to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this certification scheme. These reviews shall be conducted at least once a year. Alternatively, a complete review broken up into segments shall be completed within a 12-month time frame. Records of reviews shall be maintained.
ISO-8-5-2	The input to the management review shall include information related to the following: • results of internal and external audits; • feedback from clients and interested parties related to the fulfilment of this International Standard; • feedback from the mechanism for safeguarding impartiality; • the status of preventive and corrective actions; • follow-up actions from previous management reviews; • the fulfilment of objectives; • changes that could affect the management system; • appeals and complaints.
ISO-8-5-3	The outputs from the management review shall include decisions and actions related to the following: • improvement of the effectiveness of the management system and its processes; • improvement of the certification body related to the fulfilment of this certification scheme; • resource needs.
Internal audits (Option A) (ISO 8-6)	
ISO-8-6-1	The certification body shall establish procedures for internal audits to verify that it fulfils the requirements of this certification scheme and that the management system is effectively implemented and maintained.
ISO-8-6-2	An audit program shall be planned, taking into consideration the importance of the processes and areas to be audited, as well as the results of previous audits.
ISO-8-6-3	Internal audits shall normally be performed at least once every 12 months, or completed within a 12-month time frame for segmented (or rolling) internal audits. A documented decision-making process shall be followed to change (reduce or restore) the frequency of internal audits or the time frame in which internal audits shall be completed. Such changes shall be based on the relative stability and ongoing effectiveness of the management system. Records of decisions to change the frequency of internal audits, or the time frame in which they will be completed, including the rationale for the change, shall be maintained.
ISO-8-6-4	The certification body shall ensure that: • internal audits are conducted by personnel knowledgeable in certification, auditing and the requirements of this International Standard; • auditors do not audit their own work; • personnel responsible for the area audited are informed of the outcome of the audit; • any actions resulting from internal audits are taken in a timely and appropriate manner; • any opportunities for improvement are identified.
Corrective actions (Option A) (ISO 8-7)	

ISO-8-7-1	The certification body shall establish procedures for identification and management of nonconformities in its operations.
ISO-8-7-2	The certification body shall also, where necessary, take actions to eliminate the causes of nonconformities in order to prevent recurrence.
ISO-8-7-3	Corrective actions shall be appropriate to the impact of the problems encountered.
ISO-8-7-4	The procedures for corrective actions shall define requirements for the following: • identifying nonconformities (e.g. from complaints and internal audits); • determining the causes of nonconformity; • correcting nonconformities; • evaluating the need for actions to ensure that nonconformities do not recur; • determining and implementing the actions needed in a timely manner; • recording the results of actions taken; • reviewing the effectiveness of corrective actions.
Preventive actions (Option A) (ISO 8-8)	
ISO-8-8-1	The certification body shall establish procedures for taking preventive actions to eliminate the causes of potential nonconformities.
ISO-8-8-2	Preventive actions taken shall be appropriate to the probable impact of the potential problems.
ISO-8-8-3	The procedures for preventive actions shall define requirements for the following: • identifying potential nonconformities and their causes; • evaluating the need for action to prevent the occurrence of nonconformities; • determining and implementing the action needed; • recording the results of actions taken; reviewing the effectiveness of the preventive actions taken.

