Décision N° 14/2024 du 23 février 2024 de la Commission nationale pour la protection des données portant approbation des critères d'agrément des organismes de certification.

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après : « le RGPD ») ;

Vu la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après : « la Loi ») ;

Vu le règlement d'ordre intérieur de la Commission nationale pour la protection des données adopté par la décision n°07AD/2024 en date du 23 février 2024, notamment son article 31 ;

Vu l'article 42 paragraphe 5 du RGPD portant sur la certification délivrée par l'autorité de contrôle compétente ou les organismes de certification agrées par l'autorité de contrôle compétente ;

Vu l'avis 37/2023 du Comité européen de la protection des données (ci-après : « le CEPD ») relatif au projet de décision de l'autorité de contrôle luxembourgeoise portant sur l'approbation des critères d'agrément des organismes de certification conformément à l'article 43, paragraphe 3 du RGPD, adopté le 21 décembre 2023 ;

Considérant que l'article 58, paragraphe 3 du RGPD accorde à chaque autorité de contrôle une série de pouvoirs d'autorisation et de pouvoirs consultatifs ;

Considérant que la lettre e) de l'article 58, paragraphe 3 du RGPD prévoit plus précisément que chaque autorité de contrôle dispose du pouvoir d'agréer des organismes de certification en application de l'article 43 du RGPD ;

Considérant que l'article 43, paragraphe 3 du RGPD prévoit que chaque autorité de contrôle doit approuver les critères d'agrément des organismes de certification visés aux paragraphes 1 et 2 de l'article 43 du RGPD ;

Considérant que l'article 64, paragraphe 1, lettre c) du RGPD prévoit que chaque autorité de contrôle compétente doit communiquer pour avis un projet de décision au CEPD qui vise à approuver les critères d'agrément d'un organisme de certification en application de l'article 43, paragraphe 3 du RGPD ;

Considérant que l'article 12 de la Loi prévoit que la Commission nationale pour la protection des données (ci-après : « la CNPD ») dispose dans le cadre de ses missions de tous les pouvoirs prévus à l'article 58 du RGPD ;

Considérant que l'article 15 de la Loi prévoit que la CNPD doit agréer les organismes de certification ;

Considérant qu'en date du 21 décembre 2023, le CEPD a adopté un avis relatif au projet de décision sur les critères d'agrément des organismes de certification lui soumis par la CNPD ;

Considérant que conformément à l'article 10.7 du règlement intérieur du CEPD, la CNPD a soumis au CEPD le 20 février 2024 une mise à jour du projet de décision prenant en compte toutes les recommandations et tous les encouragements de l'avis précité du CEPD ;

Considérant que le CEPD a confirmé le même jour que la CNPD a bien tenu compte de l'avis du CEPD dans la mise à jour précitée de son projet de décision ;

Compte tenu des développements qui précèdent, la Commission nationale pour la protection des données, réunissant quatre Commissaires et délibérant à l'unanimité des voix,

Décide :

Art. 1er. – Approbation des critères d'agrément des organismes de certification

La CNPD approuve les critères d'agrément des organismes de certification, intitulés « Luxembourg accreditation requirements of certification bodies (art 43(1)(a)) – Set Beta », définis dans le document annexé et faisant partie intégrante de la présente décision.

Art. 2. – Applicabilité des critères d'agrément des organismes de certification

Les critères d'agrément des organismes de certification, approuvés par la présente décision, s'appliquent aux organismes de certification dont les activités portent sur des mécanismes et critères de certification identifiés par la CNPD sous le label « Set Beta » tel que défini dans le document annexé.

Ainsi décidé à Belvaux en date du 23 février 2024.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Marc Lemmer	Alain Herrmann
Présidente	Commissaire	Commissaire	Commissaire

LUXEMBOURG ACCREDITATION REQUIREMENTS OF CERTIFIFCATION BODIES (ART 43(1)(A)) - SET BETA

INTRODUCTION

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

In Luxembourg, the article 15 of the Act of 1 August 2018 on the organisation of the CNPD and the general data protection framework[1] has stipulated that certification bodies are to be accredited by the CNPD.

