Requirements for accreditation for certification bodies for GDPR-CARPA

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
1	**4**				**General requirements**	
1.1	**4.1**				**Legal and contractual matters**	
1.1.1	**4.1.1**				**Legal responsibility**	
1.1.1.1	4.1.1			CNPD	The certification body shall be a statutory audit firm approved by the CSSF and authorized to issue assurance reports as defined by the International Standard on Assurance Engagements ISAE 3000 (Assurance Engagements Other than Audits or Reviews of Historical Financial Information) issued by the International Auditing and Assurance Standards Board (IAASB).	A statutory audit firm approved by the CSSF (Commission de Surveillance du Secteur Financier, Luxembourgish supervisory authority for the financial sector) is a legal entity (which can be legally held responsible for its activities).
1.1.1.2				EDPB	The certification body shall be able to demonstrate to the CNPD its compliance to the requirements set out in this certification mechanism as well as the GDPR in its capacities both, as certification body as well as data controller / processor.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
1.1.2	**4.1.2**				**Certification agreement**	
1.1.2.1	4.1.2.1	27			The certification body shall have a written, legally enforceable agreement for the provision of certification activities to its clients. Certification agreements shall take into account the responsibilities of the certification body and its clients.	ISAE3000 explicitly states that a written agreement is necessary, which was not specified in ISO17065.
1.1.2.2	4.1.2.2				The certification body ensures its certification agreement requires that the client comply at least with the following: a) the client always fulfils the certification requirements, including implementing appropriate changes when they are communicated by the certification body; b) the client makes all necessary arrangements for i. the conduct of the evaluation and surveillance, including provision for examining documentation and records, and access to the relevant equipment, location(s), area(s), personnel, and client's subcontractors; ii. investigation of complaints; iii. the participation of observers (e.g. data protection supervisory authority representative); c) the client makes claims regarding certification consistent with the scope of certification; d) the client does not use its certification in such a manner as to bring the certification body into disrepute and does not make any statement regarding its certification that the certification body may consider misleading or unauthorized; e) upon suspension, withdrawal, or termination of certification, the client discontinues its use of all advertising matter that contains any reference thereto and takes action as required by the certification mechanism and takes any other required measure; f) if the client provides copies of the certification documents to others, the documents shall be reproduced in their entirety or as specified in the certification mechanism; g) in making reference to its certification in communication media such as documents, brochures or advertising, the client complies with the requirements of the certification body or as specified by the certification mechanism; h) the client complies with any requirements that may be prescribed in the certification mechanism relating to the use of marks of conformity, and on information related to the processing activities;	ISO17065 point 4.1.2.2 b) was removed as it applies to products and not processing activities.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					i) 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 i. takes appropriate action with respect to such complaints and any deficiencies found in processing activities that affect compliance with the requirements for certification; ii. documents the actions taken; j) the client informs the certification body, without delay, of changes that may affect its ability to conform with the certification requirements.	
1.1.2.3				EDPB, CNPD	The certification body shall demonstrate that its certification agreements: a) require the applicant to always comply with both the general certification requirements within the meaning of 1.1.2.2 and the criteria approved by the competent supervisory authority or the EDPB in accordance with Article 43 (2)(b) and Article 42(5); b) require the applicant to allow full transparency to the competent supervisory authority with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42(7) and 58(1)(c); c) do not reduce the responsibility of the applicant for compliance with Regulation 2016/679/EC and is without prejudice to the tasks and powers of the supervisory authorities which is competent in line with Article 42(5); d) require the applicant to provide the certification body with all information and access to its processing activities which are necessary to conduct the certification procedure pursuant to Article 42(6); e) require the applicant to comply with applicable deadlines and procedures. The certification agreement must stipulate that deadlines and procedures resulting, for example, from the certification programme or other regulations must be observed and adhered to; f) with respect to 1.1.2.2 and based on the GDPR-CARPA certification criteria set out the rules of validity, renewal, and withdrawal pursuant to Articles 42(7) and 43(4) including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7); g) allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8) and 43(5); h) include rules on the necessary precautions for the investigation of complaints within the meaning of 1.1.2.2, b(ii) & i, shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article. 43(2)(d); i) in addition to the minimum requirements referred to in 1.1.2.2, if the consequences of withdrawal or suspension of accreditation for the certification body impact on the client, in that case the consequences for the customer should all also be addressed j) require the applicant to inform the certification body in the event of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification.	Addition from annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
1.1.3	**4.1.3**				**Use of license, certificates and marks of conformity**	
1.1.3.1	4.1.3.1				The certification body shall exercise the control as specified by the certification mechanism over ownership, use and display of certificates, marks of conformity, and any other mechanisms for indicating a processing activity is certified.	
1.1.3.2	4.1.3.2			CNPD	The data protection certificates, seals and 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, shall be dealt with by suitable action, such as:	Addition of more specifications by the CNPD regarding actions the certification body can/should take.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					- 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 shall always be 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 the contract, legal proceedings might result in a court of law deciding what the corrective action will be.	
1.2	**4.2**				**Management of impartiality**	
1.2.1	4.2.1, 4.2.2, 4.2.5	21, 22, 69	21, 22		The certification body shall be responsible for the impartiality of its certification activities and shall not allow commercial, financial or other pressures to compromise impartiality. The certification body shall have top management commitment to impartiality. The certification body shall establish and communicate policies and procedures designed to provide it with reasonable assurance that the certification body, its personnel and, where applicable, others subject to independence requirements maintain independence. Such policies and procedures shall enable the certification body to identify and evaluate circumstances and relationships that create threats to independence, and to take appropriate action to eliminate those threats or reduce them to an acceptable level by applying safeguards, or, if considered appropriate, to withdraw from the engagement, where withdrawal is possible under applicable law or regulation. The policies and procedures shall stipulate that - the practitioner shall accept or continue an assurance engagement only when the practitioner has no reason to believe that relevant ethical requirements, including independence, will not be satisfied and - that the engagement partner shall be satisfied that appropriate procedures regarding the acceptance and continuance of client relationships and assurance engagements have been followed by the certification body, and shall determine that conclusions reached in this regard are appropriate. Such policies and procedures shall require: a) Engagement partners to provide the certification body with relevant information about client engagements, including the scope of services, to enable the certification body to evaluate the overall impact, if any, on independence requirements; b) Personnel to promptly notify the certification body of circumstances and relationships that create a threat to independence so that appropriate action can be taken; and c) The accumulation and communication of relevant information to appropriate personnel so that: i. The certification body and its personnel can readily determine whether they satisfy independence requirements; ii. The certification body can maintain and update its records relating to independence; and	The sentence “Certification activities shall be undertaken impartially. (4.2.1)” was removed as this is specified in subsequent criteria. Relevant sections (§3 and following) from ISAE3000 as well as ISQC1 regarding independence policies and procedures were added to provide more clarity.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					iii. The certification body can take appropriate action regarding identified threats to independence that are not at an acceptable level.	
