Additional Accreditation Requirements for Certification Bodies

8 December 2023

Version 1.2

URZĄD OCHRONY DANYCH OSOBOWYCH

Version 1.0	31 January 2022	Draft Additional Accreditation Requirements for Certification Bodies for the opinion of the EDPB
Version 1.1	31 January 2023	Draft Additional Accreditation Requirements for Certification Bodies after considering Opinion 11/2022 on the draft decision of the competent supervisory authority of Poland on the approval of the requirements for the accreditation of certification bodies in accordance with Article 43 (3) (GDPR), adopted by the European Data Protection Board on 4 July 2022
Version 1.2	8 December 2023	Additional Accreditation Requirements for Certification Bodies approved by the President of the Personal Data Protection Office after taking into account EDPB Opinion 11/2022 and updating the official journals of legal acts cited therein

Introduction

In accordance with recital 100 and Article 42 (1) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to with the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 04.05.2016, p. 1, as amended), hereinafter referred to as GDPR, the President of the Personal Data Protection Office (hereinafter the President of the Office) encourages the establishment of data protection certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with the GDPR. These certification mechanisms, as well as seals and marks, are intended not only to enable persons whose personal data will be processed to assess their level of protection quickly, but they will also allow obliged entities to implement appropriate technical and organisational measures within the meaning of the General Data Protection Regulation, including in particular, controllers and processors demonstrate compliance with the GDPR.

As part of the establishment of data protection certification mechanisms and data protection seals and marks, Article 43 (1) of the GDPR requires Member States to ensure that **Certification Bodies issuing certification under Article 42 (1) of the GDPR are accredited by either or both, the competent supervisory authority or the national accreditation body**. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied.

In Poland, in accordance with Article 12 (1) of the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws of 2019, item 1781) in conjunction with Article 43 (1)(b) of the GDPR **The Polish Centre for Accreditation (PCA)** is entitled to grant accreditation of Certification Bodies.

PCA is a national accreditation body authorised to accredit conformity assessment bodies on the basis of the Act of 13 April 2016 on conformity assessment and market surveillance systems (Journal of Laws of 2022, item 1854). This entity has the status of a state legal person and is supervised by the minister competent for economy.

In accordance with the Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93

L. 2008.218.30, as amended), PCA was designated as the only national accreditation body in the light of the above-mentioned Regulation.

In view of the above, the Polish Centre for Accreditation will grant accreditation of Certification Bodies on the basis of:

- ISO/IEC 17065/2012 and
- "Additional Accreditation Requirements for Certification Bodies" within the meaning of Article 43 (3) of the GDPR, defined by the President of the Office on the basis of the procedure laid down in the GDPR.

The content of the "Additional Accreditation Requirements for Certification Bodies" is set out in this document.

Certification Bodies will be accredited for a maximum period of five years.

The entity applying for accreditation within the meaning of Article 43 of the GDPR is obliged to contact the Polish Centre for Accreditation .

Terms of cooperation between the President of the Personal Data Protection Office and the Polish Centre for Accreditation as a national accreditation body within the meaning of Article 43 (1) (b) of the GDPR may be set out in a cooperation agreement as specified by Article 14 (5) of the Act on the Protection of Personal Data of 10 May 2018. This document may define the roles and responsibilities related to monitoring of activities of the Certification Bodies and mutual exchange of information concerning them. When concluded this document will be available both on the website of the Personal Data Protection Office and on the website of the Polish Centre for Accreditation.

The Polish Centre for Accreditation and Certification Bodies are obliged to indicate to the President of the Office the address of the electronic inbox within the meaning of Article 3 (17) of the Act of 17 February 2005 on the computerisation of the activities of entities carrying out public tasks (Journal of Laws of 2023, item 57 as amended) and use it in communication with the President of the Office related to the accreditation of Certification Bodies and certification.

§ 1.

Scope

This document sets out additional requirements to ISO/IEC 17065/2012 for the assessment of competence, consistent functioning and impartiality of Certification Bodies within the meaning of Article 42 (5) of the GDPR.

