REPUBLIC OF ALBANIA

INFORMATION AND DATA PROTECTION COMMISSIONER

GUIDELINE

No. 09, dated 20.11.2025

ON "GENERAL CRITERIA ON CERTIFICATION DHE GRANTING PERSONAL DATA PROTECTION SEALS AND MARKS"

Pursuant to article 37, paragraph 1, article 85 paragraph 1, and article 97, paragraph 2 of the 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. This Guideline provides for the general criteria for the certification and issuance of personal data protection seals and marks.
2. The process of personal data processing is controlled and certified by the certifying body only if it meets all the provisions of the certification mechanism provided for in this Guideline. Obtaining certification in accordance with the provisions of article 37 of the Law and this Guideline confirms that the process of processing personal data is carried out in accordance with the certification mechanism approved by the Commissioner.

Article 2
Definitions

1. The terms used in this Guideline have the same meaning as those provided in the Law, as well as ISO 27701 (Data security, cybersecurity and personal data protection — *Personal Data Management Systems — Criteria and Guidelines).*

   Other terms used in this Guideline have the following meanings:

   a) "***Certification"*** is the process carried out by the certifying body in accordance with the provisions of article 37 of the Law and this Guideline, for the purpose of assessing conformity, at the end of which the client is provided with the seal and marks for the protection of personal data, as well as all other aspects that include the guarantee of compliance and validity of the certification.

   b) "***Seal and mark***" is the symbol to be used by the certification body to indicate that a processing operation or operations have been assessed and found to be in conformity with the specific legal requirements on personal data protection.

   c) ***"Certification body"*** is the legal entity accredited by the General Directorate of Accreditation in accordance with 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 the Commissioner's Guideline no. 8, dated 20.11.2025 *"On Additional Accreditation Criteria on the Certifying Body*".

   ç) *"**Client*"** is any natural or legal person, public or private, who, based on the field of activity or in the exercise of powers under the law, is a controller or processor of personal data and is therefore subject to conformity assessment and certification with seals and marks according to the provisions of the Law and this Guideline.

   d) "***Audit"*** is the systematic, independent and documented control process, through which audit and assessment data are obtained that objectively determine the extent to which the legal criteria have been met.

   (dh) "***Commissioner****"* is the Information and Data Protection Commissioner.

   e) ***"Law"*** means Law no. 124/2024 "*On Protection of Personal Data*"

HEADING II
RELATIONS BETWEEN THE CLIENT AND THE CERTIFYING BODY

Article 3
Application for certification

1. The client shall submit to the certifying body a written request for certification of one or several personal data processing operations.

2. The client shall provide to the certifying body all the documentation and information necessary for carrying out the certification procedure and provides access to the processing activities.

Article 4
Use of the data protection seal and marks

1. Data protection seals and marks may only be used by those controllers or processors that have obtained the appropriate certification for the processing operations in accordance with the provisions of this Guideline.
2. The client, which has been certified in accordance with the provisions of this Directive, shall publish on the official website, in a prominent place, the result of the certification, specifying the relevant processing operation or operations.

Article 5
Publication of the list of certified entities and reporting to the Commissioner

1. The certifying body shall publish on its official website, in a dedicated space, the list of all clients that have been certified in accordance with this Guideline.
2. By the 31st of December of each calendar year, the certifying body shall submit written information to the Commissioner on the certified clients, specifying the processing operation or operations that have been certified and the issues encountered in the certification process.
3. In the event that the certifying body suspends or revokes the certification in accordance with the provisions of articles 16 and 17 of this Guideline, it shall update the list of all entities that have been certified, published on its official website.

Article 6
Certification time period

The certification issued to the controller or processor is valid for a period not exceeding 3 (three) years and may be renewed according to the same criteria set out in this Guideline.