1.2.2	4.2.12		24		All certification body personnel (either internal or external experts) or committees who could influence the certification activities shall act impartially. At least annually, the certification body shall obtain written confirmation of compliance with its policies and procedures on independence from all certification body personnel required to be independent by relevant ethical requirements.	Addition of a section from ISQC1 (second paragraph) to include a control to be performed by the certification body regarding independence.
1.2.3	4.2.3, 4.2.4, 4.2.11	52	25		The certification body shall identify risks to its impartiality on an ongoing basis. This shall include those risks that arise from its activities, from its relationships, or from the relationships of its personnel (see 1.2.12). In the case of a practitioner's external expert, the evaluation of objectivity shall include inquiry regarding interests and relationships that may create a threat to that expert's objectivity If a risk to impartiality is identified, the certification body shall be able to demonstrate how it eliminates or minimizes such risk. This information shall be made available to the mechanism specified in 2.2. The certification body shall take action to respond to any risks to its impartiality, arising from the actions of other persons, bodies or organizations, of which it becomes aware.	Removal of the sentence "However, such relationships may not necessarily present a certification body with a risk to impartiality" since it is evident. The risk analysis should include identified / potential risks. Addition of a second paragraph from ISAE3000 regarding external experts.
1.2.4	4.2.6			CNPD	The certification body and any part of the same legal entity and entities under its organizational control (see 4.5.4) shall not: a) be the designer, implementer, operator or maintainer of the certified process; b) offer or provide consultancy to its clients that impact the processing activity(ies) to be certified; c) offer or provide management system consultancy or internal auditing to its clients; d) be a processor and / or joint controller for an organization the certification body certifies with regard to the processing activities to be certified; e) Be involved in external DPO activities for the organization whose processing activities the certification body certifies.	The wording was adapted to processing activities instead of products/services.
1.2.5	4.2.7, 4.2.8				The certification body shall ensure that activities of separate legal entities, with which the certification body or the legal entity of which it forms a part has relationships, do not compromise the impartiality of its certification activities. When the separate legal entity offers or provides consultancy, the certification body's management personnel and personnel in the review and certification decision-making process shall not be involved in the activities of the separate legal entity. The personnel of the separate legal entity shall not be involved in the management of the certification body, the review, or the certification decision.	The wording was adapted to processing activities instead of products/services.
1.2.6	4.2.9				The certification body's activities shall not be marketed or offered as linked with the activities of an organization that provides consultancy. A certification body shall not state or imply that certification would be simpler, easier, faster or less expensive if a specified consultancy organization were used.	
1.2.7	4.2.10			CNPD	Within a period of 2 years, personnel shall not be used to review or make a certification decision for a processing activity for which they have provided consultancy.	The period was set to 2 years.
1.2.8	-		23		The certification body shall establish policies and procedures designed to provide it with reasonable assurance that it is notified of breaches of independence requirements, and to enable it to take appropriate actions to resolve such situations. The policies and procedures shall include requirements for: a) Personnel to promptly notify the certification body of independence breaches of which they become aware;	Additional requirement from the ISQC1 standard regarding the handling of impartiality breaches.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					b) The certification body to promptly communicate identified breaches of these policies and procedures to: i. The engagement partner who, with the certification body, needs to address the breach; and ii. Other relevant personnel in the certification body and, where appropriate, the network, and those subject to the independence requirements who need to take appropriate action; and c) Prompt communication to the certification body, if necessary, by the engagement partner and the other individuals referred to in subparagraph (b)(ii) of the actions taken to resolve the matter, so that the certification body can determine whether it should take further action.	
1.3	**4.3**				**Liability and financing**	
1.3.1	4.3.1			EDPB	The certification body has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations.	
1.3.2	4.3.2				The certification body has the financial stability and resources required for its operations.	
1.4	**4.4**				**Non-discriminatory conditions**	
1.4.1	4.4.1, 4.4.2, 4.4.3				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 as well asthose provided for in this certification mechanism. The certification body shall make its services accessible to all applicants whose activities fall within the scope of its operations. Access to the certification process shall not be subject to: - the size of the client; - membership of any association or group; - the number of certifications already issued; - undue financial or other conditions. 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 requirements, or similar client-related issues.	
1.4.2	4.4.4				The certification body shall confine its requirements, evaluation, review, decision and surveillance (if any) to those matters specifically related to the scope of certification.	
1.5	**4.5**				**Confidentiality**	
1.5.1	4.5.1		46		The certification body shall establish policies and procedures designed to maintain the confidentiality, safe custody, integrity, accessibility and retrievability of engagement documentation. The certification body shall be responsible, through legally enforceable commitments, for the management of all information obtained or created during the performance of certification activities. Except for information that the client makes publicly available, or when agreed between the certification body and the client (e.g. for the purpose of responding to complaints), all other information is considered proprietary information and shall be regarded as confidential. The certification body shall inform the client, in advance, of the information it intends to place in the public domain.	Addition of a section from ISQC1 (first paragraph) to underline the importance to establish relevant policies and procedures.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
1.5.2	4.5.2				When the certification body is required by law or authorized by contractual arrangements to release confidential information, the client or person concerned shall, unless prohibited by law, be notified of the information provided.	
1.5.3	4.5.3				Information about the client obtained from sources other than the client (e.g. from the complainant or from regulators) shall be treated as confidential.	
1.6	**4.6**				**Publicly available information**	
1.6.1				EDPB	The certification body shall maintain (through publications, electronic media or other means), and make available upon request, the following: a) information about as well as a reference to the CNPD website containing information regarding the certification mechanism, 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 the CNPD's certification mark and on the ways of referring to the certification granted; d) information about procedures for handling complaints and appeals.	