The scope of ISO/IEC 17065/2012 applies in accordance with the GDPR. For further information, see the European Data Protection Board's (EDPB) guidelines on accreditation[1] and certification[2].

The wide range of ISO/IEC 17065/2012, covering products, processes and services, should not lead to lowering or substitution of GDPR requirements. For example, the governance mechanism cannot be the only element of the certification mechanism, as certification in accordance with Article 42 (1) of the GDPR must cover personal data processing operations.

In accordance with Article 15 (1) of the Act of 10 May 2018 on the Protection of Personal Data certification shall be granted by the Certification Body upon request of:

- the controller,
- the processor,
- the manufacturer,
- or the entity marketing a service or product.

Manufacturers or entities marketing a service or product must have the status of controller or processor in the processing of personal data in which the service or product will be used. In accordance with Article 15 (2) of the Act of 10 May 2018 on the Protection of Personal Data, the principles set out in Article 42 of the GDPR, which specify the rules for the certification of personal data processing operations, prevail.

Certification mechanisms and data protection seals and marks issued to the relevant products and services covering personal data

[1] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en

[2] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en

processing operations will allow for a quick assessment of their level of data protection .

Scope of the certification mechanism (e.g. certification of cloud computing operations)
shall be taken into account in the assessment carried out by the accreditation body during the accreditation process, in particular with regard to criteria, expertise and assessment methodology.

§ 2.

Normative references

The provisions of the GDPR take precedence over ISO/IEC 17065/2012. If reference is made to other ISO standards in this document or in the certification mechanism, they should be interpreted in accordance with the requirements set out in the GDPR.

§ 3.

Terms and definitions

The terms and definitions of the guidelines on accreditation and certification shall apply and have precedence over ISO definitions. The main definitions used in this document are listed below.

1. **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (OJ L 119, 04.05.2016, p. 1, as amended);

2. **APPD** – Act of 10 May 2018 on the Protection of Personal Data (Polish Journal of Laws 2019, item 1781);

3. **Board** – European Data Protection Board;

4. **Board's Guidelines on Accreditation** – Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR (2016/679);

5. **Board's Guidelines on Certification** – Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679;

6. **Supervisory Authority** – President of the Personal Data Protection Office;

7. **PCA - Polish Centre for Accreditation** – national accreditation body, the sole body in the Member State designated in accordance with the Regulation (EC) No 765/2008 of the European Parliament and of the Council, which carries out accreditation on the basis of an authorisation from the State;

8. **Certification** – assessment and impartial third party attestation that the fulfilment of certification criteria has been demonstrated in relation to the processing operations carried out by the controller or processor;

9. **Accreditation** – attestation by the Polish Centre for Accreditation that the Certification Body is qualified to conduct certification in accordance with Articles 42 and 43 of the GDPR, taking into account ISO/IEC 17065/2012 and these additional requirements established by the supervisory authority or the Board. For more information on the interpretation of accreditation for the purposes of Article 43 GDPR, see Section 3 of the Board's Guidelines on Accreditation;

10. **Certification Body** – body operating the certification scheme, including the conformity assessment of the Target of Evaluation;

11. **Certification criteria** – criteria against which the assessment of processing operations carried out by the Applicant or Customer for the certification scheme concerned is performed;

12. **Certification scheme** – system relating to specific products, processes and services to which the same requirements, specific rules and procedures apply. It shall include certification criteria and assessment methodology;

13. **Certification mechanism** – approved certification scheme that is available for the Applicant. It is a service provided by an accredited Certification Body based on approved criteria and assessment methodology. It is a system, by which the Applicant obtains certification;

14. **Target of Evaluation** – object of certification. In the case of GDPR certification, these will be the relevant processing operations requested by the Applicant for evaluation and certification.

15. **Applicant —** the controller or processor that applied for certification of its processing operations.

16. **Customer** - entity that has been certified (previously the Applicant).

§ 4.

General requirements for accreditation

4.1. Legal and contractual matters

4.1.1. Legal responsibility

1. The Certification Body must always be able to demonstrate to the PCA that it has up-to-date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation, including the additional requirements in respect of the application of the GDPR.