HEADING III
LEGAL CRITERIA FOR CERTIFICATION AND PROVISION OF SEALS AND MARKS

Article 7
Evaluation criteria

1. The client that meets the following criteria, shall be certified according to the provisions of this Guideline:

a) it is proven that it has an Information Security Management System (ISMS) (ISO/IEC 27001) in place, which is functional and exercises specific controls regarding personal data;

b) it is proven that it acts based on the principles provided for in article 9 of this Guideline;

c) it is proven that it implements the separation of roles and responsibilities of the controller, processor and sub-processors to identify, manage and report personal data breaches or violations;

ç) it is proven that there are internal processes that demonstrate organization in such a way as to enable the exercise of the rights of data subjects;

d) it is proven that there are security/protective measures in case the subject transfers data to third countries or international organizations;

e) it is proven that there are technical and organizational measures that guarantee a level of security appropriate to the risk.

Article 8
Personal data management system

1. The Client shall establish, implement, maintain and continuously improve a *Privacy Information Management System* ("PIMS") in accordance with the provisions of ISO/IEC 27701.

2. The Client shall define and track Key Performance Indicators ("KPI") to measure the effectiveness of the PIMS, conduct management level reviews at least annually, ensure continuous improvement, and plan and conduct internal audits at least annually to assess PIMS compliance and effectiveness.

Article 9
Client guiding principles

1. The assessment carried out by the certifying body should ensure that all processing of personal data is carried out lawfully, fairly and transparently. The legal basis for each processing operation should be identified, documented/recorded and subject to review at specified

intervals or when the processing operation(s) changes, in order to ensure continued compliance and the existence of a need.

2. The records (files) of the processing operation(s) should clearly indicate the purpose of the processing and the legal basis where this processing is based.
3. The client must observe the following principles:
   a) the principle of lawfulness, fairness and transparency;
   b) the principle of processing in accordance with the purpose;
   c) the principle of data minimisation;
   ç) the principle of data accuracy;
   d) the principle of storage limitation in time;
   e) the principle of integrity and confidentiality;
   ë) the principle of accountability.
4. The Client shall conduct ongoing audits to monitor and verify compliance with these principles. The Client shall maintain records demonstrating compliance, including audit reports, verification files or other similar documents.

Article 10
Division of roles and responsibilities of the client

1. The roles and responsibilities of the controller, processor and sub-processors are clearly defined and documented.
2. The agreement(s) on personal data processing shall contain provisions on responsibilities, applicable rules between the parties and liability. The assessment includes due diligence and the implementation of contractual provisions for sub-processors, as well as the retention of records (evidence) for taking measures demonstrating compliance with the accountability principle.
3. The assessment includes verification of whether documented procedures exist to identify, manage and notify personal data breaches or breaches. The procedures for responding to personal data breaches or breaches shall be periodically tested through simulation to ensure their effectiveness.
4. The Client shall notify the Commissioner and the affected parties of the personal data breach or infringement in accordance with article 29 of Law no. 124/2024 *"On Protection of Personal Data*". The notification shall contain complete and understandable information regarding the nature and extent of the breach or infringement, as well as the measures taken to mitigate the consequences within the limited time available.
5. The Client shall implement data protection by design and by default as part of its integrated systems, services and processes. Technical and organizational measures shall be implemented

to ensure that, through data protection by default, only those personal data that are necessary for the relevant purpose are processed.

6. The Client shall conduct assessments that include ascertaining and recording the findings from the personal data breach or infringement, in order to identify opportunities for continuous improvement. The mechanism shall include a regular assessment of the policies and processes for addressing the breach or violation in order to ensure that each incident serves as an opportunity to strengthen preventive mechanisms and response measures. The process is supported by the client's management level commitment to continuous improvement of security measures and shall be recorded to evidence their effective implementation.

Article 11

Exercise of the right by the data subjects

The Client shall organize the processes in such a way as to enable the exercise of the rights of data subjects, including:

a) the right to information;

b) the right to access;

c) the right to rectification and erasure;

ç) the right to be forgotten;

d) the right to restriction of processing;

e) the right to data portability;

ë) the right to object;

f) the right not to be subject to automated decisions.

2. Data subjects shall have the right to a response within the time limits provided for in the Law.

3. The Client shall document and retain all correspondence with data subjects. The request handling system shall include verification of the identity of the requester, registration of the request, tracking of the progress of the processing and shall be reviewed periodically to verify compliance with legal obligations within the time limits.