1.7					**Other general requirements**	
1.7.1				EDPB	The certification body shall establish policies and / or procedures to follow in case any changes occur that have an impact on its certification activities, especially those covered by the requirements set out in this certification mechanism (e.g. any changes in the legal framework, in the certification mechanism itself, the state of the art and the implementation costs of technical and organizational measures, etc.).	Addition from annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
1.7.2				EDPB	The certification body shall establish relevant procedures regarding the implementation of appropriate communication structures between the certification body and its clients in the context of: - information requests (status of a certification application, feedback / decisions taken by the CNPD, etc.); - complaints regarding a certification.	Addition from annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
2	**5**				**Structural requirements**	
2.1	**5.1**				**Organizational structure and top management**	
	5.1.1					This part was removed as it is covered by ISO 4.2 (CNPD 1.2).
2.1.1	5.1.2		16, 17, 30, 32, 33		The certification body shall document its organizational structure, showing duties, responsibilities and authorities of management and other certification personnel and any committees. When the certification body is a defined part of a legal entity, the structure shall include the line of authority and the relationship to other parts within the same legal entity. This documentation shall also include a description of duties, responsibilities and authorities of management in the context of the practitioner's system of quality control as specified in ISQC1.	Addition of a ISQC1 section (last paragraph) to detail the requirements regarding the documentation.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
2.1.2	5.1.3		16, 17, 30, 32, 33		The management of the certification body shall identify the board, group of persons, or person having overall authority and responsibility for each of the following: a) development of policies relating to the operation of the certification body; b) supervision of the implementation of the policies and procedures; c) supervision of the finances of the certification body; d) development of certification activities; e) evaluation (see 4.3); f) review (see 4.4); g) decisions on certification (see 4.5); h) delegation of authority to committees or personnel, as required, to undertake defined activities on its behalf; i) contractual arrangements; j) provision of adequate resources for certification activities; k) responsiveness to complaints and appeals; l) personnel competence requirements; m) management system of the certification body (see Clause 5); n) quality control system as specified in ISQC1.	Addition of a requirement to designate a person responsible for the quality control system as specified in ISQC1. Removal of point e) as the CNPD develops the certification requirements under GDPR-CARPA.
2.1.3	5.1.4				The certification body shall have formal rules for the appointment, terms of reference and operation of any committees that are involved in the certification process. Such committees shall be free from any commercial, financial and other pressures that might influence decisions. The certification body shall retain authority to appoint and withdraw members of such committees.	
2.2	**5.2**				**Mechanism for safeguarding impartiality**	
2.2.1	5.2.1				The certification body shall have a mechanism for safeguarding its impartiality. The mechanism shall provide input on the following: a) the policies and principles relating to the impartiality of its certification activities; b) any tendency on the part of a certification body to allow commercial or other considerations to prevent the consistent impartial provision of certification activities; c) matters affecting impartiality and confidence in certification, including openness.	
2.2.2	5.2.2				The mechanism shall be formally documented to ensure the following: a) a balanced representation of significantly interested parties, such that no single interest predominates; b) access to all the information necessary to enable it to fulfil all its functions	
2.2.3	5.2.3				If the top management of the certification body does not follow the input of this mechanism, the mechanism shall have the right to take independent action (e.g. informing the CNPD, stakeholders). In taking appropriate action, the confidentiality requirements of 1.5 relating to the client and certification body shall be respected. Input that is in conflict with the operating procedures of the certification body or other mandatory requirements should not be followed. Management should document the reasoning behind the decision to not follow the input and maintain the document for review by appropriate personnel.	
2.2.4	5.2.4				Although every interest cannot be represented in the mechanism, a certification body shall identify and invite significantly interested parties.	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
3	**6**				**Resource requirements**	
3.1	**6.1**				**Certification body personnel**	
3.1.1	**6.1.1**				**General**	
3.1.1.1	6.1.1.1	31 - 36	29		The certification body shall employ, or have access to, a sufficient number of personnel to cover its operations related to the certification mechanism. *Note: The personnel include those normally working for the certification body, as well as persons working under an individual contract or a formal agreement that places them within the management control and systems/procedures of the certification body (see 3.1.3).*	
3.1.1.2	6.1.1.2	31 - 39	29		The personnel shall be competent for the functions they perform, including making required judgments, defining policies and implementing them. The engagement partner shall have competence in assurance skills and techniques developed through extensive training and practical application and sufficient competence in the underlying subject matter and its measurement or evaluation to accept responsibility for the assurance conclusion as well as for the overall quality on the engagement. The engagement partner shall be satisfied that those persons who are to perform the engagement collectively have the appropriate competence and capabilities to perform the engagement in accordance with relevant standards and applicable legal and regulatory requirements, and enable an assurance report that is appropriate in the circumstances to be issued. The engagement partner shall be satisfied that the practitioner will be able to be involved in the work of a practitioner's expert where the work of that expert is to be used, and another practitioner, not part of the engagement team, where the assurance work of that practitioner is to be used, to an extent that is sufficient to accept responsibility for the assurance conclusion on the subject matter information.	Removal of the word "technical" as it is too specific; judgments in this context are not exclusively of a technical nature. Addition of ISAE3000 sections regarding competency requirements of the engagement partner as well as his or her engagement team in order to be more specific (as of second paragraph).
3.1.1.3	6.1.1.3				Personnel, including any committee members, personnel of external bodies, or personnel acting on the certification body's behalf, shall keep confidential all information obtained or created during the performance of the certification activities, except as required by law or by the certification mechanism.	
