REPUBLIC OF ALBANIA

INFORMATION AND DATA PROTECTION COMMISSIONER

GUIDELINE

No. 08, date 20.11.2025

ON ADDITIONAL CRITERIA FOR THE ACCREDITATION OF CERTIFYING BODIES

In accordance with point 1, article 38, point 1, article 85 and point 2, article 97 of Law no. 124/2024 "*On Protection of Personal Data*", the Information and Data Protection Commissioner, hereby, issues the following:

GUIDELINE:

HEADING I

GENERAL RULES

Article 1
Scope

1. The purpose of this Guideline is to determine additional criteria for the accreditation of bodies that will carry out certification, in accordance with the provisions of article 37 and article 38 of Law no. 124/2024 "*On Protection of Personal Data*".
2. The additional criteria complement the applicable legal framework and together constitute the certification mechanism.
3. All criteria and provisions of the international standard ISO 17065 (*Conformity Assessment - Criteria for Products, Processes and Services Certification Bodies*) are applicable for the purpose of accreditation as a certification body.
4. The provisions of this Guideline do not alter or prejudice the provisions of special laws, regulations or other sub-legal acts adopted by the General Accreditation Directorate or any national body competent for accreditation, which are applicable in addition to the criteria set out in this Guideline.

Article 2
Definitions

The terms used in this Guideline have the same meaning as those provided for in Law No. 124/2024 "*On Protection of Personal Data*" and ISO 17065 (*Conformity Assessment - Criteria for Products, Processes and Services Certifying Bodies*). The following definitions are added to this Guideline:

a) "**Accreditation"** is the attestation /certificate issued by the national accreditation body to the certification body, which meets the requirements set out in the harmonized standards based on the procedure and legal criteria provided for in Law no. 116/2014, *"On the Accreditation of Conformity Assessment Bodies in the Republic of Albania",* as well as the additional criteria set out in article 38 of Law no. 124/2024 "*On Protection of Personal Data"* and in this Guideline.

b) **"Certifying body**" is any legal entity that carries out conformity assessment activities, according to the accreditation by the General Accreditation Directorate in accordance with the provisions of Law no. 116/2014, *"On the Accreditation of Conformity Assessment Bodies in the Republic of Albania*", Law no. 124/2024 *"On Protection of Personal Data",* as well as this Guideline.

c) **"General Accreditation Directorate"** is the national organization that carries out the accreditation of certifying bodies and issues the relevant attestation/certificate;

ç) "**Certification mechanism"** is the set of structural, functional and operational criteria and competencies necessary for carrying out certification activities that ensures coherence, sustainability and impartiality.

d) "**Certification scheme"** means the set of internal rules and procedures, designed and implemented by the certification body, which includes the method of verifying compliance with the certification criteria and the assessment methodology for the certification of the processing operation(s).

e) **"Client"** means any personal data controller or processor, which asks the certifying body to provide it with the certification of the personal data processing operation(s) according to the provisions of Law no. 124/2024 "*On Protection of Personal Data*" and the Commissioner's Guideline no. 9 dated 20.11.2025 "*On the General Criteria for Certification and for Providing Granting Seals and Marks of Personal Data Protection*" (hereinafter Guideline no. 9).

ë) "**Commissioner"** means the Information and Data Protection Commissioner.

HEADING II
ACCREDITATION PROCEDURE

Article 3
Accreditation Principles

1. The entity that seeks to be accredited as a certification body, shall establish that it carries out certification activities in accordance with these principles:
   a) ***impartiality and independence***, which means exercising the activity independently, free from inappropriate influences, as well as guaranteeing impartial decision-making in all certification activities;
   b) ***confidentiality***, which means the guarantee of taking measures to prevent unauthorized access to information obtained within the framework of the certification activity, except when otherwise provided for by law;
   c) ***accountability***, which implies transparency in decision-making regarding certification and in certification processes, with the aim of demonstrating compliance with legal provisions;
   ç) ***responsibility***, which means assuming responsibility for the certification activity, including legal responsibility that may arise in the context of performing the certification activity;
   d) a clear and documented organizational structure that ensures effective functioning of the certification activity and compliance with the standards applicable to this nature of activity;
   e) necessary financial and technical resources as well as continuous training of human resources to carry out certification activities in accordance with the Right to Information and Personal Data Protection Commissioner's Guideline, no. 9, dated 20.11.2025 "*On General Criteria for Certification and for Granting Personal Data Protection Seals and Marks*".
2. The applicability of these principles is subject to monitoring by the Commissioner in accordance with the provisions of Law no. 124/2024 *"On Protection of Personal Data*" and this Guideline.

Article 4
Accreditation

1. The entity that intends to be accredited as a certifying body shall undergo the accreditation procedure at the General Accreditation Directorate, in accordance with the provisions of Law no. 116/2014, *"On the Accreditation of Conformity Assessment Bodies in the Republic of Albania".*

2. Accreditation is granted for a maximum term of 5 (five) years and may be renewed under the same conditions as the initial accreditation.