ADDITIONAL SUPERVISORY AUTHORITY REQUIREMENTS

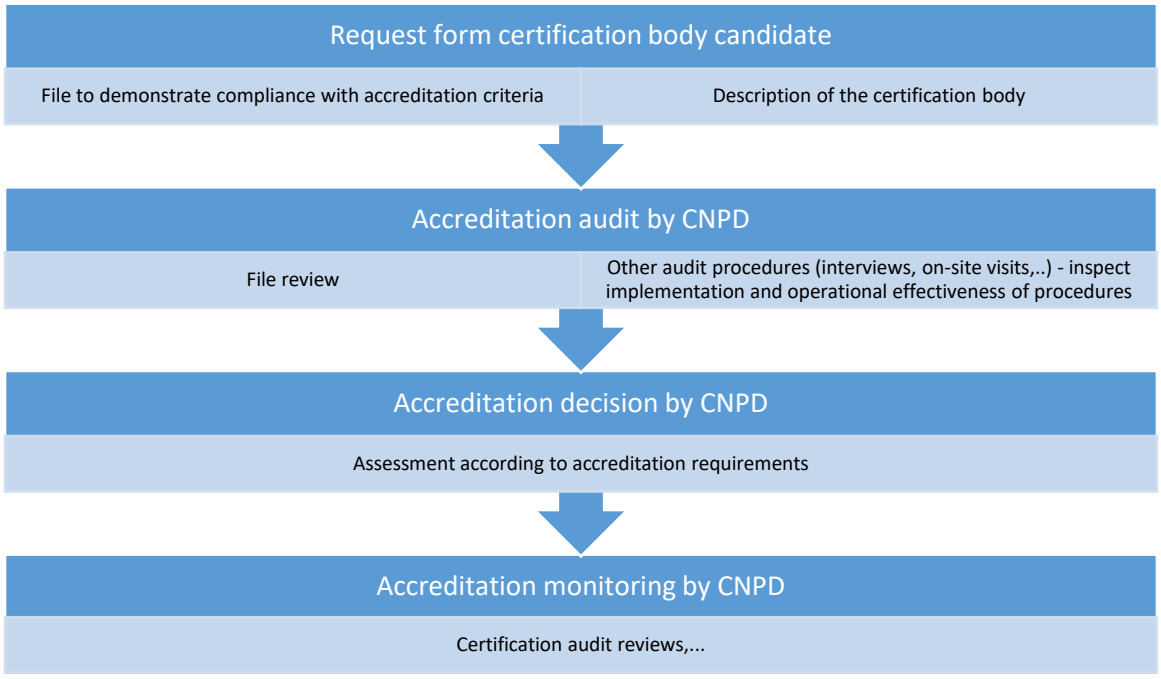
Additional requirements should be especially focused on ensuring that certification bodies have an appropriate level of data protection expertise in accordance with Article 43(1). The additional accreditation requirements and criteria established by the supervisory authority will apply to all certification bodies requesting accreditation. The accreditation body will evaluate whether that certification body is competent to carry out the certification activity in line with the additional requirements and the subject matter of certification.

Personal competencies	
P-01	The certification body has developed a specific data protection training program for the individuals involved in the attestation engagement. This program must contain a component to validate the competences acquired by the personnel that followed the training program (for example: an exam).
P-02	The certification body implements a mechanism to ensure that the staff involved in the attestation engagement has an adequate level of knowledge of data protection.
P-03	The certification body ensures that an individual – or team of individuals - that can demonstrate thorough experience in the domain of data protection performs the quality review of the content of the attestation engagement
P-04	The certification body involves at least one individual with legal or regulatory competencies in the conduct of the attestation engagement.
P-05	The certification body involves at least one individual with IT technical competencies in the attestation engagement.
Independence and conflicts of interest	
I-01	The certification body declares and sets up a mechanism to ensure that there is no overlap between consulting activities and certification otherwise specific rules have to be defined and followed.
I-02	The certification body can't be processor for an organization that it certifies.
I-03	The certification body can't be involved in the design and/or implementation of processing activities for the certified company (i.e. to avoid a conflict between selling a product and certifying the usage of the product)

ACCREDITATION PROCESS

PROCESS

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



Only CNPD is entitled to provide an accreditation for the GDPR – CARPA certification mechanism described in this document.

The accreditation is granted to the certification body and not to individual persons. Application of criteria that apply to the personnel involved need to be ensured by the certification body during certification engagements.

It is highly recommended that an entity that applies for accreditation by CNPD for this scheme has familiarized itself with the accreditation requirements upfront.

The application for accreditation needs to be addressed in writing to CNPD. The application needs to contain the documentation necessary for CNPD to assess all accreditation requirements. Incomplete applications will be subject to delay until all information is received.

Upon receipt of the application, you will be allocated a case manager who will be your main contact during the assessment. The case manager will review the documentation and guide you through the process of gaining accreditation.

Your case manager will guide you through the process and agree timescales for key milestones.

A pre-assessment is an informal visit to determine your current level of maturity for being accredited. A pre-assessment visit is optional, but it can be a valuable step in the process to reduce delays in gaining accreditation.

Once you have addressed any issues raised during the pre-assessment visit, the initial assessment is the first formal assessment.

Should you have any findings, you will have approximately 12 weeks (this may vary but will be agreed with your case manager) to provide suitable evidence to your case manager that they have been addressed.

Once any mandatory findings have been satisfactorily cleared, the case manager will submit a recommendation to the Commissioners of the CNPD.

Following ratification of the decision to grant accreditation you will be notified in writing. You will also receive a certificate of accreditation, and a schedule will be made publicly available on the CNPD website.