3.1.1.4				EDPB, CNPD	The certification body shall ensure that its personnel: a) has demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43(1); b) has independence and ongoing expertise with regard to the object of certification pursuant to Article 43(2)(a) and does not have a conflict of interest pursuant to Article 43(2)(e); c) undertakes to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b); d) has relevant and appropriate knowledge about and experience in applying data protection legislation; e) has relevant and appropriate knowledge about and experience in technical and organizational data protection measures as relevant; f) is able to demonstrate experience in the fields mentioned in the additional requirements a), d), e) specifically For personnel with technical expertise (internal as well as external experts) the certification body shall ensure that:	Addition from annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					- It has obtained a qualification in a relevant area of technical expertise to at least EQF[1] level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession or have significant professional experience; - personnel responsible for certification decisions has significant professional experience in identifying and implementing data protection measures; - personnel responsible for evaluations has professional experience in technical data protection and knowledge and experience in comparable procedure (e.g. certifications / audits), and registered as applicable. The certification body shall demonstrate that its personnel maintains domain specific knowledge in technical and audit skills through continuous professional development. For personnel with legal expertise (internal as well as external experts) the certification body shall ensure that: - it accomplished legal studies at a EU or state-recognised university for at least eight semesters including the academic degree Master (LL.M.) or equivalent, or significant professional experience; - personnel responsible for certification decisions has significant professional experience in data protection law and is registered as required by the Member State. - personnel responsible for evaluations has at least two years of professional experience in data protection law and knowledge and experience in comparable procedures (e.g. certifications/audits), and when required by the Member State is registered. The certification body shall demonstrate that its personnel maintain domain specific knowledge in technical and audit skills through continuous professional development. The certification body ensures that the individuals performing the mandatory engagement quality reviews (see point 4.4) demonstrate thorough experience in the domain of data protection.	
3.1.2	**6.1.2**				**Management of competence for personnel involved in the certification process**	
3.1.2.1	6.1.2.1			CNPD, EDPB	The certification body shall establish, implement and maintain a procedure for management of competencies of personnel involved in the certification process (see Clause 4). Certification body personnel as well as any member of committees, if applicable, should at least have the competencies outlined by the requirements defined in section 3.1.1. The procedure shall require the certification body to: a) determine the criteria for the competence of personnel for each function in the certification process, taking into account the requirements of the certification mechanism; b) identify training needs and provide, as necessary, training programmes on certification processes, requirements, methodologies, activities and other relevant certification mechanism requirements taking also into account point 1.7; c) demonstrate that the personnel have the required competencies for the duties and responsibilities they undertake; d) formally authorize personnel for functions in the certification process; e) monitor the performance of the personnel. The certification body shall develop a specific data protection training programme for the individuals involved in the attestation engagement. This programme must contain a component to validate the competences acquired by the personnel that followed the training programme (e.g. an exam).	Addition of competencies and training requirements. Addition from annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
3.1.2.2	6.1.2.2			CNPD	The certification body shall maintain the following records on the personnel involved in the certification process (see Clause 4):	The retention period has been changed from 3 to 5 years due to the general record retention period of 5 years for all certification-relevant documents (see further below).

[1] See qualification framework comparison tool at https://ec.europa.eu/ploteus/en/compare?

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					a) name and address; b) employer(s) and position held; c) educational qualification and professional status; d) experience and training; e) the assessment of competence; f) performance monitoring; g) authorizations held within the certification body; h) date of most recent updating of each record. Records shall be retained until 5 years after the last certification engagement the person has been involved in has expired.	
3.1.3	**6.1.3**				**Contract with the personnel**	
3.1.3.1					The certification body shall require personnel involved in the certification process to sign a contract or other document by which they commit themselves to the following: a) to comply with the rules defined by the certification body, including those relating to confidentiality (see 1.5) and independence from commercial and other interests; b) to declare any prior and/or present association on their own part, or on the part of their employer, with the client; c) to reveal any situation known to them that may present them or the certification body with a conflict of interest (see 1.2). Certification bodies shall use this information as input into identifying risks to impartiality raised by the activities of such personnel, or by the organizations that employ them (see 1.2.3).	Removal of parts under point b) to avoid narrowing down the application of this requirement too much. The interpretation of point b) should be broad.
3.2	**6.2**				**Resources for evaluation**	
3.2.1	**6.2.1**				**Internal resources**	
3.2.1.1		33, 34			When a certification body performs evaluation activities, either with its internal resources or with other resources under its direct control, it shall meet the applicable requirements of the relevant International Standards and, as specified by this certification mechanism, of other documents. The impartiality requirements of the evaluation personnel stipulated in the relevant standard shall always be applicable. Throughout the engagement, the engagement partner shall remain alert, through observation and making inquiries as necessary, for evidence of non-compliance with relevant ethical requirements by members of the engagement team. If matters come to the engagement partner's attention through the certification body's system of quality control or otherwise that indicate that members of the engagement team have not complied with relevant ethical requirements, the engagement partner, in consultation with others in the certification body, shall determine the appropriate action.	Removal of references to ISO/IEC 17025/17020/17021 as those requirements are covered by the ISAE3000 / ISQC1 as well as additional requirements. Addition of a part of ISAE3000 regarding the compliance to ethical requirements.
	6.2.2				**External resources (outsourcing)**	Outsourcing, as defined under the ISO17065 standard, is not permitted under GDPR-CARPA.
	6.2.2.1					
	6.2.2.2					

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
	6.2.2.3					
	6.2.2.4					
4	**7**				**Process requirements**	
	7.1				**General**	This section is not applicable to GDPR-CARPA as the CNPD provides the certification mechanism.
	7.1.1					
	7.1.2					
	7.1.3					
4.1	**7.2**				**Application**	
4.1.1	7.2			EDPB	For application, the certification body shall obtain all the necessary information to complete the certification process in accordance with the CARPA-GDPR certification mechanism. *Note: The following are examples of necessary information:* - *the processing activity(ies) to be certified as well as the object of certification (Target of Evaluation, ToE) must be described in detail in the application. This also includes interfaces and transfers to other systems and organizations, protocols and other assurances;* - *the application shall specify whether processors are used, and when processors are the applicant, their responsibilities and tasks shall be described, and the application shall contain the relevant controller/processor contract(s).* - *the general features of the client, including its name and the address(es) of its physical location(s), significant aspects of its process and operations (if required by the relevant certification mechanism), and any relevant legal obligations*	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) Irrelevant examples have been removed.