Article 5
List of documents for accreditation

1. The entity seeking accreditation presents the following documents that prove compliance with the legal criteria provided for in article 38, point 2 of Law no. 124/2024 "*On Protection of Personal Data*" and the additional ones specified in this Guideline.
   a) documents or acts of domestic or foreign authorities that certify the appropriate level of knowledge regarding the certification activity, seals or marks, as well as the implementation of data protection for the processing operation, subject of certification;
   b) internal documents or acts of the entity that confirm the establishment of the Independence Guarantee Committee, adopted by the competent internal bodies according to the statute or act of incorporation, which prove independence and commitment in exercising responsibilities and duties in a manner that does not cause a conflict of interest according to the provisions of this Guideline;
   c) documents or regulations demonstrating a certification scheme, consisting of recording the criteria, procedures or protocols to be applied for the assessment of personal data processing operation(s), periodic review, suspension and revocation of certification, seals and protection marks of personal data;
   ç) internal documents or regulations of the entity that reflect the commitment to respect the certification criteria set out in Guideline no. 9 and the certification mechanism, approved by the relevant bodies according to the statute or act of incorporation;
   d) internal documents or acts of the entity that define the procedures and structures responsible for reviewing complaints about infringement of the certification procedure or the way in which certification has been implemented, or is being implemented by the controller or processor, as well as to make these procedures and structures transparent to data subjects and the public;
   dh) model certification agreement to be signed between the certifying organization and the clients;
   e) internal documents or regulations that demonstrate the commitment of the entity seeking accreditation to maintain confidentiality;
   ë) documents or regulations that provide for compliance with the requirements for access to information under article 11 of this Guideline;
   f) documents or regulations proving compliance with the responsibility criteria under article 12 of this Guideline;

g) documents or regulations certifying compliance with the structural criterion under article 13 of this Guideline;

gj) documents or regulations certifying compliance with regard to sources under article 14 of this Guideline;

h) documents or regulations of domestic or foreign authorities certifying the technical suitability, ability, certification or training of staff;

i) internal documents or regulations indicating the manner of handling and preventing conflict of interest situations;

j) internal documents or regulations that determine the procedure to be followed in the event of a violation of the certification procedure or violations during the implementation of certification by the controller or processor.

2. The provisions of paragraph 1 of this article shall not affect the right of the General Accreditation Directorate to request the submission of other documents in accordance with the provisions of Law no. 116/2014, "*On the Accreditation of Conformity Assessment Bodies in the Republic of Albania",* and its implementing by-laws.

HEADING III
ACCREDITATION CRITERIA

Article 6
Legal obligations of the certifying organization

1. Regardless of fulfilling the criteria provided for in paragraph 4.1.1 of ISO 17065, the certifying body, when carrying out the certifying activity, shall implement updated procedures regarding legal responsibilities according to the provisions of this Guideline.
2. The certifying body shall implement procedures and measures for the processing of personal data of clients, as part of the certification process, in accordance with the provisions of Law no. 124/2024 "*On Protection of Personal Data*". Information on such measures and procedures shall be made available to the Commissioner to verify the control and management of client data.
3. The certifying body shall notify the General Accreditation Directorate of any substantial change in factual or legal circumstances related to the certification, immediately, and in any case no later than 15 days after the circumstance was identified. Substantial circumstances are those circumstances that affect the ability of the certifying body to provide reliable and reasoned certifications, including but not limited to accountability, impartiality, financial capacity, confidentiality, transparency, competence and prompt handling of complaints.

4. The certifying body shall confirm that there are no legal procedures that may result in non-compliance with the accreditation criteria under article 38 of Law no. 124/2024 "*On Protection of Personal Data*" and this Guideline.

Article 7

Certification Agreement

1. In addition to meeting the criteria set out in paragraph 4.1.2 of ISO 17065, the certification agreement signed by the legal representatives of the certifying body and the client, respectively, shall include and contain the agreement of the parties regarding the following aspects:
   a) compliance with certification criteria and implementation of any updates communicated by the certifying body;
   b) granting access to information, documentation, records, equipment, locations, personnel or information about the client's contractors or subcontractors, in order for the certifying body to carry out the certification procedure in accordance with Law no. 124/2024 "*On Protection of Personal Data*" and the provisions of Guideline no. 9;
   c) the conclusion/completion within the deadlines of the certification procedure provided for in the relevant certification scheme;
   ç) notification of the certifying body on substantial changes in the legal status, personal data processing operations, compliance with the certification criteria or information on the formal certification document. Substantial changes to the product, processes and services are those that constitute changes to the certification object, as they imply additions or substantial changes to the scope of certification or the type of product, processing scope and the manner of providing services;
   d) cooperation in monitoring activities, periodic audits and corrective measures requested by the certifying body. Failure to comply with this obligation shall result in the suspension or revocation of the certification for the entity subject to certification, in accordance with the provisions of Commissioner's Guideline no. 9, dated 20.11.2025 "*On the General Criteria for Certification and for Providing Granting Seals and Marks of Personal Data Protection*";
   e) immediate reporting of any legal or regulatory violations that may lead to non-compliance with certification criteria.
2. The certification agreement shall also contain provisions regarding:
   a) responsibility to the client that certification does not exempt them from legal obligations under personal data protection legislation;
   b) the assessment methods, complaints and relevant procedures, as well as the obligations towards the client in relation to these processes that are determined by the

certifying body in accordance with paragraph 4.1.2.2. of ISO 17065 and the provisions of this Guideline;

c) the rules on the validity, renewal, suspension and revocation of certification, including periodic reassessment in accordance with paragraph 4.1.2.2 of ISO 17065 and the provisions of this Guideline;
d) the consequences of the expiration, suspension, revocation or non-issuance of the certificate as well as the actions to maintain or renew the certification.