2. The Certification Body must be able to demonstrate that its procedures and measures concerning, in particular, the control and processing of personal data of the Applicant and the Customers' organisation as part of the certification process comply with GDPR and APPD. Therefore, as part of the accreditation procedure, the Certification Body is required to provide evidence of compliance required during the accreditation process.

3. The evidence of compliance referred to in point 2 shall, in particular, include the demonstration by the Certification Body that the above-mentioned procedures and measures used in the certification process are not and have not been the subject of proceedings before the Supervisory Authority.

4. Before proceeding with the accreditation process, the PCA shall contact the Supervisory Authority to verify the information referred to in point 3. Where appropriate the Supervisory Authority shall verify that information.

5. The Certification Body also confirms to the PCA that its procedures and measures relating in particular to controls and the processing of personal data of Applicants and Customers' organisations as part of the certification process are implemented and followed and are not and have not been the subject of proceedings of other supervisory authorities in other

sectors if those proceedings concern the processing of personal data and may result in the Certification Body not complying with this requirement and may therefore prevent its accreditation.

6. The Certification Body immediately informs the PCA of infringements of the GDPR or APPD established by the Supervisory Authority, supervisory authorities in other sectors or competent judicial authorities which may affect its accreditation.

7. Before issuing or renewing or refusing certification, the Certification Body shall be obliged to inform the Supervisory Authority in accordance with Article 43 (1) of the GDPR and Article 19 of the APPD.

8. The Supervisory Authority may establish further requirements and procedures to verify compliance of Certification Bodies with GDPR prior to accreditation.

4.1.2 Certification agreement

In addition to the requirements of ISO/IEC 17065/2012, the Certification Body shall demonstrate that its certification agreement referred to in Article 15 (3) of the APPD:

1. requires the Applicant to always comply with both the general certification requirements within the meaning of point 4.1.2.2(a) of ISO/IEC 17065/2012, as well as the criteria approved by the Supervisory Authority or the Board in accordance with Article 43 (2) (b) and Article 42 (5) of the GDPR,

2. requires the Applicant to allow full transparency to the Supervisory Authority with respect to the certification procedure, including matters covered by the contractual provisions on confidentiality regarding data protection, in accordance with Article 42 (7) and Article 58 (1) (c) of the GDPR,

3. does not reduce the Applicant's liability for compliance with GDPR and is without prejudice to the tasks and powers of the supervisory authorities, which are competent in accordance with Article 42 (5) of the GDPR,

4. requires the Applicant to provide the Certification Body with all information and access to its processing activities which are necessary to conduct the certification procedure in accordance with Article 42 (6) GDPR,

5. requires the Applicant to comply with the applicable deadlines and procedures — the certification agreement must provide for appropriate deadlines and procedures to be complied with by the Applicant, certification program and other regulations must be observed and adhered to,

6. with reference to point 4.1.2.2(c)(1) of ISO/IEC 17065/2012, sets out the rules of validity, renewal and withdrawal in accordance with Article 42 (7) and Article 43 (4) of the GDPR, including rules setting appropriate intervals for re-evaluation or review (regularity) in accordance with Article 42 (7) of the GDPR and clause 7.9 of these requirements,

7. allows the Certification Body to disclose to the Supervisory Authority all information necessary to grant the certification in accordance with Article 42 (8) and Article 43 (5) of the GDPR,

8. contains provisions on the necessary precautions with regard to the handling of complaints within the meaning of point 4.1.2.2 (c) (2) and (j) of ISO/IEC 17065/2012, shall also contain explicit statements on the structure and procedure for handling complaints in accordance with Article 43 (2) (d) GDPR,

9. in addition to the minimum requirements referred to in point 4.1.2.2 of ISO/IEC 17065/2012, indicates the consequences for the Customer in the event of withdrawal or suspension or refusal to issue an accreditation for the Certification Body. In particular, the Customer shall be informed of the conditions applicable to the transfer of certification and of the procedure to be followed when the accreditation of Certification Body is refused, suspended or withdrawn in respect of an approved certification mechanism under Article 42 of the GDPR,

10. obliges the Applicant to inform the Certification Body of any significant changes in its factual or legal situation and changes to the products, processes and services covered by the certification,

11. includes binding evaluation methods with respect to the Target of Evaluation.