4.2	**7.3**				**Application review**	
4.2.1	7.3.1	23, 42		(EDPB)	The certification body shall conduct a review of the information obtained (see 4.1) to ensure that: a) the information about the client and the processing activity is sufficient for the conduct of the certification process; b) any known difference in understanding between the certification body and the client is resolved, including agreement regarding standards or other normative documents; c) the scope of certification sought is defined; d) the means are available to perform all evaluation activities; e) the certification body has the competence and capability to perform the certification activity. If it is discovered after the engagement has been accepted, that one or more preconditions (as set out by this certification mechanism as well as the International Standard on Assurance Engagements ISAE 3000) for an assurance engagement is not present, the practitioner shall discuss the matter with the appropriate party(ies), and shall determine: a) Whether the matter can be resolved to the practitioner's satisfaction; b) Whether it is appropriate to continue with the engagement; and c) Whether and, if so, how to communicate the matter in the assurance report. In this case the matter shall be escalated to the CNPD.	The addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) was not incorporated as: - with regard to point 1, point 1.1.2 defines the content of certification agreements, and - competence requirements are already covered in previous sections. Addition of relevant ISAE3000 sections regarding engagement acceptance.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					If the engagement partner obtains information that would have caused the certification body to decline the engagement had that information been available earlier, the engagement partner shall communicate that information promptly to the certification body, so that the certification body and the engagement partner can take the necessary action.	
	7.3.2					Section removed as it is already covered by 4.2.1.
	7.3.3					Section removed as it is already covered by 4.2.1.
	7.3.4					Section removed as it is already covered by 4.2.1.
	7.3.5					The basis for the certification decision under GDPR-CARPA are ISAE3000 assurance reports. Each ISAE3000 report is unique and cannot include a reference to another report. This means that if some testing can be "re-used" for a relevant report, the work needs to be documented again in full without referring to another report.
4.3	**7.4**				**Evaluation**	
4.3.1	7.4.1	40		CNPD	The certification body shall respect the requirements set out in the International Standard on Assurance Engagements ISAE 3000 (Assurance Engagements Other than Audits or Reviews of Historical Financial Information) issued by the International Auditing and Assurance Standards Board (IAASB) as well as the International Standard on Quality Control 1 (Quality Control for Firms that Perform Audits and Reviews of Financial Statement, and Other Assurance and Related Services Engagements). The certification body shall have a plan for the evaluation activities to allow for the necessary arrangements to be managed. The practitioner shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the engagement, and determining the nature, timing and extent of planned procedures that are required to be carried out in order to achieve the objective of the practitioner. The certification body involves at least one individual with legal or regulatory competencies and one individual with IT technical competencies in the attestation engagement (see point 3.1.1.4).	The ISO17065 part was replaced by the relevant passage from ISAE3000 as it is provides more information.
4.3.2	7.4.2			EDPB, CNPD	The certification body can use external experts for its evaluation activities should it lack the relevant competencies internally. The certification body shall ensure that in this case it complies with the requirements set out in this certification mechanism as well as with relevant laws and regulations. *Note: Outsourcing as defined by ISO17065 is not permitted under the GDPR-CARPA mechanism. The certification body can only use external experts for specific areas where it lacks relevant competencies.*	Removal of the entry as outsourcing as defined by ISO17065 is not allowed under GDPR-CARPA, which makes this requirement unnecessary. Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) Addition from the CNPD to stress the importance that external experts need to comply with the requirements of this certification mechanism
4.3.3	7.4.3	56, 60, 64, 65, 66			The certification body shall ensure all necessary information and/or documentation is made available for performing the evaluation tasks (the evaluation tasks can include activities such as design and documentation review, sampling, testing, inspection and audit). The practitioner shall request from the appropriate party(ies) a written representation: a) That it has provided the practitioner with all information of which the appropriate party(ies) is aware that is relevant to the engagement. b) Confirming the measurement or evaluation of the underlying subject matter against the applicable criteria, including that all relevant matters are reflected in the subject matter information.	Addition of relevant ISAE3000 sections regarding: - written representations; - the sufficiency and appropriateness of evidence; - material misstatements.

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					If one or more of the requested written representations are not provided or the practitioner concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations, or that the written representations are otherwise not reliable, the practitioner shall: a) Discuss the matter with the appropriate party(ies); b) Reevaluate the integrity of those from whom the representations were requested or received and evaluate the effect that this may have on the reliability of representations (oral or written) and evidence in general; and c) Take appropriate actions, including determining the possible effect on the conclusion in the assurance report. In this case the matter shall be escalated to the CNPD. The practitioner shall evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement and, if necessary in the circumstances, attempt to obtain further evidence. The practitioner shall consider all relevant evidence, regardless of whether it appears to corroborate or to contradict the measurement or evaluation of the underlying subject matter against the applicable criteria. The practitioner shall form a conclusion about whether the subject matter information is free of material misstatement. In forming that conclusion, the practitioner shall consider the sufficiency and appropriateness of evidence obtained as stated above and evaluate whether uncorrected misstatements are material, individually or in the aggregate. If the practitioner is unable to obtain sufficient appropriate evidence, a scope limitation exists and the practitioner shall express a qualified conclusion, disclaim a conclusion, or withdraw from the engagement, where withdrawal is possible under applicable law or regulation, as appropriate.	