Your accreditation will be confirmed on an annual basis by surveillance visits, with a full re-assessment every fourth year.

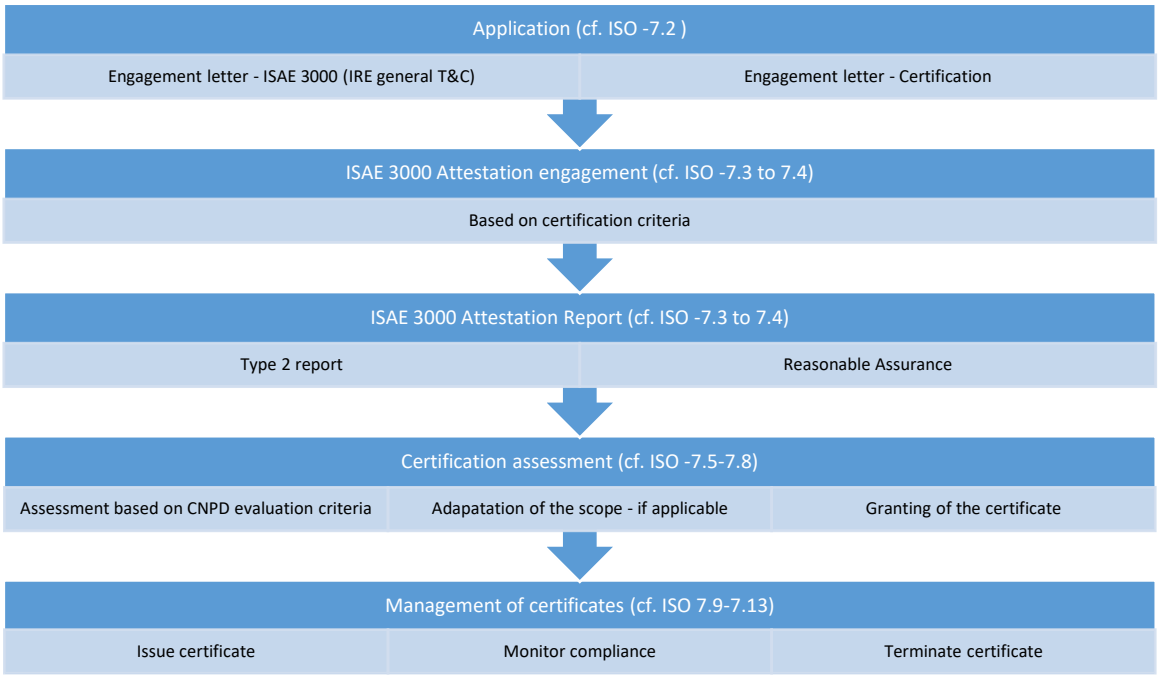
OTHER CONSIDERATIONS

- **Liability of the certification body:** Pursuant to article 83 (4) (b) of the Regulation the certification body might be subject to administrative fines by the supervisory authority if it infringes its obligations as certification body. This liability is without any prejudice of other responsibilities the certification body engages for (e.g. contractual arrangements between the certification body and the certified entity, or its professional obligations in regards to ISAE 3000 engagements). Professionalism is of utmost importance to ensure relevance and added-value of the given certification scheme.

CERTIFICATION PROCESS AND EVALUATION

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

PROCESS



The certification process is aligned to ISO 17065 requirements -references to ISO section are indicated in brackets. Please refer to the ISO standard and/or ISAE3000 requirements for more details.

A model of the certificate will be provided at a later stage.

EVALUATION

This section further specifies how the certification decision as indicated in the process description needs to be taken and documented based upon the ISAE 3000 Attestation Report. Classification of non-conformities for the assessed requirements in the scope have to follow the following rules:

Major non-conformity:

If one of the following elements applies to the result of an audit, it has to be considered a major non-conformity:

- Systematic major problem at a governance level
- Systematic dysfunction of the processing record (as defined under article 30 of the Regulation)
- Procedure for determining the lawfulness of a processing is missing or weak
- Absence of systematic involvement of adequate / competent staff (for data protection control activities that need to be executed by the controller/processor)
- Non-compliance identified in a previous audit (minor and major)

Minor non-conformity:

If one of the following elements applies to the result of an audit, it has to be considered a minor non-conformity:

- Punctual dysfunction in the execution of a procedure
- Dysfunction without any impact or minor impact on data subjects
- Missing documentation / evidences but the requirement is met

APPLICATION OF NON-CONFORMITIES

Taking into account the entire scope of requirements of the section I of the certification criteria, the following rules apply:

- A major non-compliance leads to a complete rejection of the certification.
- Cumulative minor non-conformities that leads to conclude on a major governance problem (taking into account minor non-conformities of the requirements in section II of the certification requirements) leads to a complete rejection of the certification.