This document provides additional accreditation requirements to ISO/IEC 17065:2012[2] in accordance with Articles 43(1)(a) and 43(3) of the General Data Protection Regulation ("GDPR") and taking into account the EDPB guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)[3]. These additional accreditation requirements have been established by the *Commission nationale pour la protection des données* (CNPD) to provide a framework to assess the competence, consistent operation and impartiality of GDPR certification bodies.

Certification bodies that wish to provide certification services in the context of the GDPR-CARPA certification scheme (which is a Luxembourgish certification scheme) need to comply with the "Luxembourg accreditation requirements of certification bodies (art 43(1)(a)) – Set Alpha" as this set has been specifically tailored to this certification scheme. The accreditation requirements in this document are thus not applicable for the above-mentioned certification bodies.

1. SCOPE

The scope of these additional accreditation requirements shall be applied in accordance with the GDPR and further information is provided by the EDPB guidelines 4/2018 on accreditation and the EDPD Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation[4].

Pursuant to Article 42(1), GDPR certification can only be awarded in relation to controller and processor's personal data processing operations. A governance system cannot be the only element of a certification mechanism, it can only form a part of it.

2. NORMATIVE REFERENCE

GDPR has precedence over ISO standards. If a GDPR certification mechanism or accreditation requirements for certification bodies make a reference to other ISO standards, they shall be interpreted in line with the requirements set out in the GDPR.

3. TERMS AND DEFINITIONS

The terms and definitions of the GDPR (Art. 4), EDPB Guidelines on accreditation and EDPB Guidelines on certification shall apply and have precedence over ISO definitions.

---

[1] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données - https://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo

[2] SO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, processes and service

[3] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

[4] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

To facilitate a common understanding the main definitions are set out below:

- **'Accreditation'** means an attestation[5] by a national accreditation body and/or by a supervisory authority, that a certification body[6] is qualified to carry out certification pursuant to article 42 and 43 of the GDPR, taking into account ISO/IEC 17065:2012 and the additional requirements established by the supervisory authority and/or by the European Data Protection Board ("EDPB");
- **'Additional (accreditation) requirements'** means the requirements established by the competent supervisory authority against which an accreditation is performed[7] and which are defined in addition to the requirements set out in EN-ISO/IEC 17065/2012;
- **'Certification'** means the assessment[8] and impartial, third-party attestation that the fulfilment of certification criteria has been demonstrated;
- **'Certification body'** means a third-party conformity assessment body[9] operating a certification mechanism[10];
- **'Certification mechanism'** means a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply;
- **'Client'** means the controller or processor applying for certification of their processing operation(s);
- **'Criteria'** or **'certification criteria'** means the criteria against which a certification (conformity assessment) is performed[11];
- **'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);
- **'Target of Evaluation (ToE)'** means the object of certification. In the case of GDPR certification this will be the relevant processing operations, including the personal data processed, the technical systems used and the related processes and procedures, that the controller or processor is applying to have evaluated and certified.

4. ADDITIONAL ACCREDITATION REQUIREMENTS

This document follows the structure of ISO/IEC 17065/2012 and presents the requirements in table form:

- The column "Ref." contains the references for the respective ISO requirements.
- The column "Comment" contains explanations with regard to the relation the additional accreditation requirement has to the aforementioned ISO standard:
  - "Unchanged" means that the relevant ISO requirement applies and no additional requirements have been specified for this reference.
  - "Complement" means that the referenced ISO requirement has been completed with additional requirements.
  - "New" means that additional requirements with new references were added; those references are numbered in continuation of the existing ISO references.
  - "Not applicable" means that the relevant ISO requirement is not applicable for certification bodies.