4.1.3 Use of data protection seals and marks

Certificates, seals and marks shall only be used in accordance with Articles 42 and 43 of the GDPR and the Board's Guidelines on Accreditation and Certification.

4.2. Management of impartiality

The PCA shall ensure that in addition to the requirement set out in point 4.2 of ISO/IEC 17065/2012:

1. The Certification Body complies with the additional requirements of the Supervisory Authority (according to Article 43 (1) (b) of the GDPR)

   a) in accordance with Article 43 (2) (a) of the GDPR the Certification Body must provide separate evidence of its independence. This applies in particular to evidence concerning the financing of the Certification Body in so far as it concerns the assurance of impartiality,

   b) the tasks and obligations of the Certification Body do not lead to a conflict of interest in accordance with Article 43 (2) (e) of the GDPR,

2. The Certification Body hasno significant connection with the Customer being assessed (e.g. the Certification Body may not belong to the same group of enterprises, the Certification Body may not in any way be controlled by the Customer whom it assesses). Any economic links between the Certification Body and the Applicant, depending on its characteristics, may affect the impartiality of its certification activities.

4.3. Liability and financing

In addition to the requirement set out in point 4.3.1 of ISO/IEC 17065/2012, the PCA shall ensure on a regular basis that the Certification Body has appropriate measures (e.g. insurance or reserves) to cover its liabilities in geographical regions in which operates.

4.4. Non-discriminatory conditions

The requirements of ISO/IEC 17065/2012 shall apply.

4.5. Confidentiality

The requirements of ISO/IEC 17065/2012 shall apply.

4.6. Publicly available information

In addition to the requirement set out in point 4.6 of ISO/IEC 17065/2012, the PCA shall require the Certification Body, at minimum, that:

1. all versions (current and previous) of the approved criteria used within the meaning of Article 42 (5) of the GDPR (certification criteria) are published and easily publicly available, as well as all certification procedures, generally stating a relevant period of validity;

2. information on complaint and appeal procedures are made public in accordance with Article 43 (2) (d) of the GDPR.

§ 5.

Structural requirements, Article 43 (4) GDPR

(“proper assessment”)

5.1. Organisational structure and top management

The requirements of ISO/IEC 17065/2012 shall apply.

5.2. Mechanisms for safeguarding impartiality

The requirements of ISO/IEC 17065/2012 shall apply.

§ 6.

Resource requirements

6.1 Certification Body personnel

In addition to the requirement in Section 6 of ISO/IEC 17065/2012, the PCA shall ensure for each Certifying Body that its personnel performing the certification compliance tasks:

1. has demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43 (1) of the GDPR,

2. has independence and ongoing expertise with regard to the Target of Evaluation pursuant to Article 43 (2)(a) of the GDPR and do not have a conflict of interest pursuant to Article 43 (2)(e) of the GDPR,

3. undertakes to respect the criteria referred to in Article 42 (5) pursuant to Article 43 (2)(b) GDPR,

4. has relevant and appropriate knowledge about and experience in applying data protection legislation,

5. has relevant and appropriate knowledge about and experience in technical and organisational data protection measures as relevant,

6. has been able to demonstrate experience in the areas referred to in points 6.1(1), (4) and (5), in particular:

    a) personnel with technical expertise:

        - have obtained qualifications in a relevant area of technical expertise to at least level 6 according to the European Qualifications Framework or a recognised protected title (e.g. engineering diploma) in a relevant regulated profession or must have significant professional experience,

        - in addition, the personnel responsible for certification decisions must have significant professional experience in data protection law, including identifying and implementing data protection measures or access to a person with that knowledge and relevant professional qualifications / post-graduate level education,

        - in addition, personnel responsible for evaluations must have professional experience in technical data protection measures and knowledge and experience in comparable procedures (e.g. certification/audits) and, where applicable, demonstrate registration.