4.3.4	7.4.4	63			The certification body shall carry out the evaluation activities that it undertakes with its internal resources (see 3.2.1) in accordance with the evaluation plan (see 4.3.1). The processing activities shall be evaluated against the requirements covered by the scope of certification and other requirements specified in the certification mechanism. *Note: The certification decision is based on the conclusions reached in the assurance report respecting the ISAE3000 standard (type 2). One of the conditions for a positive certification decision is that the practitioner expresses in this report a reasonable assurance that the subject matter information is prepared, in all material respects, in accordance with the applicable criteria.*	Removal of the outsourcing part as outsourcing as defined by ISO17065 is not allowed under GDPR-CARPA Addition of a note mentioning that under GDPR-CARPA the certification decision is based on the assurance report according to the standard ISAE3000
	7.4.5			EDPB		Please refer to the comment for ISO17065, section 7.3.5
4.3.5	7.4.6			EDPB	The certification body shall inform the client of all nonconformities. The certification body shall set out procedures defining how, when and what it will communicate to its client.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
	7.4.7					ISAE3000 rules apply
	7.4.8					ISAE3000 rules apply
4.3.6	7.4.9	79-83		EDPB, CNPD	The results of all evaluation activities shall be documented prior to review (see 4.4) and shall be made available to the CNPD upon request. The practitioner shall prepare on a timely basis engagement documentation that provides a record of the basis for the assurance report that is sufficient and appropriate to enable an experienced practitioner, having no previous connection with the engagement, to understand:	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) Addition of relevant extracts from ISAE3000 regarding documentation requirements

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					a) The nature, timing and extent of the procedures performed to comply with relevant ISAEs and applicable legal and regulatory requirements; b) The results of the procedures performed, and the evidence obtained; and c) Significant matters arising during the engagement, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions. If the practitioner identifies information that is inconsistent with the practitioner's final conclusion regarding a significant matter, the practitioner shall document how the practitioner addressed the inconsistency. The practitioner shall assemble the engagement documentation in an engagement file and complete the administrative process of assembling the final engagement file before the date of the assurance report. The signed ISAE 3000 type 2 assurance report is the result of the evaluation phase. **Requirements regarding the scope of the assurance report and the certification**: The objective of the assurance engagement is to have an engagement partner's opinion on the suitability of the design, implementation and operating effectiveness of the internal controls over data protection in relation to the CARPA framework. The assurance report must state the point in time or period of time to which the measurement or evaluation of the underlying subject matter relates. Defining the scope of the auditor's assurance engagement implies that an analysis be made to determine which services, business units, functional areas, and applications are likely to be relevant to the client's internal control over data protection. The assurance report shall also highlight the scope limitation, meaning the areas, which are not in scope of the engagement, so that the intended user understand its full implication. The scope description is: - specific; - detailed at process level; - clearly understandable to a third person. It should not be: - generic; - a description at firm level; - misleading.	
4.4	**7.5**				**Review**	
4.4.1	7.5.1			CNPD	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. This engagement quality review shall be mandatory and shall be carried out according to the requirements set out in the International Standard on Quality Control 1 (Quality Control for Firms that Perform Audits and Reviews of Financial Statement, and Other Assurance and Related Services Engagements).	Addition of the reference to ISQC1 regarding engagement quality reviews
4.4.2	7.5.2			EDPB	Recommendations for a certification decision, a successful certification review, a suspension or a revocation of a certification based on the review shall be documented, unless the review and the certification decision are completed concurrently by the same person.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
4.5	**7.6**				**Certification decision**	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
4.5.1	7.6.1			EDPB	The certification body shall be responsible for, and shall retain authority for, its decisions relating to certification. The certification body shall establish policies and procedures defining in detail how its independence and responsibility with regard to individual certification decisions are ensured.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
4.5.2	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 [e.g. a committee (see 2.1.3)] that has not been involved in the process for evaluation (see 4.3). *Note: The review and the certification decision can be completed concurrently by the same person or group of persons.*	
4.5.3	7.6.3				The person(s) [excluding members of committees (see 2.1.3)] assigned by the certification body to make a certification decision shall be employed by the certification body.	The certification decision should be taken by the certification body's own personnel as the certification body is responsible (4.5.1)
4.5.4	7.6.4				A certification body's organizational control shall be one of the following: - whole or majority ownership of another entity by the certification body; - majority participation by the certification body on the board of directors of another entity; - a documented authority by the certification body over another entity in a network of legal entities (in which the certification body resides), linked by ownership or board of director control.	
4.5.5	7.6.5				The persons employed by, or under contract with, entities under organizational control shall fulfil the same requirements of this certification mechanism as persons employed by, or under contract with, the certification body.	
4.5.6	7.6.6				The certification body shall notify the client of a decision not to grant certification, and shall identify the reasons for the decision.	
4.6	**7.7**				**Certification documentation**	
4.6.1	7.7.1			CNPD, EDPB	The certification body shall provide the client with formal certification documentation that clearly conveys, or permits identification of the following: a) the name and address of the certification body; b) the date certification is granted (starting the first day following the period under review); c) the name and address of the client; d) the scope of certification (i.e. the list of certified processing activities); e) the period of validity of the certification (including start and expiration date); f) the data protection mark and/or seal and the related rules of use; g) the unique certification ID, as well as any revision ID (see section 4.8), if applicable (indicated by "R" followed by the revision date: "RYYYYMMDD"); a mention of the possibility to access the ISAE assurance statement on requestThe certification body shall create the certificate according to the GDPR-CARPA template provided by the CNPD.	Additional GDPR-CARPA-specific requirements Additional requirements from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) are covered in other sections of this document
4.6.2	7.7.2				The formal certification documentation shall include the signature or other defined authorization of the person(s) of the certification body assigned such responsibility.	
4.6.3	7.7.3				Formal certification documentation (see 4.6) shall only be issued after, or concurrent with, the following: a) the decision to grant or extend the scope of certification (see 4.5.1) has been made;	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					b) certification requirements have been fulfilled; c) the certification agreement (see 1.1.2) has been completed/signed.	
4.6.4	-			CNPD	When a certificate is renewed after its initial validity period, a new certification ID provided by the supervisory authority will be issued. The supervisory authority keeps a record with information regarding all certificates granted to controllers and processors and their historical evolution.	Additional GDPR-CARPA-specific requirements
4.7	**7.8**				**Directory of certified processing activities**	
4.7.1				EDPB	The certification body shall maintain information on certified processing activities which contains at least the following: a) certification ID; b) identification of the client; c) identification of the scope (as defined in GDPR-CARPA); d) identification of the period covered; e) where relevant, comments regarding any changes on the certification status (e.g. suspension and reinstatement of a certificate, etc.). As a minimum, the certification body shall provide information, upon request, about the scope and validity of a given certification. The certification body shall keep the information on certified processing activities available. The certification body shall provide to the public upon request an executive summary of the evaluation report containing among others: a) the scope of the certification and a meaningful description of the object of certification; b) the respective certification criteria (including version or functional status); and c) the result(s). Pursuant to Article 43(5) GDPR, the certification body shall inform the competent supervisory authorities of the reasons for granting or revoking the requested certification.	Additional GDPR-CARPA-specific requirements Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), except point c) as this is already defined by GDPR-CARPA.