[5] 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.
[6] Cf. with the definition of the term "accreditation" pursuant to ISO/IEC 17011:2017.
[7] Article 43(1)(b), 43(3), 43(6).
[8] 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/IEC 17000:2020, 2.4.
[9] See ISO/IEC 17000:2020, 2.5: "body that performs conformity assessment services"; ISO/IEC 17011:2017: "body that performs conformity assessment services and that can be the object of accreditation"; ISO/IEC 17065:2012, 3.12.
[10] Article 42(1), 42(5) GDPR.
[11] See Article 42(5).

- The column "Requirement description" contains the additional accreditation requirement.

Ref.	Comment	Requirement description
4		**General requirements**
4.1		**Legal and contractual matters**
4.1.1	Unchanged	**Legal responsibility**
4.1.1.1	New	The certification body shall be able to demonstrate to the CNPD its compliance to the ISO/IEC 17065/2012 requirements, the additional accreditation requirements, as well as the GDPR in its capacities both, as certification body as well as data controller / processor in the context of the certification activities.
4.1.2		**Certification agreement**
4.1.2.1	Complement	The legally enforceable agreement shall be in written form.
4.1.2.2	Complement	The certification body shall demonstrate in addition to the requirements 4.1.2.2 of ISO/IEC 17065:2012 that the certification agreement: a) require the client to always comply with both the general certification requirements within the meaning of 4.1.2.2 (a) of ISO/IEC 17065:2012 and the criteria approved by the CNPD or the EDPB in accordance with Article 43(2)(b) and Article 42(5) of the GDPR; b) require the client to allow full transparency to the CNPD with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42(7) and 58(1)(c) of the GDPR; c) do not reduce the responsibility of the client for compliance with the GDPR and is without prejudice to the tasks and powers of the CNPD which is competent in line with Article 42(5) of the GDPR; d) require the client 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) of the GDPR; e) require the client to comply with applicable deadlines and procedures. The certification agreement must stipulate that deadlines and procedures resulting, for example, from the certification program or other regulations must be observed and adhered to; f) set out, with respect to 4.1.2.2 (c)(1) of ISO/IEC 17065:2012, the rules of validity, renewal, and withdrawal pursuant to Articles 42(7) and 43(4) of the GDPR including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7) of the GDPR and section 7.9 of this document; g) allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8) and 43(5) of the GDPR; h) include rules on the necessary precautions for the investigation of complaints within the meaning of 4.1.2.2 (c)(2) of ISO/IEC 17065:2012 in a transparent and easily accessible manner. Additionally, 4.1.2.2(j) of ISO/IEC 17065:2012 shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article. 43(2)(d) of the GDPR;

Ref.	Comment	Requirement description
		i) in addition to the minimum requirements referred to in 4.1.2.2 of ISO/IEC 17065:2012, the certification agreement shall contain an explanation of the consequences of withdrawal or suspension of accreditation for the certification body and how this impacts the client; j) require the client 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; k) require the client to inform the certification body of any infringements of the GDPR or national data protection laws that may affect certification; l) set out the terms and conditions defining the duration of the certification procedure and binding evaluation methods with respect to the target of evaluation (ToE).
4.1.3		**Use of license, certificates and marks of conformity**
4.1.3.1	Complement	Certificates, seals and marks shall only be used in compliance with Articles 42 and 43 of the GDPR and the official EDPB guidelines on accreditation of certification bodies and certification.
4.1.3.2	Complement	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. Failure to comply with requirements of requirement 4.1.3.1 of ISO/IEC 17065:2012 shall be dealt with by suitable action, such as: • Taking any action to stop the misleading / wrong communication and thus removing the visibility of the data protection certificate, mark and seal; • Informing the public about the misuse; • Immediately informing the CNPD 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 processing activities.