Article 8
Use of the certificate, seal and mark

1. In addition to meeting the criteria set out in paragraph 4.1.3 of ISO 17065, the certifying body, through the creation/design of an internal mechanism, maintains control over the use and display of the certificate, seal and mark as well as any other aspect of the certification, ensuring that:
   a) the certification mechanism is clearly identifiable. The communications transparently describe the scope of the processing operation(s) involved in the certification;
   b) the scope of certification is clearly defined and avoids any misinterpretation regarding the processing action(s) assessed within the certification process;
   c) The rules for using the certification seal apply only to certified clients.
2. Any incorrect, misleading or potentially misinterpretable use of the certificate, seal or mark or any other aspect of the certification shall be addressed through applicable corrective tools, which shall include at least the following:
   a) the request to the client to avoid incorrect practice or one that may lead to misinterpretation;
   b) ensuring that the client updates public information through communication tools similar to those previously implemented;
   c) notifying the certifying body without delay about the non-conformity and the corrective measures taken.
3. Other additional measures that are assessed by the certifying body may include suspension or revocation of certification, publication of the violation and, if deemed necessary, taking legal proceedings.

Article 9
Impartiality and independence

1. In addition to meeting the criteria set out in paragraph 4.2 of ISO 17065, the certifying body shall ensure impartiality and independence in the exercise of certification activities by establishing, organizing and operating a special committee, with balanced participation

of representatives of interest groups, ensuring that no interest prevails. The committee shall meet periodically, at least once a year, to assess the risks related to independence and effectiveness of the measures implemented by the certifying body. The certifying body shall present documents or regulations that prove independence, in particular with regard to financing, including, but not limited to:

a) the statute and the act of incorporation;
b) internal rules and procedures relating to the membership, appointment, remuneration and duration of the term of office of the members of the body who have decision-making powers over certification;
c) documents reflecting commercial, financial, contractual or other relationships between the certifying body and the clients, including annual financial statements and records of funding sources.

2. The certifying body shall ensure that it does not maintain any relationship of any kind with the client being assessed. In particular, the certifying body shall identify risks to impartiality and independence on a regular basis and take effective measures to address risks arising from the actions of third parties, including individuals, commercial entities or public bodies. Risks to impartiality and independence include threats arising from financial, commercial, contractual or personal relationships.
3. The certifying body shall ensure for each client that:
   a) personnel involved in the assessment, review or decision-making process shall not have any relationship with the client beyond the activity within the framework of the certification process and shall not perform other actions that may compromise impartiality;
   b) the client has no family or other relationship that may pose a risk to the impartiality of the certifying body;
   c) there is no financial relationship, beyond the activity within the framework of the certification process, between the certifying body and the client. The certifying body shall document and manage the risk to impartiality.
4. Internal organization shall ensure that functions, tasks, and organizational structures leave no room for suspicions of conflict of interest. The certifying body shall establish and ensure the implementation of an internal mechanism that guarantees the effective identification, prevention and management of conflicts of interest. All employees shall declare any actual, potential or perceived conflicts of interest according to internal procedures approved by the relevant structure of the certifying body. Conflicts may arise, but are not limited to, in the following situations:
   a) the certifying body has a financial relationship with the client, which exerts an influence on the income or financial influence;
   b) the certifying body or its employees have quota or shares in the company that provides consultancy services related to the products, processes or services to be certified;

c) the certifying body does not engage in consultancy services or other activities that compromise impartiality and independence, including but not limited to acting as a data protection officer or consultancy services regarding compliance with data protection legislation.

5. The management level and responsible personnel of the certifying body engaged in conformity assessment shall not:
   a) have participated in the design, production, distribution, installation or purchase of the product, process or service subject to assessment;
   b) be the owner, user or maintainer of the product, process or service in question;
   c) to act as an authorized person of the entities involved in the roles mentioned in paragraph 5/b) of this article.
6. The certifying body shall implement internal procedures and mechanisms for the continuous identification and management of risks to impartiality and independence and shall ensure that all personnel maintain independence and impartiality in all certification activities.
7. In addition to the criteria provided for in paragraph 4.4 of ISO 17065, the certifying body shall implement fair and non-discriminatory certification procedures and shall ensure equal access to these certification procedures regardless of the size of the client, affiliation, origin of the product and shall ensure equal applicability of the procedure to all clients.

Article 10
Confidentiality

1. In addition to the criteria set out in paragraph 4.5 of ISO 17065, the certifying body shall be responsible for the management of information collected, created or used in the context of the certification activity. The certifying body shall ensure to current or prospective clients that its personnel, in particular those involved in the assessment and decision-making process, maintain the confidentiality of information through the implementation of confidentiality agreements, self-declarations or other documents of a binding nature. The obligation includes all information, regardless of its sensitive, commercial, proprietary nature, trade secret, business process(es), technical documentation and personal data, without prejudice to the certifying body's obligation to act in accordance with the legal framework on transparency or to comply with legal obligations.
2. The obligation under paragraph 1 of this article does not prevent the certifying body from publishing the certification criteria, methodology and results of a non-confidential nature.

Article 11
Accountability and access to information

1. In addition to the criteria provided for in paragraph 4.6 of ISO 17065, the certifying body shall publish and make publicly available information on:
   a) all versions (current and repealed) of the certification criteria specifying the respective validity period;
   b) updated certification procedures including the appeals procedure;
   c) information about the certification procedure applied in practice, including information about the data subject affected by the data processing according to the scope of certification as well as the way to submit and handle a complaint;
   ç) public register of registered seals and marks.