The personnel shall demonstrate that they maintain expertise in technical and audit skills through continuous professional development.

b) personnel with legal expertise:

- have completed legal studies at an EU or national recognised university lasting at least eight semesters and have obtained a master's degree in law or an equivalent degree, or have significant professional experience,
- in addition, personnel responsible for certification decisions shall demonstrate significant professional experience in data protection law, including implementing and identifying data protection measures and be registered as required by the Member State,
- in addition, personnel responsible for evaluations shall demonstrate their possession at least two years of professional experience in data protection law and knowledge and experience in comparable procedures (e.g. certification/audit) and be registered if required by the Member State concerned.
    - personnel shall demonstrate that they maintain expertise in technical and audit skills through continuous professional development.

The Certification Body shall be able to identify and explain to the PCA which professional experience and expertise requirements are appropriate to the scope of the certification scheme and the given Target of Evaluation.

The Certification Body is fully responsible for making decisions even if it is assisted by subcontractors.

Subcontractors must not be involved in decision-making processes.

Subcontractors shall meet the requirements laid down for the Certification Body's personnel.

6.2 Resources for evaluation

The requirements of ISO/IEC 17065/2012 shall apply.

§ 7.

Process requirements, Article 43 (2)(c) and (d) of the GDPR

7.1 General guidelines

In addition to the requirement set out in Section 7.1 of ISO/IEC 17065/2012, the PCA shall ensure that:

1. when submitting the application, the Certification Bodies comply with these additional requirements of the Supervisory Authority (in accordance with Article 43 (1) (b) of the GDPR) so that the tasks and obligations performed in connection with the granting of accreditation do not lead to a conflict of interest in accordance with Article 43 (2) (e) of the GDPR;

2. if the Certification Body intends to act in other Member States from a satellite office, it shall notify and, when necessary, obtain the necessary approval from the relevant competent authorities, including for the operation of a European Data Protection Seal in accordance with Article 42(5) of the GDPR[3];

3. Certification Bodies have procedures in place to notify the Supervisory Authority immediately prior to the issue, renewal or withdrawal of the certification and they shall state the reasons for such action. This includes providing the Supervisory Authority with a copy of the summary of the assessment report referred to in point 7.8 of this document;

4. in case the Customer or the Supervisory Authority notifies the Certification Bodies about any significant investigations or regulatory activities of the Supervisory Authority or other supervisory authorities in other sectors, linked to the scope of the certification and Target of Evaluation, which undermine the Customer's compliance with data protection, the Certification Bodies are obliged to assess whether the Customer still meets the certification criteria. The Certification Bodies shall provide the Supervisory Authority with a report containing information on the results of that assessment. The assessment will relate to the scope of the certification and the Target of Evaluation.

[3] See in this regard the Board's Guidelines on Certification, paragraph 44.

7.2. Application

In addition to the requirements set out in Article 17 of the APPD and point 7.2 of ISO/IEC 17065/2012, the Certification Body shall require that the application for certification:

1. includes a detailed description of the Target of Evaluation, including interfaces and transfers to other systems and organisations, protocols and other assurances;

2. specifies whether the Applicant uses the services of processors and, if the Applicant is a processor, its responsibilities and tasks shall be described, and the application shall be accompanied by a contract/s between the controller and the processor (certified copies);

3. determines whether the joint controllers are involved in the processing of personal data and whether the joint controller is the Applicant — in such a situation the its responsibilities and tasks shall be described and the application shall be accompanied by a joint controllership agreement (certified copy);

4. discloses any ongoing or recent proceedings or regulatory activities carried out by the Supervisory Authority or supervisory authorities in other sectors to which the Applicant is subject, where those proceedings or regulatory actions concern the processing of personal data related to the scope of the certification and the Target of Evaluation.

The Certification Body is obliged to inform the Supervisory Authority about the receipt of an application in order to enable it to carry out tasks arising from the GDPR and APPD.

7.3. Application review

In addition to the requirements of point 7.3 of ISO/IEC 17065/2012 the PCA requires that:

1. the certification agreement sets out binding assessment methods with respect to the Target of Evaluation,

2. the assessment of sufficient expertise, as provided for in point 7.3(e) of ISO/IEC 17065/2012, takes into account, to an appropriate extent, both technical and legal expertise in the field of data protection.