Ref.	Comment	Requirement description
		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.
4.2		**Management of impartiality**
4.2.1	Complement	The certification body shall also ensure that: • it provides separate evidence of its independence in line with Article 43(2)(a) of the GDPR. This applies in particular to evidence concerning the financing of the certification body in so far as it concerns the assurance of impartiality; • it provides separate evidence that its tasks and obligations do not lead to a conflict of interest pursuant to Article 43(2)€ of the GDPR; • it does not have any relevant connection to the client it assesses and does not belong to the same company group nor be controlled in any way by the client it assesses. The certification body shall establish policies and procedures designed to provide it with reasonable assurance that the certification body, its personnel and, where applicable, others subject to impartiality requirements maintain impartiality and communicate these policies and procedures to all personnel taking part directly or indirectly in certification activities as well as the CNPD. Such policies and procedures shall enable the certification body to identify and evaluate circumstances and relationships that create threats to impartiality, 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 certification engagement.
4.2.2	Unchanged	
4.2.3	Unchanged	
4.2.4	Unchanged	
4.2.5	Unchanged	
4.2.6	Complement	Furthermore, the certification body and any part of the same legal entity and entities under its organisational control shall not: • be a processor and / or joint controller for a client with regard to the processing activities to be certified; • be involved in external DPO activities for the organization whose processing activities the certification body certifies.

Ref.	Comment	Requirement description
4.2.7	Unchanged	
4.2.8	Unchanged	
4.2.9	Unchanged	
4.2.10	Complement	The period referred to in the requirement of 4.2.10 of the ISO/IEC 17065:2012 shall be at least 2 years.
4.2.11	Complement	In addition, the certification body shall establish policies and procedures designed to provide it with reasonable assurance that it is notified of breaches of impartiality 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 impartiality breaches of which they become aware ; b) The certification body to promptly communicate identified breaches of these policies and procedures to : i. The lead auditor of the engagement 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 impartiality requirements who need to take appropriate action; and c) Prompt communication to the certification body, if necessary, by the lead auditor of the engagement 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.
4.2.12	Complement	Furthermore, at least annually, the certification body shall obtain written confirmation of compliance with its policies and procedures on impartiality from all certification body personnel required to be impartial.
4.3		**Liability and financing**
4.3.1	Complement	The certification body shall, in addition to the requirement 4.3.1 of ISO/IEC 17065:2012, ensure on a regular basis that: a) It has evaluated the financial risks related to its certification activities. b) It implemented appropriate measures (e.g. insurance or financial reserves) to cover liabilities arising from its operations and fields of activities in the geographical regions where it operates.
4.3.2	Unchanged	

Ref.	Comment	Requirement description
4.4	**Unchanged**	**Non-discriminatory conditions**
4.4.1	Unchanged	
4.4.2	Unchanged	
4.4.3	Unchanged	
4.4.4	Unchanged	
4.5		**Confidentiality**
4.5.1	Unchanged	
4.5.2	Unchanged	
4.5.3	Unchanged	
4.5.4	New	The certification body shall establish policies and procedures designed to maintain the confidentiality, integrity and availability of all documentation related to its certification activities.
4.6	Unchanged	**Publicly available information**
4.6.1	New	The certification body shall at minimum publish and make publicly available: a) all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) of the GDPR as well as all certification procedures, generally stating the respective period of validity; b) information about complaints handling procedures and appeals pursuant to Article 43(2)(d) of the GDPR.
4.7	**New**	**Other general requirements**
4.7.1	New	The certification body shall establish procedures regarding the implementation of appropriate communication structures between the certification body and its clients in the context of:

Ref.	Comment	Requirement description
		• information requests (status of a certification application, feedback / decisions taken as well as evaluations performed by the CNPD, etc.); • complaints regarding a certification.
4.7.2	New	The certification body shall have a procedure in place to inform the CNPD without delay of substantial changes that may affect its ability to conform with the accreditation requirements. Such substantial changes may include: a) a change in its legal, commercial, organizational or ownership status; b) a change in the organisation's senior management and key staff; and, or c) a change in its financial resources.
4.7.3	New	The certification body shall establish and implement procedures applying in the event of a suspension or the withdrawal of its accreditation, including among others the notification of clients.
4.7.4	New	The administrative language of the certification body is one of the following: Luxembourgish, French, German, English.
5	**Unchanged**	**Structural requirements**
5.1	**Unchanged**	**Organizational structure and top management**
5.1.1	Unchanged	
5.1.2	Unchanged	
5.1.3	Unchanged	
5.1.4	Unchanged	
5.2	**Unchanged**	**Mechanism for safeguarding impartiality**
5.2.1	Unchanged	
5.2.2	Unchanged	

Ref.	Comment	Requirement description
5.2.3	Unchanged	
5.2.4	Unchanged	
6		**Resource requirements**
6.1		**Certification body personnel**
6.1.1		**General**
6.1.1.1	Unchanged	
6.1.1.2	Unchanged	
6.1.1.3	Unchanged	
6.1.1.4	New	Furthermore, 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) of the GDPR; b) has independence and ongoing expertise with regard to the ToE pursuant to Article 43(2)(a) and do not have a conflict of interest pursuant to Article 43(2)(e) of the GDPR; c) undertakes to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b) of the GDPR; 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 organisational data protection measures as relevant ; f) is able to demonstrate experience in the fields mentioned in these additional requirements a), d), e), specifically for personnel mentioned in requirements 6.1.1.5 and 6.1.1.6.
6.1.1.5	New	For personnel with technical expertise (internal as well as external experts) the certification body shall ensure that: a) they have obtained a qualification in a relevant area of technical expertise to at least EQF level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession or have significant professional experience;

Ref.	Comment	Requirement description
		b) personnel responsible for certification decisions has significant professional experience in identifying and implementing data protection measures or equivalent (e.g. : significant experience in implementing laws and regulations, experience in compliance or in internal audit); c) personnel responsible for evaluations has professional experience in technical data protection or equivalent and knowledge and experience in comparable procedures (e.g. certifications / audits), and registered as applicable.
6.1.1.6	New	For personnel with legal expertise (internal as well as external experts) the certification body shall ensure that: a) they have 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; b) personnel responsible for certification decisions has significant professional experience in data protection law and is registered as required by the Member State. c) 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.
6.1.1.7	New	The certification body shall demonstrate that its personnel maintains domain specific knowledge in technical, legal and audit skills through continuous professional development.
6.1.1.8	New	The certification body shall ensure that the individuals performing the review (see section 7.5) demonstrate thorough experience in the domain of data protection.
6.1.2		**Management of competence for personnel involved in the certification process**
6.1.2.1	Unchanged	
6.1.2.2	Unchanged	
6.1.2.3	New	Certification bodies shall establish procedures to ensure the training of their employees with a view to updating their skills taking into account the developments listed in point 7.4.11 of this document.
6.1.3	Unchanged	**Contract with the personnel**
6.2		**Resources for evaluation**
6.2.1	Unchanged	Internal resources

Ref.	Comment	Requirement description
6.2.2		External resources (outsourcing)
6.2.2.1	Unchanged	
6.2.2.2	Unchanged	
6.2.2.3	Unchanged	
6.2.2.4	Unchanged	
6.2.2.5	New	If evaluation activities are outsourced to external bodies, the certification body, in addition to the requirements of section 6.2 of ISO/IEC 17065:2012, shall demonstrate that the conditions in point 6.1 of these requirements apply to personnel of this external bodies. *Note: Even when such activities are outsourced, the certification body will retain the responsibility for the decision-making.*
7		**Process requirements**
7.1		**General**
7.1.1	Unchanged	
7.1.2	Unchanged	
7.1.3	Unchanged	
7.1.4	New	The certification body shall have established procedures/mechanisms to inform the CNPD before granting, extending, renewing, or withdrawing/revoking the requested certification. The certification body shall provide to the CNPD the reasons for the relevant decision and a copy of the executive summary of the evaluation report mentioned in section 7.8. The purpose of this requirement is to increase transparency, and it does not entail a supervision of the draft approval.
7.1.5	New	In addition to the requirements of section 7.1 of ISO/IEC 17065:2012, the certification body shall: a) comply with the additional requirements of the competent supervisory authority (pursuant to Article 43(1)(a) of the GDPR) when submitting the application, in order that tasks and obligations do not lead to a conflict of interests pursuant to Article 43(2)(b) of the GDPR;