Article 12
Responsibility

1. In addition to the criteria provided for in paragraph 4.3 of ISO 17065, the certifying body shall establish and implement appropriate measures, such as professional insurance or financial reserves, to cover any liability arising from certification activities. The certifying body shall implement appropriate measures to ensure comprehensive jurisdictional coverage and the fulfilment of this obligation is subject to verification by the General Accreditation Directorate.
2. The certifying body shall establish the fulfilment of the obligation related to responsibility through documents, acts or attestations (insurance policies) as follows:
   a) professional insurance to cover liabilities arising from certification activities;
   b) is not in liquidation or bankruptcy proceedings under applicable legislation;
   c) has paid all obligations for health and social contributions according to the legislation in force;
   ç) is not undergoing execution procedures for tax obligations;
   d) the legal representative has not been convicted by a final decision for criminal offences related to the activity of the certifying body.
3. The certifying body shall conduct a risk assessment in relation to the certification activity and implement appropriate measures to address the identified risks, and shall make the relevant documentation available to the General Accreditation Directorate and the Commissioner, if requested. Risks related to certification activities may include, but are not limited to, the following:
   a) setting the audit objectives;
   b) methods of collecting data during the audit process;
   c) existing and perceived risk to impartiality;

d) issues related to liability and legal obligations, including compliance with personal data protection legislation;
e) the organizational and operational characteristics of the audited client;
f) the potential effect of the audit on the client and the activities it carries out;
g) health and safety aspects for the audit team;
h) inaccurate or misleading customer statements;
i) use and protection of trademarks.

4. Appropriate measures to mitigate the identified risk may include, among others, contracting insurance policies that cover potential claims, creating sufficient budget lines or similar measures. The certifying body shall conduct periodic risk assessments, at least once a year, to identify risks that may arise or those that have changed in relation to the activity and personnel.

Article 13
Structural criteria

1. The criteria provided for in paragraph 5.1 of ISO/IEC 17065 shall apply with regard to the structural organization and the senior management level.
2. The criteria set out in paragraph 5.2 of ISO/IEC 17065 shall apply to mechanism that guarantee impartiality.

Article 14
Resources

1. In addition to the criteria set out in paragraph 6.1 of ISO 17065, the certifying body shall establish, implement and maintain management procedures that demonstrate that the personnel have the skills, knowledge and expertise necessary to carry out the certification activities. Information on personnel shall be processed lawfully, fairly and transparently in accordance with the legislation on personal data protection. The certifying body shall ensure that the personnel are individuals with the technical and legal knowledge necessary for the certification process, including the area of personal data protection, rules applicable to customer data protection, technical and organisational measures for the protection of personal data, as well as the assessment and audit of data processing operations.
2. The certifying body shall provide and present the necessary documentation that proves the technical knowledge of the personnel, including:
   a) degree in computer science, information systems or cybersecurity or similar fields;
   b) at least 5 years of professional experience in personal data protection;
   c) at least 2 days of training related to information system security management, including rules, standards, methods, good practices and risk management.

3. The certifying body shall provide and present the necessary documentation that proves the legal knowledge of the personnel, including:
   a) master's degree or equivalent qualification;
   b) at least 5 years of professional experience in the area of personal data protection.
4. The certifying body shall ensure continuous strengthening of personnel capacities through professional training programs that include technical standards, regulatory criteria and obligations related to personal data protection. Training and updating of knowledge/skills shall be carried out annually and shall be formally recorded.
5. The certifying body shall provide personnel with the technical knowledge and skills/experience as follows:
   a) for assessors, at least 2 years of professional experience in the area of personal data, including analysing and implementing technical and organizational measures for the protection of personal data, security testing, technical assessments or certifications;
   b) for managers or decision-makers, at least 2 years of professional experience in identifying, defining, monitoring and advising on personal data protection measures.
6. The certifying body shall provide with the legal knowledge and skills/experience as follows:
   a) for assessors, at least 2 years of professional experience in the area of personal data protection, including analysing or implementing compliance of personal data processing operations, audits, or contract reviews;
   b) for managers or decision-makers, at least 2 years of professional experience in compliance monitoring or consulting in the area of personal data protection.
7. In addition to the criteria provided for in paragraph 6.2 of ISO 170656 regarding independence from commercial or other interests with the client, personnel engaged in the certification process shall act in accordance with the rules approved by the certifying body.
8. The certifying body shall use information about personnel to identify and address risks to impartiality arising from activities or institutional affiliations. All potential conflicts of interest shall be verified and addressed to ensure that personnel maintain independence from commercial or other interests with the client.
9. In case certification activities are carried out by subcontracted entities, the certifying body shall ensure that the subcontracted entity and its personnel meet the applicable criteria in relation to the assessment activities.
10. In accordance with paragraph 6.2.24 and 7.6.1 of ISO 17065, the certifying body shall bear full responsibility and accountability for all subcontracted activities and ensures that the subcontracted entity and its personnel meet all applicable criteria, including the provisions of Law no. 124/2024 "*On Protection of Personal Data"* and remains responsible for decision-making related to certification.

HEADING IV
IMPLEMENTATION OF THE CERTIFICATION PROCESS

Article 15
Implementation of ISO 17065

The criteria of paragraph 7.1 of ISO 17065 shall be applied within the framework of the certification process. The personal data processing operation(s) are assessed according to the legal criteria provided for in Law no. 124/2024 "*On Protection of Personal Data*" and this Guideline.