7.4. Evaluation

In addition to the requirements set out in point 7.4 of ISO/IEC 17065/2012, certification mechanisms shall specify sufficient methods for assessing the compliance of processing operations with the certification criteria, including areas such as:

1. a method for assessing the necessity and proportionality of the processing operations in relation to their purpose and the concerned data subjects,

2. a method for evaluating the coverage, composition and assessment of all risks considered by the controller and processor, with regard to legal consequences in accordance with Articles 30, 32, 35 and 36 of the GDPR and with regard to the definition of technical and organisational measures in accordance with Articles 24, 25 and 32 of the GDPR, insofar as the above-mentioned Articles apply to the Target of Evaluation,

3. a method for assessing the remedies, including guarantees, safeguards and procedures to ensure the protection of personal data in the context of processing,
   to be attributed to the Target of Evaluation and to demonstrate that the legal requirements as set out in the adopted criteria are met, and

4. documentation of methods and findings.

The Certification Body is required to ensure standardisation and consistent application of assessment methods. This means using comparable assessment methods to comparable targets of evaluation. Any deviation from this procedure shall
be justified by the Certification Body.

In addition to the requirements set out in point 7.4.2 of ISO/IEC 17065/2012, the assessment may be carried out by subcontractors who have been recognised by the Certification Body, applying the same personnel requirements set out in § 6 of this document.

In addition to point 7.4.5 of ISO 17065, it should be provided that existing certification, regarding data protection in line with Article 42 and 43 GDPR, which already includes the part of the Target of Evaluation, may be taken into account in a new assessment, but is not sufficient to completely replace partial evaluations. However, the certificate itself will not be a sufficient proof and the Certification

Body shall be obliged to verify compliance with the criteria in relation to the object of the assessment. In order to take an informed decision, the full assessment report and other relevant information enabling the assessment of the existing certification and its results shall be taken into account. A certification statement or similar certification certificates should not be considered sufficient to replace a report.

In cases where an existing certification is taken into account in a new assessment, the scope of that certification should also be assessed in detail for its conformity with the relevant certification criteria.

In addition to point 7.4.6 of ISO/IEC 17065/2012, the Certification Body shall specify in detail in its certification scheme how the information required by ISO/IEC 17065/2012 allows the Customer (Applicant) to be aware of the non-conformities in relation to to the certification mechanism. In this context, at least the nature and timing of such information should be defined. The Certification Body shall indicate this in a written document which may be a certification scheme or, if the Certification Body is not the owner of the system, another document relating to the certification process.

In addition to point 7.4.9 of ISO/IEC 17065/2012, the Certification Body shall provide the Supervisory Authority with full access to the documentation of the Applicant's assessment.

7.5. Review

In addition to point 7.5 of ISO/IEC 17065/2012, the Certification Body shall specify the procedures for the granting, regular review and revocation of the relevant certifications in accordance with Article 43 (2) and (3) of the GDPR.

The Certification Body shall provide the Supervisory Authority with full access to the Customer's documentation related to the granting, review and revocation of certification.

7.6. Certification decision

In addition to point 7.6.1 of ISO/IEC 17065/2012, the Certification Body is required to specify in detail in its procedures how its independence and responsibility have been ensured in relation to each certification decision.

7.7. Certification documentation

In addition to point 7.7.1(e) of ISO/IEC 17065/2012 and in accordance with Article 42 (7) GDPR it is required that the period of validity of certifications does not exceed three years.

In addition to point 7.7.1(e) of ISO/IEC 17065/2012, documentation of the period of intended monitoring within the meaning of point 7.9 of this document is also required.

In addition to point 7.7.1(f) of ISO/IEC 17065/2012, the Certification Body is required to indicate the Target of Evaluation in the certification documentation (indicating the status of the version or similar characteristics, if applicable).

When issuing the certificate, the Certification Body shall provide the Supervisory Authority with a copy of the certification documentation referred to in point 7.7.1 of ISO/IEC 17065/2012.

7.8. Directory of certified products

In addition to point 7.8 of ISO/IEC 17065/2012, the Certification Body is obliged to maintain the internal and public availability of information on certified products, processes and services.