Ref.	Comment	Requirement description
		a) notify the relevant competent supervisory authorities before it starts operating an approved European Data Protection Seal in another member state from a satellite office.
7.2	Unchanged	**Application**
7.2.1	New	The certification body shall require that: a) the processing activity(ies) to be certified as well as the ToE must be described in detail in the application. This also includes interfaces and transfers to other systems and organizations, protocols and other assurances; b) the application shall specify whether processors are used, and when processors are the client, their responsibilities and tasks shall be described, and the application shall contain the relevant controller / processor contract(s) / contractual templates; c) in case a joint controller, in addition to the client, is responsible for parts of the personal data processing pursuant to Article 26(1) of the GDPR, the application shall specify the elements for which the client and other controllers are responsible and shall include the common understanding between the client and other controllers.
7.3		**Application review**
7.3.1	Unchanged	
7.3.2	Unchanged	
7.3.3	Unchanged	
7.3.4	Unchanged	
7.3.5	Unchanged	
7.3.6	New	The certification body shall ensure that: a) the assessment in 7.3.1(e) of ISO/IEC 17065:2012 takes into account both technical and legal expertise in data protection to an appropriate extent; b) the application review shall consider all the information referred to in point 7.2 of these requirements.
7.4		**Evaluation**

Ref.	Comment	Requirement description
7.4.1	Unchanged	
7.4.2	Complement	In addition to the requirement 7.4.2 of ISO/IEC 17065:2012, the evaluation may be carried out by sub-contractors who have been recognised by the certification body, using the same personnel requirements as those contained in section 6.1 of this document. The use of sub-contractors does not exempt the certification body from its responsibilities.
7.4.3	Unchanged	
7.4.4	Unchanged	
7.4.5	Complement	In addition to the requirement 7.4.5 of ISO/IEC 17065:2012, it shall be provided that existing certification in accordance with Articles 42 and 43 of the GDPR, which relates to the same ToE, may be taken into account as part of a new evaluation. However, existing data protection certification alone will not be sufficient evidence to completely or partially replace a certification body's own evaluation, and the certification body shall be obliged to check the compliance with the certification criteria to be applied in respect of the ToE. Recognition shall in any way require the preparation of a complete evaluation report or information enabling an evaluation of the previous certification activity and its results. A certification statement or similar certification certificates should not be considered sufficient to replace a report.
7.4.6	Complement	Furthermore, the certification body shall set out in detail how the information required in 7.4.6 informs clients about non-conformities with the certification scheme. In this context, at least the nature and timing of such information should be defined.
7.4.7	Unchanged	
7.4.8	Unchanged	
7.4.9	Complement	In addition, evaluation documentation shall be made fully accessible to the CNPD upon request.
7.4.11	New	Evaluation methods shall include, where applicable: **a)** a method for assessing the necessity and proportionality of processing operations in relation to their purpose and the data subjects concerned; **b)** a method for evaluating the coverage, composition and assessment of all risks considered by controller and processor with regard to the legal consequences pursuant to Articles 30, 32 and 35 and 36 GDPR, and with regard to the definition of technical and organisational measures pursuant to Articles 24, 25 and 32 GDPR, insofar as the aforementioned Articles apply to the ToE, and