Article 16
Submission of an application by the client

1. The client shall submit a written request for assessment and certification to the certifying body. The request shall specify the cooperation that may in place between the client and third parties, for the control or engagement of data processors that will be subject to certification. In the event that the client acts as a co-controller or co-processor, the application shall specify the client's responsibilities, duties and contractual and legal documentation on which the cooperation is based.
2. In addition to the criteria provided for in paragraph 7.2 of ISO 17065, the client shall provide the certifying body with the following information regarding the assessment:
   a) detailed description of the scope of assessment, including aspects related to the interface with external systems or other entities, implemented protocols and guarantees for the security of data communication;
   b) list of international data transfers, including the legal framework of the data recipient and the safeguards that have been implemented to protect them;
   c) list of data processors or sub-processors, including responsibilities, data processing activities, main or model contracts on which the relationship with the customer is based.
   ç) the list of co-controllers, including responsibilities and duties as well as the principles and legal instruments on which the relationship with the client is based.
   d) the general characteristics of the data processing operations that will be the subject to certification, including the physical location where the data is processed, the category of data, and the applicable legal obligations;
   dh) information on certifications or other results of assessments that have been carried out previously, if any, and whether the nature of these assessments and their scope can be considered within the framework of the certification process;

e) information regarding investigations, newly imposed sanctions or corrective measures imposed by the Commissioner or other competent authorities in relation to the processing of personal data within the scope of the certification;

ë) where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals, such as the processing of sensitive data or the use of advanced technologies or automated decision-making processes, the client shall carry out and submit a data protection impact assessment in accordance with article 31 of the Law no. 124/2024 *"On Protection of Personal Data"*.

Article 17
Review of the application for certification

1. The certifying body shall examine the application in accordance with paragraph 7.3 of ISO 17065 and the provisions of paragraph 2 of this article.
2. In addition to meeting the criteria set out in paragraph 7.3.1, the certifying body shall assess the documentation submitted and ensure that:
   a) the client is a suitable candidate for assessment against the certification criteria taking into account the rules set out in the certification mechanism, and shall verify that the client and the data processing operations are within the scope of the certification, the client's responsibilities under the legal framework on personal data protection and types of data processing operations for which certification criteria have been adopted;
   b) there are appropriate assessment methods for the client, taking into account the rules set out in the certification scheme, the legal framework on personal data protection and any ongoing investigations, newly imposed sanctions or corrective measures imposed by the Commissioner. The assessment methods are applied to similar clients to produce comparable results;
   c) has the necessary technical and legal knowledge on personal data protection to carry out certification activities, especially if there has been no previous experience in carrying out assessments with the same or similar scope.
3. If the certification scheme establishes rules for calculating the duration of the certification activity, the certifying body shall implement a procedure to calculate the duration of the assessment taking into account:
   a) the extent of data processing operations that will be subject to certification;
   b) the nature of the processed data;
   c) risks to data subjects;
   ç) the complexity of the technologies used;
   d) engagement of data processors;
   e) the number of countries or structures in which client data processing is carried out.

4. The certifying body calculates the duration of the audit in accordance with the certification scheme and determines whether it is sufficient to complete the assessment or whether additional time is needed. The duration of the audit is set in the agreement between the certifying body and the client.
5. The certifying body shall ensure that the certification agreement contains the mandatory methodology for the assessment of the client and that the assessment reasonably covers technical and legal competences in the area of personal data protection. Possession of these competences is deemed to be fulfilled when the personnel engaged in the certification process meets the technical and legal criteria provided for in article 14 of this Guideline, including documentation regarding professional education and experience as well as attendance at continuous training.
6. The certifying body maintains records that demonstrate the competences and verifies the fulfilment of the criteria for all personnel, including, where applicable, those for subcontracted assessors.

Article 18
Assessment plan

In addition to the criteria set out in paragraph 7.4 of ISO 17065, the certifying body shall draw up and implement an assessment plan which provides for the application of the assessment methodology set out in the agreement. The methodology may include on-site assessments, paper-based assessments, the conduct of audits, interviews or the application of other appropriate instruments to collect findings that demonstrate compliance with the assessment criteria. The assessment plan shall include a risk assessment and a data protection impact assessment for processing operations with a high risk to the fundamental rights and freedoms of individuals.

Article 19
Assessment methodology

1. Deflection from the assessment methodology shall be recorded by setting out the reasons, the risk assessment and the effects of the findings that are of value for certification.
2. The certifying body shall ensure that the assessment methodology is appropriate to assess compliance with the certification criteria, standardized and applicable. The assessment methodology shall include compliance with the legal certification criteria referred to in this Guideline. The certifying body shall ensure that the methodology applied and the relevant results are documented and maintained. The assessment methodology shall be adapted to the typology, complexity and level of risk of the processing operations to ensure that high-risk processing is fully assessed.

3. The tasks related to the assessment may be assigned to internal staff or external experts approved by the certifying body, provided that the team engaged in the assessment meets the criteria for legal and technical knowledge referred to in article 14 of this Guideline. The certifying body ensures that the client meets the criteria of the certification mechanism, if reference is made to previous certification results. Previous assessment reports shall be accessible and other findings are documented.
4. In accordance with the criteria of paragraph 7.5 of ISO 17065, the certifying body shall evaluate all information and assessment results. The assessment process shall ensure compatibility between the scope of certification and scope of the assessment and that the assessment methodology has been applied coherently against the documented findings.
5.

Article 20
Client information

1. In addition to the criteria provided for in paragraph 7.4.6 of ISO 17065, the certifying body shall determine the procedures for informing the client on the assessment results, including non-conformities, and specifying the type, form and time frame in accordance with the certification scheme.
2. In addition to the criteria provided for in paragraph 7.4.9 of ISO 17065, the assessment findings shall be documented for each assessment criterion in accordance with the certification scheme. The documents collected during the assessment shall be clearly highlighted in order to establish a link with the relevant certification criterion and the relevant findings. The client shall be invited to propose corrective and preventive measures which shall be attached to the action plan and verified before the certification decision is taken. The assessment report shall contain:
   a) a description of the client;
   b) evaluation plan;
   c) references to the documents reviewed;
   ç) references to the processing operations that have been assessed;
   d) functions of persons interviewed, location of findings, description of non-conformity including scale and extent;
   dh) the certifying body shall establish, implement and maintain a formal assessment methodology that specifies the approach, criteria, time frames and decision-making rules that determine the fulfilment of each certification criterion. The methodology shall be applied in a coherent manner to the client and shall be recorded in the assessment plan and reports.