The Certification Body shall make publicly available an executive summary of the evaluation report, to ensure transparency as to the Target of Evaluation and the way in which it is assessed. The summary shall include, inter alia:

a) the scope of the certification and a meaningful description of the object of certification (Target of Evaluation),

b) the relevant certification criteria (specifying version or functional status),

c) the methods and tests conducted,

d) the results.

In addition to point 7.8 of ISO/IEC 17065/2012 and in accordance with Article 43 (5) of the GDPR the Certificationn Body shall inform competent supervisory authorities of the reasons for granting or revoking or refusing the requested certification.

7.9. Surveillance

In addition to point 7.9.1, 7.9.2 and 7.9.3 of ISO/IEC 17065/2012 and in accordance with Article 43 (2)(c) of the GDPR it shall be required that, in order to maintain certification during the monitoring period, the Certification Body shall specify regular monitoring measures. Such measures should be risk-based and proportionate and the maximum period between surveillance activities should not exceed 12 months.

7.10. Changes affecting certification

In addition to point 7.10.1 and 7.10.2 of ISO/IEC 17065/2012, amendments affecting certification to be taken into account by the Certification Body include:

1. any personal data breach or other infringement of GDPR or APPD identified by the Supervisory Authority, supervisory authorities in other sectors or judicial authorities that concern certification, reported by the Customer or the Supervisory Authority. Above mentioned infringements shall be taken into account only when relate to the certification.

2. changes due to new technological developments (to the extent relevant for future certification and surveillance),

3. amendments to the legal provisions on the protection of personal data,

4. adoption of delegated acts of the European Commission in accordance with Article 43 (8) and Article 43 (9) GDPR,

5. decisions, opinions, guidelines, recommendations, best practices or other documents adopted by the Board, and

6. court decisions on data protection.

The procedures for changes by the Certification Body shall cover issues such as: transition periods, approval process by the competent supervisory authority, reassessment of the relevant Targets of Evaluation and the appropriate measures to revoke the certification if the certified processing operation no longer meets the updated criteria.

7.11. Termination, reduction, suspension or withdrawal of certification

In addition to point 7.11.1 of ISO/IEC 17065/2012 and point 7.1(3) of this document, the Certification Body is obliged to inform the Supervisory Authority and, where appropriate, the PCA without delay, in writing, of the measures taken and about continuation, restriction, suspension and revocation of certification.

In accordance with Article 58 (2) (h) of the GDPR the Certification Body is obliged to accept decisions and orders of the Supervisory Authority regarding the withdrawal or refusal of certification to the Customer (Applicant) if the certification requirement is not or is no longer met.

7.12. Records

In addition to the requirements of ISO/IEC 17065/2012, the Certification Body is obliged to keep all documentation in a complete, comprehensible, up-to-date and fit to audit form.

7.13. Complaints and appeals, Article 43 (2)(d) GDPR

In addition to point 7.13.1 of ISO/IEC 17065/2012, the Certification Body shall specify:

a) who can file complaints or objections,

b) who processes complaints or objections on the part of the Certification Body,

c) which verifications take place in this context, and

d) the possibilities for consultation with interested parties.

In addition to point 7.13.2 of ISO/IEC 17065/2012, the Certification Body shall specify:

a) how and to whom the confirmation referred to in point 7.13.2 of ISO/IEC 17065/2012 should be issued,

b) time limits in this respect, and

c) which processes should then be initiated.

Certification Bodies are obliged to make their complaint handling procedures publicly available to data subjects and to provide easy access to them.

The Certification Body is obliged to inform complainants within a reasonable time on the progress and outcome of the complaint.

In addition to point 7.13.1 of ISO/IEC 17065/2012, the Certification Body must specify how it ensures that certification activities are separated from the handling of appeals and complaints.

§ 8.

Management system requirements

The general requirement of the management system in accordance with Chapter 8 of ISO/IEC 17065/2012 is that the implementation of all the requirements from the previous chapters for the application of the certification mechanism by the Certification Body is documented, evaluated, controlled and monitored independently.