Ref.	Comment	Requirement description
		c) a method for assessing the remedies, including guarantees, safeguards and procedures to ensure the protection of personal data in the context of the processing to be attributed to the ToE and to demonstrate that the legal requirements as set out in the criteria are met; and d) documentation of methods and findings. The certification body shall ensure that these evaluation methods are standardized and applied consistently. This means that comparable evaluation methods are used for comparable ToEs. Any deviation from this procedure shall be justified by the certification body. The certification body shall establish procedures to review these evaluation methods on a regular basis and to assess whether they need to be updated. An update must take place in the course of relevant changes such as changes in the legal framework, the applicable international standards, the relevant risk(s), the state of the art and the implementation costs of technical and organisational measures.
7.5		**Review**
7.5.1	Unchanged	
7.5.2	Unchanged	
7.5.3	New	The certification body shall define and implement procedures for the granting, regular review and revocation of the respective certifications pursuant to Articles 43(2) and 43(3) of the GDPR.
7.6		**Certification decision**
7.6.1	Complement	In addition, the certification body shall establish and implement policies and procedures defining in detail how its impartiality and responsibility with regard to individual certification decisions are ensured.
7.6.2	Unchanged	
7.6.3	Unchanged	
7.6.4	Unchanged	
7.6.5	Unchanged	
7.6.6	Unchanged	

Ref.	Comment	Requirement description
7.6.7	New	In addition to the checks carried out at application stage, prior to issuing or renewing certification, the certification body shall be required to confirm with the client that they are not the subject of any investigation or regulatory action by the CNPD, by any other supervisory authority and, or by competent judicial authorities in relation to the ToE which might prevent certification being issued.
7.7		**Certification documentation**
7.7.1	Unchanged	In addition to requirement 7.7.1.e of ISO/IEC 17065:2012 and in accordance with Article 42(7) GDPR, the period of validity of certifications shall not exceed three years. Furthermore, it shall be required that the period of the intended monitoring within the meaning of section 7.9 will also be documented. In addition to requirement 7.7.1.f of ISO/IEC 17065:2012, the certification body shall be required to name the ToE in the certification documentation (stating the version status or similar characteristics, if applicable).
7.7.2	Unchanged	
7.7.3	Unchanged	
7.8	Unchanged	**Directory of certified processing activities**
7.8.1	New	The certification body shall keep the information on certified processing activities available internally as well as externally by providing to the public an executive summary of the certification decision documentation containing among others: a) the name and contact details of the client, b) the scope of the certification and a meaningful description of the ToE; c) the respective certification criteria (including version or functional status); d) the evaluation methods and tests conducted, e) the result(s), f) the date of granting and the date of expiration of the current certification, and g) the initial and all re-certification dates.
7.9		**Surveillance**
7.9.1	Unchanged	

Ref.	Comment	Requirement description
7.9.2	Unchanged	
7.9.3	Unchanged	
7.9.4	Unchanged	
7.9.5	New	Surveillance activities shall be risk based and proportionate and the maximum period between surveillance activities shall not exceed twelve (12) months.
7.10		**Changes affecting certification**
7.10.1	Complement	Changes affecting certification to be considered by the certification body shall include: a) amendments to data protection legislation, b) the adoption of delegated acts of the European Commission in accordance with Articles 43(8) and 43(9) of the GDPR, c) documents or publications adopted by the European Data Protection Board, d) court decisions related to data protection, e) any personal data breach, or any infringement of GDPR and, or national data protection decisions established by the CNPD or by competent judicial authorities in relation to the subject matter of certification, reported either by the client or by the CNPD; and, or f) changes in the state-of-the-art technology, which was valid at the time of certification and had been taken into account in order to grant certification, has now become obsolete in the light of recent technological developments, insofar as relevant in relation to the ToEof the certification. The certification body shall define and implement procedures regarding such changes which shall take into account among others: a) transition periods, b) approvals process with the CNPD, c) reassessment of the relevant ToE, and d) appropriate measures to revoke the certification if the certified processing operation is no longer in compliance with the updated criteria.
7.10.2	Unchanged	
7.10.3	Unchanged	