Article 21
Access to the assessment reports

1. The assessment reports and relevant annexes are fully accessible upon request by the Commissioner and are retained for a period of 6 years.
2. The Commissioner may participate as an observer during the assessment procedure.

HEADING V

DECISION ON CERTIFICATION, MONITORING AND RENEWAL OF CERTIFICATION

Article 22
Decision on certification

1. In addition to the criteria set out in paragraph 7.6 of ISO 17065, the certifying body shall establish and implement procedures that ensure independence and accountability in relation to the certification decision. The decision-making procedures shall include risk analysis and shall ensure that the decision is supported by documents and evidence.
2. The person(s) or team responsible for the certification decision must not have participated directly or indirectly in assessment or advisory activities for the same client and must sign a conflict-of-interest declaration. Where necessary to maintain independence, personnel rotation is applied.
3. The certifying body shall document and maintains all certification decisions, including the reasoning, supporting documentation and identification of decision-makers, and shall establish an internal mechanism for the evaluation and review of complaints.

Article 23
The document proving certification

1. In addition to the criteria provided for in paragraph 7.7 of ISO 17065, the certifying body shall deliver to the client a formal document (certificate) whereby it is identified:
   a) the full name and version of the certification criteria that were used for the assessment;
   b) the scope of certification, including a clear and understandable statement (formulation) of the scope of certification, a description of the type of personal data, the processing operations involved and a list of the locations where these processing operations are carried out;
   c) the client, including the unique entity identification number (NUIS).

2. The validity period of the certification may not exceed 3 years. Periodic monitoring of the certification shall be carried out and documented in accordance with article 25 of this Guideline.
3. In the event of legal or regulatory changes that affect the client's compliance, the certifying body shall ensure, within a reasonable time, the updating of the certificate and other documents.

Article 24
Obligation to publish the assessment report

1. In addition to the criteria provided for in paragraph 7.8 of ISO 17065, the certifying body shall store the information of the certified client, enabling access via the official website to a summary (extract) of this information. The summary (extract) of the assessment report shall contain the following data:
   a) the scope of the certification, including a clear and understandable presentation of the scope of the certification and any personal data processing operations included in the certification;
   b) relevant certification criteria including version, status and applicable references to recognized standards or other reference rules;
   c) assessment methods and tests performed;
   ç) results, including non-conformity, assessment limitations and identified unaddressed risks.
2. The summary (extract) is assessed and updated at least once a year or when there are substantial changes in the scope, criteria, assessment methodology, unaddressed risks, ensuring that the information remains accurate, complete and up-to-date.

Article 25
Obligation to implement monitoring measures

1. The certifying body shall implement monitoring measures throughout the validity of the certification to verify continued compliance with the certification criteria, ensuring that the scope, periodicity and intensity of monitoring is proportionate to the assessed risks to data subjects and the non-conformity likelihood.
2. Monitoring activities shall be planned and carried out based on the risk assessment, the risks associated with the customer and the certified processing operations. In addition to the criteria provided for in paragraph 7.9 of ISO 17065, monitoring includes the assessment of the following aspects:
   a) change in data processing operations since the last assessment;
   b) implementation of previously postponed evaluation criteria;

c) corrective actions from previous audits; and

ç) the criteria selected based on the identified risk of non-conformity.

3. The monitoring procedure shall be transparent, effective, verifiable and operationally feasible and appropriate for the certification scheme. The monitoring procedures shall be independent of operational or commercial influences that could compromise impartiality. These procedures shall include:
   a) responsibilities, structure and resources allocated for monitoring;
   b) periodic monitoring activities that may include inspection, audit or similar assessments;
   c) the mechanism to assess whether the criteria for maintaining certification continue to be considered met;
   ç) additional assessments resulting from complaints, publicly identified non-conformity or Guidelines from the General Accreditation Directorate or the Commissioner.
4. The certifying body, for the purpose of transparency, shall publish an updated register regarding the status of the certification (validity, suspension or revocation).
5. All monitoring activities, risk assessment, corrective measures and relevant decisions shall be recorded to ensure traceability, accountability and transparency in accordance with Law no. 124/2024 "*On Protection of Personal Data*" and relevant sub-legal acts.

Article 26
Changes affecting certification

1. In addition to the criteria provided for in paragraph 7.10 of ISO 17065, the certifying body shall consider as changes affecting certification:
   a) any changes in the legislation on the protection of personal data with respect to the scope of the certification mechanism;
   b) the Commissioner's decisions regarding the scope of the certification mechanism;
   c) court decisions related to the protection of personal data on matters submitted for review in relation to the subject of certification;
   ç) new technological developments used for data processing operations;
   d) new risks to personal data protection including dentification and assessment of new or evolving risks from innovation in technology, changes in data processing practices, or other developments that may affect the effectiveness of the certification process and the implementation of technical and organizational measures to mitigate these risks.
2. Changes may be managed through special procedures, including transition periods, client reassessments, and if deemed appropriate, measures to revoke certification if processing does not meet the updated criteria.