4.8	**7.9**				**Surveillance**	
	7.9.1					ISAE3000 and GDPR-CARPA rules apply
	7.9.2					ISAE3000 and GDPR-CARPA rules apply
	7.9.3					ISAE3000 and GDPR-CARPA rules apply
	7.9.4					ISAE3000 and GDPR-CARPA rules apply
4.9	**7.10**				**Changes affecting certification**	
4.9.1	7.10.1			EDPB	When the certification mechanism introduces new or revised requirements that affect the certified entities, the certification body shall ensure these changes are communicated to all clients. The certification body shall verify the implementation of the changes by its clients and shall take actions required by the certification mechanism and/or specified by the CNPD.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					Note: Changes affecting certification include among others: amendments to data protection legislation, the adoption of delegated acts of the European Commission in accordance with 43(8) and 43(9), decisions of the European Data Protection Board and court decisions related to data protection.	
4.9.2	7.10.2				The certification body shall consider other changes affecting certification, including changes initiated by the client, and shall decide upon the appropriate action, in accordance with the requirements set out in the International Standard on Assurance Engagements ISAE 3000 (Assurance Engagements Other than Audits or Reviews of Historical Financial Information). *Note: Changes affecting certification can include new information related to the fulfilment of certification requirements obtained by the certification body after certification has been established.*	Addition referring to the rules set out in the ISAE3000 standard
	7.10.3					See 4.9.2 (7.10.2)
4.10	**7.11**				**Termination, reduction, suspension or withdrawal of certification**	
4.10.1	7.11.1			EDPB	When a nonconformity with certification requirements is substantiated, either as a result of surveillance or otherwise, the certification body shall consider and decide upon the appropriate action in consultation with the CNPD. *Note: Appropriate action can include the following:* a) *continuation of certification under conditions specified by the certification body (e.g. increased surveillance);* b) *reduction in the scope of certification to remove nonconforming processing activities;* c) *suspension of the certification pending remedial action by the client;* d) *withdrawal of the certification.* The certification body shall inform the CNPD in writing without undue delay about measures taken in case of substantiated nonconformities with certification requirements.	Additional GDPR-CARPA requirements (prior consultation) Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
4.10.2	7.11.2				When the appropriate action includes evaluation, review or a certification decision, the requirements in 4.3, 4.4 or 4.5, respectively, shall be fulfilled.	
4.10.3	7.11.3				If certification is terminated (by request of the client), suspended or withdrawn, the certification body shall take actions specified by the certification mechanism 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. If a scope of certification is reduced, the certification body shall take actions specified by the certification mechanism 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.	
4.10.4	7.11.4				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 mechanism; - any other actions required by the certification mechanism. These persons shall be competent in their knowledge and understanding of all aspects of the handling of suspended certifications (see 3.1).	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
4.10.5	7.11.5				Any evaluations, reviews or decisions needed to resolve the suspension, or that are required by the certification scheme, shall be completed in accordance with the applicable parts of 4.3, 4.4, 4.5, 4.6.3, 4.8 and 6.10.3.	
4.10.6	7.11.6				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 continues to be certified. 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.	
4.11					**Renewal of a certification**	
4.11.1				CNPD	When a certificate is renewed after its initial validity period, a new certification ID provided by the supervisory authority will be issued. The supervisory authority keeps a record with information regarding all certificates granted to controllers and processors and their historical evolution.	Addition of a section regarding the renewal of a certificate after its validity period
4.12	**7.12**				**Records**	
4.12.1	7.12.1			EDPB, CNPD	The certification body shall retain records to demonstrate that all certification process requirements as per GDPR-CARPA have been effectively fulfilled (see also 5.3). The certification body shall keep records that are complete, comprehensible, up-to-date, accurate and available.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
4.12.2	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 (see also 1.5).	
4.12.3	7.12.3			CNPD	Records must be kept for five years starting from the date of the auditor's report.	The retention period for GDPR-CARPA is 5 years. Please also refer to the ISAE3000 standard (A200: […] "The retention period for assurance engagements ordinarily is no shorter than five years from the date of the assurance report.").
4.13	**7.13**				**Complaints and appeals**	
4.13.1	7.13.1		55	EDPB	The certification body shall have a documented process to receive, evaluate and make decisions on complaints and appeals originating from within or outside the certification body. The certification body shall record and track complaints and appeals, as well as actions undertaken to resolve them. The certification body shall specify: a) who can file complaints or objections; b) who processes them on behalf of the certification body; c) which verifications take place in this context; and d) the possibilities for consultation of interested parties. The certification Body shall maintain a record of all complaints it receives and the actions taken, which the CNPD can access at any time.	Addition of a specification regarding the origin of a complaint (ISQC1, A70) Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - 7.13 - 9.3.3: complaints are already mentioned in section 5 (formerly 8 under ISO17065) on management system requirements; only the last sentence was added
4.13.2	7.13.2			EDPB	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.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					The certification body shall specify: a) how and to whom such confirmation must be given; b) the respective time limits; and c) which processes are to be initiated afterwards.	
4.13.3	7.13.3				The certification body shall acknowledge receipt of a formal complaint or appeal.	
4.13.4	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.	
4.13.5	7.13.5			EDPB	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. The certification body shall establish relevant policies and procedures to ensure a separation between certification activities and the handling of appeals and complaints.	Addition from the annex 1 to the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
4.13.6	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.	
4.13.7	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.	
4.13.8	7.13.8				The certification body shall give formal notice of the outcome and the end of the appeal process to the appellant.	
4.13.9	7.13.9				The certification body shall take any subsequent action needed to resolve the complaint or appeal.	
5	**8**				**Management system requirements**	
	8.1				**Options**	Not applicable
	8.1.1					Not applicable
	8.1.2					Not applicable
	8.1.3					Not applicable
5.1	**8.2**				**General management system documentation**	
5.1.1	8.2.1				The certification body's top management shall establish, document, and maintain policies and objectives for fulfilment of this certification mechanism and shall ensure the policies and objectives are acknowledged and implemented at all levels of the certification body’s organization.	
5.1.2	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 mechanism.	
5.1.3	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:	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					a) ensuring that processes and procedures needed for the management system are established, implemented and maintained; b) reporting to top management on the performance of the management system and any need for improvement.	
5.1.4	8.2.4				All documentation, processes, systems, records, etc. related to the fulfilment of the requirements of this certification mechanism shall be included, referenced, or linked to documentation of the management system.	
5.1.5	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.	