For section II of the certification criteria, the decision to apply a non-conformity has to be performed for each processing activity in the scope:

- A major non-conformity for a specific processing leads to the exclusion of the processing from the certification scope (the certification can still be granted for the other processing in scope)
- If a minor non-conformity for a specific processing is identified, the certification body has to assess the impacts on the fundamental rights and freedoms of the data subjects linked to the identified non-conformity:
    - If there is a risk of an impact on data subjects, the certification the concerned specific processing has to be rejected and it has to be excluded from the scope of certification;
    - If there is no risk of an impact on data subjects, the specific concerned processing can remain in the scope of certification; an instruction to mitigate the minor non-conformity has to be issued.

For section III of the certification criteria, the decision to apply a non-conformity has to be performed for each processing following the same rules as for section II.

OTHER CONSIDERATIONS

- **Sectoral criteria:** The GDPR –CARP certification criteria have been designed in a way so that they are flexible enough to be applied independently of any given sector. Each entity is flexible to define the measures it puts in place in order to fulfil the criteria. Sector specific elements might be added under the form of "focus points" or "guidance" for the practitioners.
- **Period covered:** The certifications scheme as understood by article 42 of GDPR upon the completion of an ISAE 3000 report must cover a period of at least 6 month and a maximum of 12-month (backwards looking). The certificate is valid for a period as long in the future as the period covered by of the ISAE engagement. This means that a certificate based on an ISAE engagement covering 12 month, is valid for 12 month starting on the end of the period covered by the report.
- **Legal value:** The GDPR –CARP certification criteria, and the related ISAE 3000 report have been designed to support a certification scheme as understood by article 42 of GDPR. Under GDPR it is stated that entities (controllers and processors) can rely on certification to demonstrate their compliance in regards of certain elements of GDPR. However, it is also stated that certification pursuant to this 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.
- **Impact of certification and administrative fines**: In case an administrative fine is to be imposed on an entity, article 83 (2) (j) obliges the national supervisory authority / CNPD to give due regard to the adherence of the entity to approved certification mechanisms. It is however to be noted that certification can have relieving an alleviating as well as aggravating impact – it would in particular have an aggravating impact in case the entity is not following / effectively operating the controls it claims to have in place during certification. This risk is mitigated through the fact that the certificate covers a past period that has been subject to assurance, however inherent risks of assurance engagements include the fact that not all exceptions might be detected.
- **Point of focus - privacy**: The GDPR Governance criteria have a clear focus on data protection. While some information security elements have been integrated, they do not constitute the main focus. Other information security certifications and reference models should be used in the course of a certification. It is the role of the certification body to assess the extent to which it can rely on these elements.

ANNEX I – Template ISAE 3000 Report

Report on the [XYZ Entity]'s compliance with the GDPR - CARP Criteria identified in the schedule hereto governing the [XYZ ENTITY]'s activity in relation to the application of GDPR for the period

Report on the [XYZ Entity]'s compliance with the GDPR CARP – Criteria identified in the schedule hereto governing the [XYZ ENTITY]'s activity in relation to the application of GDPR for the period from 1 January 20XX to 31 December 20XX.

Contents

1 Section One: Scope of the report

This report is intended to describe certain procedures, activities and controls at [XYZ Entity] ("the Company" or "[XYZ ENTITY]") related to its internal control system for the period from 1 January 20XX to 31 December 20XX in accordance with the criteria set by the [identify engaging party, e.g. the board of directors of XYZ Entity] and uses as a framework the requirements set out in GDPR CARPA criteria, as issued by CNPD, identified in the schedule hereto governing the [XYZ ENTITY]'s activity in relation to the application of GDPR (each a "GDPR CARP – Criteria").

It is designed to provide intended users of this report with information as required by the GDPR CARP – Criteria.

This report relates to the [XYZ ENTITY] policies and procedures that cover the scope of the report.

It does not cover [XYZ ENTITY] policies and procedures that are applicable to other areas of business, notably the _____ covering the specific processes for _____.