Article 27
Termination, suspension and revocation of certification

1. In addition to the criteria provided for in paragraph 7.11 of ISO 17065, the certifying body shall develop and implement procedures to promptly notify in writing the client, the General Accreditation Directorate and the Commissioner on any certification decision regarding the validity, reduction of scope, suspension or revocation, including decisions taken as a result of complaints:
   a) in case of termination at the request of the client, the certifying body shall inform the General Accreditation Directorate within 30 calendar days from the date of receipt of the request for termination of certification;
   b) in the event of the of suspension or lifting thereof, revocation or reduction of the facility, the certification body shall inform the General Directorate of Accreditation and the Commissioner without delay.
2. The certifying body shall establish procedures for handling client non-conformity according to the rules set out in the certification scheme, which shall include at least the following aspects:
   a) whether the corrective measures proposed by the client are adequate to address the problem, before a decision on certification is taken. For all non-conformities, the certifying body assesses whether the action plan is adequate to ensure compliance with the data processing operations, before a decision on certification is taken. In the event that an action plan is inadequate to ensure compliance, the certifying body suspends the certification decision until evidence of the implementation of the corrective measures is provided;
   b) determines delays in the implementation of corrective measures (action plan) from 30 to 60 days, taking into account the extent and nature of the non-conformity;
   c) if certification is conditional on the implementation of the action plan, the certifying body shall verify the corrective measures that have been implemented and take the necessary actions if the non-conformity with the criteria has not been addressed according to the action plan.
3. The certifying body shall implement the binding acts of the General Accreditation Directorate and the Commissioner, including revocation, suspension and refusal of certification if it is found that the criteria are not met.
4. In the event of a refusal, suspension or revocation of certification, the client is informed of the right to appeal the decision, the available remedies and the relevant deadlines.

Article 28
Record-keeping

1. In addition to the criteria provided for in paragraph 7.12 of ISO 17065, the certifying body shall maintain records in a complete, understandable, up-to-date and verifiable manner.
2. The records must include at least the following:
    a) documents related to the certification(s) that has/have been granted or rejection decisions;
    b) documents related to the procedures under consideration for certification.
3. The records shall be accessible for a period of 6 years. In the event of a dispute between the certifying body and the client or in the event of a complaint, the period for which the records must be retained for the purpose of resolving the dispute is determined by the applicable rules of the dispute.

Article 29
Appeal

1. The certifying body shall have ensure complaint mechanisms for any data subject or organization active in the personal data protection, authorized by a data subject, in relation to certification activities, without prejudice to the right of data subjects to file a complaint with the Commissioner or a lawsuit in court.
2. In addition to the criteria set out in paragraph 7.13 of ISO 17065, the certifying body shall implement a documented procedure for receiving, examining and deciding on complaints relating to the certification process, taking into account the rules set out in the certification scheme. The procedure shall be accessible to the public and to all data subjects and competent authorities within the scope of the certification.
3. The complaint handling procedure shall ensure participation, impartiality and the right to be heard. The complainant shall be informed about the progress and decision-making within a reasonable period, but no later than 3 months from the date of submission of the complaint. A preliminary assessment of the complaint shall be copied within one month from the date of submission of the complaint, setting out the preliminary response and the steps to be taken in the next 2 (two) months. If a formal decision cannot be reached within the 3 (three) month period, the certifying body shall inform the complainant about the conclusion of the process and the reasons why it was not possible to reach a conclusion within this period.
4. The appeal procedure must at least include the following:
    a) subjects who are entitled to legal standing to file a complaint;
    b) the entity responsible for collecting and verifying the necessary information for the progress of the complaint until decision-making;

c) the entity responsible for decision-making and resolution of the complaint;

ç) the different stages for informing the complainant regarding the progress, outcome and conclusion of the complaint, including the relevant time limits;

d) the way in which verification is carried out;

dh) the procedure that may be undertaken to resolve the complaint, including consultations with the stakeholders involved;

e) the parties to whom confirmation of the notification is sent, within 1 (one) month from receipt, that may be extended if necessary and justified by another 1 (one) month;

ë) the deadlines which the party must be aware of;

f) other procedures when the case (complaint) remains unresolved or unfinished.

5. The certifying body shall ensure that the handling of complaints is separate from the assessment, review and decision-making on certification, in order to avoid conflicts of interest.
6. The certifying body shall create and update the Register of Complaints which must include:
   a) the status of each complaint (filed, under investigation, or completed);
   b) dates of actions taken (complaint registration, receipt of notice, progress update, decision-making, etc.).
7. The Register shall be accessible for inspections by the General Accreditation Directorate and the Commissioner.

HEADING VI
CRITERIA FOR THE MANAGEMENT SYSTEM

Article 30
General criteria of the management system

1. In addition to the criteria set out in paragraph 8 of ISO 17065, the certification body shall develop and maintain a management system that meets the criteria set out in this Guideline for all certification activities and within the scope of accreditation. The system shall include documentation, assessment and independent monitoring of additional criteria to ensure compliance, transparency and traceability.
2. The management system shall be based on a methodology on implementation and control of criteria, in accordance with Law no. 124/2024 "*On Protection of Personal Data*" and this Guideline, including continuous monitoring to ensure compliance. The system shall be harmonized with the general principles of ISO 17065 management, documentation and

control, internal audit reports, management body assessments, and corrective and preventive measures.