Ref.	Comment	Requirement description
7.11		**Termination, reduction, suspension or withdrawal of certification**
7.11.1	Complement	Furthermore, the certification body shall be required to immediately inform the CNPD in writing without undue delay about measures taken and about continuation, restrictions, suspension and withdrawal of certification (see also requirement 7.1.4).
7.11.2	Unchanged	
7.11.3	Unchanged	
7.11.4	Unchanged	
7.11.5	Unchanged	
7.11.6	Unchanged	
7.11.7	New	According to Article 58(2) (h) of the GDPR, the certification body shall be required to accept decisions and orders from the CNPD to withdraw or not to issue certification to a client if the requirement for certification is not or no longer met. In such cases, the certification body shall provide clear and documented evidence to the CNPD that proper action has been taken.
7.12		**Records**
7.12.1	Unchanged	
7.12.2	Unchanged	
7.12.3	Unchanged	
7.12.4	New	The certification body shall keep all documentation complete, comprehensible, up-to-date and fit to audit.
7.12.5	New	Records must be kept at least for five years starting from the date of the auditor's report.
7.13		**Complaints and appeals**

Ref.	Comment	Requirement description
7.13.1	Complement	Furthermore, the certification body shall define, a) who can file complaints or objections, b) who processes them on the part of the certification body, c) which verifications take place in this context; and d) the possibilities for consultation of interested parties. In addition, the certification body must define how separation between certification activities and the handling of appeals and complaints is ensured.
7.13.2	Complement	Furthermore, the certification body shall define a) how and to whom such confirmation must be given, b) the time limits for this; and c) which processes are to be initiated afterwards.
7.13.3	Unchanged	
7.13.4	Unchanged	
7.13.5	Unchanged	
7.13.6	Unchanged	
7.13.7	Unchanged	Furthermore, the certification body shall define reasonable time limits for properly informing the complainants about the progress, the outcome and the end of the complaint process.
7.13.8	Unchanged	Furthermore, the certification body shall define reasonable time limits for properly informing the complainants about the progress, the outcome and the end of the complaint process.
7.13.9	Unchanged	
7.13.10	New	The certification body shall ensure that its complaints handling procedures are publicly available and easily accessible to data subjects.

Ref.	Comment	Requirement description
7.13.11	New	The certification body shall maintain a record of all complaints it receives and the actions taken, which the CNPD can access at any time.
8		**Management system requirements**
8.1		**Options**
8.1.1	Unchanged	**General**
8.1.2	Unchanged	**Option A**
8.1.3	Not applicable	**Option B** The requirements of section 8.1.3 of ISO/IEC 17065:2012 are not applicable.
8.2	Unchanged	**Management system documentation**
8.2.1	Unchanged	
8.2.2	Unchanged	
8.2.3	Unchanged	
8.2.4	Unchanged	
8.2.5	Unchanged	
8.3	Unchanged	**Control of documents**
8.3.1	Unchanged	
8.3.2	Unchanged	
8.4	Unchanged	**Control of records**

Ref.	Comment	Requirement description
8.4.1	Unchanged	
8.4.2	Unchanged	
8.5	Unchanged	**Management review**
8.5.1	Unchanged	**General**
8.5.1.1	Unchanged	
8.5.1.2	Unchanged	
8.5.2	Unchanged	**Review inputs**
8.5.3	Unchanged	**Review outputs**
8.6	Unchanged	**Internal Audits**
8.6.1	Unchanged	
8.6.6	Unchanged	
8.6.3	Unchanged	
8.6.4	Unchanged	
8.7	Unchanged	**Corrective actions**
8.7.1	Unchanged	
8.7.2	Unchanged	
8.7.3	Unchanged	

Ref.	Comment	Requirement description
8.7.4	Unchanged	
8.8	Unchanged	**Preventive actions**
8.8.1	Unchanged	
8.8.2	Unchanged	
8.8.3	Unchanged	