This report was prepared in accordance with International Standard on Assurance Engagement ("ISAE") 3000, as adopted for Luxembourg by the Institut des Réviseurs d'Entreprises.

[XYZ ENTITY] provided the procedures and documents "[XYZ ENTITY] GDPR CARP – Criteria" dated _____ which was used as the main basis for writing this report.

Tests of effectiveness

The types of tests performed and results with respect to the operating effectiveness of controls are detailed in Section Four.

Inquiry	Inquired of appropriate personnel. Inquiries seeking relevant information or representation from [XYZ ENTITY] personnel were performed to obtain, among other factors: - Knowledge and additional information regarding the control; - Corroborating evidence of the controls. Even where not expressly stated, inquiries were performed to determine that the procedures were in place as described.
Observation	Observed the application or existence of specific controls as represented.
Inspection	Inspected documents and records indicating performance of the control. This includes, among other things: - Inspections of the list of supporting documents to assess whether they exist; - Inspection of the documents to assess whether they support the procedures and comments from by [XYZ ENTITY] in the column "[XYZ ENTITY]'s descriptions, procedures and policies on its compliance with the GDPR CARP – Criteria".

Report on the [XYZ Entity]'s compliance with the GDPR CARP – Criteria identified in the schedule hereto governing the [XYZ ENTITY]'s activity in relation to the application of GDPR for the period from 1 January 20XX to 31 December 20XX.

2 Section Two: Assurance report of Independent Auditors

Independent Assurance Report to the [identify engaging party, e.g. the board of directors of XYZ Entity] Regarding the System of Internal Control Regarding Compliance with the GDPR governance – Criteria.

3 Section Three: [XYZ ENTITY] Management Statement

[XYZ Entity] confirms that:

(a) The accompanying description in Section 4 fairly presents the system of internal control regarding compliance with [XYZ Entity]'s GDPR CARP – Criteria throughout the period from January 1, 20XX to December 31, 20XX. The criteria we used in making this statement were that the accompanying description:

(i). Presents how the system has been designed and implemented to comply with GDPR Criteria based on the elements of the GDPR CARP – Criteria issued by the Commission Nationale Pour la Protection des Données ('CNPD'), including:

- The different kinds of services that can be outsourced to the Company and are in scope.
- The procedures, within both information technology and manual systems, by which those services are initiated, recorded, processed, corrected as necessary.
- The relevant control objectives and controls designed to achieve those objectives.

(ii). Includes relevant details of changes to the [XYZ Entity]'s system during the period from January 1, 20XX to December 31, 20XX.

(iii). Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the GDPR governance – Criteria and may not, therefore, include every aspect of the system that other users than the intended users of this report may consider important in its own particular environment.

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from January 1, 20XX to December 31, 20XX.

(c) Intended users of the Report are:
(i) [XYZ entity], its management;
(ii) The user entities of the Entity;
(iii) The CNPD and the certification body.

Report on the [XYZ Entity]'s compliance with the GDPR CARP – Criteria identified in the schedule hereto governing the [XYZ ENTITY]'s activity in relation to the application of GDPR for the period from 1 January 20XX to 31 December 20XX.

4 Section Four: [XYZ ENTITY]'s descriptions, procedures and policies on its compliance with the GDPR CARP – Criteria.

Report on the [XYZ Entity]'s compliance with the GDPR CARP – Criteria identified in the schedule hereto governing the [XYZ ENTITY]'s activity in relation to the application of GDPR for the period from 1 January 20XX to 31 December 20XX.

CNPD Criteria			[XYZ ENTITY]'s descriptions, procedures and policies on its compliance with the GDPR CARP – Criteria	Independent auditor testing and results
Ref.	**Label**	**Policies and procedures (article 5-2)**	**Control objectives:** The entity has implemented organizational measures that ensure management is informed, involved and accountable for all decisions related to personal data processing activities.	
I-1	Accountability	The entity has implemented organizational measures that ensure management is **informed, involved and accountable for all decisions related to personal data processing activities**. Measures include, but are not limited to: — the implementation of appropriate data protection policies; — formal allocation of responsibilities; — formal reporting lines; — documentation of privacy decisions.	XYZ as formal data protection policies. General policies that apply to all processing activities are documented with the Risk management policies. Policies that relate to specific data processing activities by business are documented in the business policies. Management reviews design and application of policies once year and reports the results towards the board. Reporting lines for data protection issues are defined as follows: …..	...