The basic principle of management is to define a system according which its objectives are set effectively and efficiently, in particular the implementation of certification services — on the basis of the relevant specifications. This requires transparency and verifiability of the implementation of the accreditation requirements by the Certification Body and it permanent compliance.

To this end, the management system should specify the methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them with the Certification Body itself.

These management principles and their documented implementation must be transparent and be disclosed by the accredited Certification Body pursuant in the accreditation procedure pursuant to Article 58 of GDPR and thereafter at the request of the data protection Supervisory Authority at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) of GDPR or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c) of GDPR.

In particular, the accredited Certification Body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100 of GDPR), irrespective of the obligation under Article 23 of APPD, i.e. to provide the Supervisory Authority with the data of the certified entity and the entity to which the certification has been withdrawn, together with an indication of the reason for its revocation.

The procedures to be followed in the event of suspension or withdrawal of accreditation shall be integrated into the Certification Bodies' management system, including the notification of their Customers and the Applicants.

The Certification Body shall establish a complaint-handling process with the necessary levels of independence as an integral part of the governance system, which in particular implements the requirements set out in points 4.1.2.2(c) and (j), 4.6(d) and 7.13 of ISO/IEC 17065/2012. Relevant complaints and objections should be raised to the Supervisory Authority.

8.1. General management system requirements

The requirements of ISO/IEC 17065/2012 shall apply.

8.2. Management system documentation

The requirements of ISO/IEC 17065/2012 shall apply.

8.3. Control of documents

The requirements of ISO/IEC 17065/2012 shall apply.

8.4. Control of records

The requirements of ISO/IEC 17065/2012 shall apply.

8.5. Management review

The requirements of ISO/IEC 17065/2012 shall apply.

8.6. Internal audits

The requirements of ISO/IEC 17065/2012 shall apply.

8.7. Corrective actions

The requirements of ISO/IEC 17065/2012 shall apply.

8.8. Preventive action

The requirements of ISO/IEC 17065/2012 shall apply.

§ 9.

Further additional requirements

9.1. Updating of evaluation methods

The Certification Body shall establish procedures for updating the assessment methods used in the context of the assessment in accordance with point 7.4 of ISO/IEC 17065/2012 and this document. The update must take place in the event of changes to the legal framework, the relevant risks, the state of the art and the costs of implementing technical and organisational measures.

9.2. Maintaining expertise

Certification Bodies shall establish procedures to ensure the training of their staff to update their skills, taking into account the changes mentioned in point 9.1 of this document.

9.3. Responsibilities and competences

9.3.1. Communication between Certification Body and its Customers and Applicants

Procedures shall be in place for implementing appropriate procedures and communication structures between the Certification body and its Customer/Applicant. This shall include:

1. maintenance by the Certification Body of documentation of the division of tasks and responsibilities for the purposes of:
    a) responding to information requests , or
    b) enabling contact in case of a certification complaint;
2. conduct the process of receiving applications in order to:
    a) provide information on the status of an application;
    b) he Supervisory Authority’s assessment of:
        - feedback;
        - the decision of the Supervisory Authority.

9.3.2. Documentation of evaluation activities

The Certification Body shall put in place systems for the implementation of the relevant procedures and communication structures between the Certification Body and the Supervisory Authority. This includes a reporting framework to inform the Supervisory Authority of:

1. details of the Applicant to enable the Supervisory Authority to verify whether it has been a party to proceedings before the Supervisory Authority in the past;

2. the reasons for granting/withdrawing certification in accordance with Article 43 (5) of the GDPR immediately before issuing, renewing, suspending or withdrawing certification in accordance with section 7.1 (3) of this document.

9.3.3. Management of complaints handling

An integral part of the management system shall be the complaint-handling procedure which shall comply with the requirements of points 4.1.2.2(c) and (j), 4.6(d) and 7.13 of ISO/IEC 17065/2012.

The Certification Body shall submit relevant complaints and objections to the Supervisory Authority.

9.3.4. Management of withdrawal

The procedure to be followed in the event of suspension or withdrawal of accreditation shall be part of the Certification Body's management system. It also includes notifying Customers.

ul. Stawki 2
00-193 Warszawa
POLAND

www.uodo.gov.pl/en