5.2	**8.3**				**Control of documents**	
5.2.1	8.3.1		35		The certification body shall establish procedures to control the documents (internal and external) that relate to the fulfilment of this certification mechanism. The certification body shall establish policies and procedures requiring, for each certification engagement, an engagement quality control review that provides an objective evaluation of the significant judgments made by the engagement team and the conclusions reached in formulating the report.	Addition of the requirement to perform a mandatory engagement quality control for each engagement as set out in ISQC1
5.2.2	8.3.2		36		The procedures shall define the controls needed to: a) approve documents for adequacy prior to issue; b) review and update (as necessary) and re-approve documents; c) ensure that changes and the current revision status of documents are identified; d) ensure that relevant versions of applicable documents are available at points of use; e) ensure that documents remain legible and readily identifiable; f) ensure that documents of external origin are identified and their distribution controlled; g) prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose. The engagement report shall not be dated until the completion of the engagement quality control review (see point 4.4).	Addition of the ISQC1 requirement that the report can only be signed after completion of the engagement quality review, which is mandatory under GDPR-CARPA
5.3	**8.4**				**Control of records**	
5.3.1	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 mechanism.	
5.3.2	8.4.2				The certification body shall establish procedures for retaining records (see 4.12) for a period of five years from the date of the auditor's report. Access to these records shall be consistent with the confidentiality arrangements.	Addition of the GDPR-CARPA retention period requirement
5.4	**8.5**				**Management review**	
5.4.1	**8.5.1**				**General**	
5.4.1.1	8.5.1.1		48		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 mechanism.	Addition of the ISQC1 requirement regarding the ongoing consideration and evaluation of the certification body's system of quality control

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					This procedure shall also include an ongoing consideration and evaluation of the certification body's system of quality control including inspection of at least one completed engagement for each engagement partner and require that those performing the engagement or the engagement quality control review are not involved in inspecting the engagements.	
5.4.1.2	8.5.1.2				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.	
5.4.2	**8.5.2**				**Review inputs**	
5.4.2.1	8.5.2		49, 50		The input to the management review shall include information related to the following: a) results of internal and external audits as well as quality reviews; b) feedback from clients and interested parties related to the fulfilment of this certification mechanism; c) feedback from the mechanism for safeguarding impartiality; d) the status of preventive and corrective actions; e) follow-up actions from previous management reviews; f) the fulfilment of objectives; g) changes that could affect the management system; h) appeals and complaints.	The management review should also include information related to the quality reviews (ISQC1)
5.4.3	**8.5.3**				**Review outputs**	
5.4.3.1	8.5.3				The outputs from the management review shall include decisions and actions related to the following: a) improvement of the effectiveness of the management system and its processes; b) improvement of the certification body related to the fulfilment of this certification mechanism; c) resource needs.	
5.5	**8.6**				**Internal Audits**	
5.5.1	8.6.1				The certification body shall establish procedures for internal audits to verify that it fulfils the requirements of this certification mechanism and that the management system is effectively implemented and maintained.	
5.5.2	8.6.2				An audit programme shall be planned, taking into consideration the importance of the processes and areas to be audited, as well as the results of previous audits.	
5.5.3	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.	
5.5.4	8.6.4				The certification body shall ensure that: a) internal audits are conducted by personnel knowledgeable in certification, auditing and the requirements of this certification mechanism; b) auditors do not audit their own work; c) personnel responsible for the area audited are informed of the outcome of the audit;	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
					d) any actions resulting from internal audits are taken in a timely and appropriate manner; e) any opportunities for improvement are identified.	
5.6	**8.7**				**Corrective actions**	
5.6.1	8.7.1		49		The certification body shall establish procedures for identification and management of nonconformities in its operations. These procedures shall among others specify how the certification body shall evaluate the effect of deficiencies noted as a result of the monitoring process and determine whether they are either: a) Instances that do not necessarily indicate that the certification body's system of quality control is insufficient to provide it with reasonable assurance that it complies with professional standards and applicable legal and regulatory requirements, and that the reports as well as certificates issued by the certification body or engagement partners are appropriate in the circumstances; or b) Systemic, repetitive or other significant deficiencies that require prompt corrective action.	Addition of ISQC1 requirements specifying the procedures to establish.
5.6.2	8.7.2				The certification body shall also, where necessary, take actions to eliminate the causes of nonconformities in order to prevent recurrence.	
5.6.3	8.7.3		51, 52		Corrective actions shall be appropriate to the impact of the problems encountered. Recommendations for appropriate remedial actions for deficiencies noted shall include one or more of the following: a) Taking appropriate remedial action in relation to an individual engagement or member of personnel; b) The communication of the findings to those responsible for training and professional development; c) Changes to the quality control policies and procedures; and d) Disciplinary action against those who fail to comply with the policies and procedures of the certification body, especially those who do so repeatedly. The certification body shall establish policies and procedures to address cases where the results of the monitoring procedures indicate that a report may be inappropriate or that procedures were omitted during the performance of the engagement. Such policies and procedures shall require the certification body to determine what further action is appropriate to comply with relevant professional standards and applicable legal and regulatory requirements and to consider whether to obtain legal advice.	Addition of ISQC1 requirements and recommendations regarding corrective actions
5.6.4	8.7.4				The procedures for corrective actions shall define requirements for the following: a) identifying nonconformities (e.g. from complaints and internal audits); b) determining the causes of nonconformity; c) correcting nonconformities; d) evaluating the need for actions to ensure that nonconformities do not recur; e) determining and implementing the actions needed in a timely manner; f) recording the results of actions taken; g) reviewing the effectiveness of corrective actions.	
5.7	**8.8**				**Preventive actions**	
5.7.1	8.8.1				The certification body shall establish procedures for taking preventive actions to eliminate the causes of potential nonconformities.	
5.7.2	8.8.2				Preventive actions taken shall be appropriate to the probable impact of the potential problems.	

CARPA ref.	Ref. source documents				GDPR-CARPA requirements for accreditation description	Comments
	ISO	ISAE	ISQC1	Other		
5.7.3	8.8.3				The procedures for preventive actions shall define requirements for the following: a) identifying potential nonconformities and their causes; b) evaluating the need for action to prevent the occurrence of nonconformities; c) determining and implementing the action needed; d) recording the results of actions taken; e) reviewing the effectiveness of the preventive actions taken.	