3. In particular, the management system shall ensure:
   a) information on certification, including the certification mechanism or scheme applied, the validity period, and the relevant conditions that are accessible to the public on a permanent and ongoing basis. The information shall be regularly updated in relation to changes to the certification scheme or other relevant decisions;
   b) fulfilment of the criteria of articles 11 and 24 of this Guideline;
   c) that the implementation of management principles is transparent and verified during the accreditation process or at the request of the General Accreditation Directorate or the Commissioner;
   ç) that the management system complies with the following criteria:
      (i) paragraph 8.2 of ISO 17065 regarding management system documentation, including the process of drafting, updating and maintaining documents according to legal changes and standards. The documentation shall be accessible to all interested parties, as long as the confidentiality and integrity of the data are maintained;
      (ii) paragraphs 8.3 and 8.4 of ISO 17065 regarding version control to ensure that all documentation is archived in accordance with security elements and updated. Changes to documentation shall be monitored and audited to ensure accuracy and consistency of data;
      (iii) paragraph 8.5 of ISO 17065 regarding management level assessment, including analysis of internal audit and external assessment results. Assessment shall be carried out regularly and be part of the process of continuous improvement of the management system;
      (iv) paragraph 8.6 of ISO 17065 regarding internal audit. The audit shall be carried out in a documented manner and cover all aspects of the management system, including quality, regulatory compliance and data security. Auditors shall be independent of the departments they audit and have completed the relevant training. The audit results shall be documented and include specific recommendations for improvement and a detailed action plan for their implementation;
      (v) paragraph 8.7 of ISO 17065 regarding corrective actions taken to address identified nonconformities. Corrective actions shall include an analysis and are subject to assessment by internal audit. They shall be monitored and implemented within a specified time period. The certifying body shall report on the progress of the implementation of these actions and ensure that the effects are measurable and evaluable;
      (vi) paragraph 8.8. of ISO 17065 regarding preventive measures to identify and reduce the risk that may cause non-conformities in the future. Actions shall be taken based on a risk analysis and include measures that reduce the likelihood that the risk

will materialize. Preventive measures shall be documented and reviewed periodically to ensure that they effectively prevent non-conformities.

Article 31
Procedures for updating valuation methods

1. The certifying body shall develop procedures for updating the assessment methodology to be applied when there are changes in the legal framework, the overall situation, and in the implementation of the costs of technical and organizational measures and significant risks. The update shall include a risk analysis and an assessment of the impact of these changes on the assessment process and its effectiveness.
2. The certifying body shall develop procedures to ensure training of personnel to update capacities/skills taking into account the changes mentioned in paragraph 1 of this article.
3. The certifying body shall develop procedures in the event of reduction, suspension or revocation of accreditation, including the criteria for these cases and notification of the client. Notification of clients shall be carried out within a period of 30 (thirty) days and the customer has the possibility of appealing within 30 (thirty) days from the date of notification.

HEADING VII
COMMISSIONER 'S MONITORING

Article 32
Monitoring and supervision of certification bodies by the Commissioner

1. The Commissioner shall monitor and supervise whether the certification bodies meet the criteria provided for in Law no. 124/2024 "*On Protection of Personal Data*" and this Guideline, regardless of and without prejudice to the supervisory powers exercised by the General Accreditation Directorate according to the provisions of Law no. 116/2014, *"On the Accreditation of Conformity Assessment Bodies in the Republic of Albania"*.
2. The Commissioner, may, within the framework of monitoring and supervision, request from the certifying body:
   a) various documents or acts, including internal procedures implemented by it in order to meet the legal and additional criteria under this Guideline;
   b) the documentation or information necessary to verify compliance with Law no. 124/2024 "*On Protection of Personal Data*", setting deadlines for their submission;
   c) conducting on-site inspections, audits and other similar technical assessments. For this purpose, the Commissioner shall notify the certifying body at least 7 days prior to the inspection, audit or assessment.

3. The certifying body shall cooperate with the Commissioner and make available in full and within the specified deadline any requested information/document, as well as perform any other necessary actions to facilitate monitoring and supervision.
4. The Commissioner, in order to facilitate monitoring, compliance assessment and risk assessment related to certification, shall request from the certifying body a written report on the certification issued pursuant to article 37 of Law no. 124/2024 "*On Protection of Personal Data*", including the subject of the certification, its number and validity period.
5. Within the framework of institutional cooperation, the Commissioner may request from the General Accreditation Directorate a copy of the supervision report on conformity assessment drafted within the framework of the implementation of Law no. 116/2014, *"On the Accreditation of Conformity Assessment Bodies in the Republic of Albania",* as well as any other information on the certifying bodies accredited as per this Guideline, the scope and relevant status of the accreditation (validity, suspension or revocation) or other data necessary for the effective implementation of monitoring and supervisory powers under Law no. 124/2024 "*On Protection of Personal Data*".

Article 33
Sanctions

1. If the Commissioner finds inconsistencies in the exercise of the activity by the certification body in relation to Law No. 124/2024 "*On Protection of Personal Data*", he exercises, as appropriate, the investigative, corrective or sanctioning powers provided for in Law No. 124/2024 "*On Protection of Personal Data*".
2. The Commissioner may propose to the General Accreditation Directorate the revocation of the accreditation of the certifying body if he/she finds that the conditions and criteria for accreditation have not been met or are no longer met or if the actions of the certification body violate Law No. 124/2024 "*On Protection of Personal Data*".

Article 34
Transitional and final provisions

1. Certifying bodies that were accredited before the entry into force of this Guideline in line with the Commissioner's Guideline no. 48, dated 14.09.2018 *"On the Certification of Information Security Management Systems, Personal Data and their Protection"*, continue to carry out certification activities until the end of the accreditation period.

2. Guideline no. 47 dated 14.09.2018 "*On Determining the Rules for Maintaining the Security of Personal Data processed by Large Processing Entities*" and Guideline no. 48,

dated 14.09.2018 "*On the Certification of Information Security Management Systems, Personal Data and their Protection",* shall be repealed.

This Guideline shall enter into force upon its publication in the Official Journal.

COMMISSIONER

Besnik Dervishi