Article 12

Data protection risk assessment and impact assessment

1. The Client shall carry out a regular assessment of the risks associated with the personal data processing operations.
2. The assessment shall take into account the likelihood, the extent and potential impact on the rights and freedoms of data subjects.
3. A data protection impact assessment shall be carried out for processing operations likely to result in a high risk to the fundamental rights and freedoms of individuals in accordance with

article 31 of the Law and the results shall be recorded, evaluated and integrated into the risk management processes. The data protection impact assessment shall be updated in case the risk may have changed as a result of external factors, such as changes in legislation, technology or organizational policies. This process shall be carried out on an ongoing basis in order to ensure compliance and protection of personal data.

4. The results of the data protection impact assessment and decisions on the treatment of the risk shall be approved by the relevant management structure in accordance with the applicable legislation and the internal regulations of the Client and their effectiveness shall be subject to continuous monitoring. Event-based reassessments shall be performed whenever processing operations change or there are regulatory updates.

Article 13

Technical and organizational measures

The Client shall implement the necessary technical and organizational measures that guarantee a level of security appropriate to the risk and include:

a) pseudonymization and encryption;

b) access control and identity management;

c) resilience and availability restoration capabilities;

ç) continuous testing and evaluation of security measures, including attack simulations and security audits that are necessary to ensure compliance with international standards and identify vulnerabilities that may pose a risk to data.

d) regular penetration testing and vulnerability assessments, including corrective measures.

2. The measures referred to in paragraph 1 of this article shall be reviewed periodically to ensure continued effectiveness. The Client shall take recorded preventive actions that include continuous monitoring and the identification of irregularities.

3. The client shall take ongoing measures to enhance the security of the systems, including analyzing the results of security audits and testing, as well as identifying opportunities for improvement. The process shall include cooperation with external and internal experts, the use of detailed reports on system vulnerabilities and suggestions for improvement. Part of the process is also considered to be the evaluation and updating of security policies to maintain a high level of protection against new risks.

Article 14
International data transfer

1. The transfer of data to third countries or international organizations shall only be carried out if there are safeguards in place as provided for in Heading IV of the Law.
2. The assessment shall include the documentation and preservation of evidence of the transfer mechanism, such as the adequacy decision, standard data protection clauses or binding rules of the group of commercial companies. The adequacy of the transfer shall be reviewed periodically and shall be linked to the specific purpose of the processing and the legal basis.
3. The assessment shall identify the purpose of the data transfer and the relevant legal basis for this transfer. The information shall be recorded in a clear and accessible manner for external inspections and audits, as well as to ensure transparency and conformity in data protection.

Article 15
Internal administration of the client

The management structure of the client undergoing assessment must demonstrate leadership and commitment in relation to the *Privacy Information Management System* "PIMS") by:

a) developing security policies aligned with ISO/IEC 27701 and embedded in internal management and organizational strategies;

b) defining clear roles and responsibilities for data protection, including the appointment of a data protection officer, where necessary;

c) integrating data protection objectives into all organizational strategies of the business activity and the SMSI framework, including key performance indicators that show them.

2. The client shall develop, document and maintain specific policies and procedures on personal data protection.

2. The policies cover the processing of personal data, storage, approval of the governing body(ies) and international transfer and shall be reviewed and updated at specified intervals. Periodic verifications by the management level shall ensure that the policies are consistently implemented.
3. The Client shall conduct data protection training and awareness programs. The training shall be organized based on the respective roles and responsibilities, shall be continuous in nature and documented as training in the management of responsibilities related to personal data. Effectiveness indicators shall be traceable and include the percentages of staff who have completed the training, the relevant assessment, etc.
4. The Client shall maintain documented information on the processing of personal data in accordance with the provisions of article 27 of the Law. The documentation shall include the categories of data, the purpose, the legal basis, the retention period and the transfer mechanisms.

6. The Client shall implement structured processes for assessing the risk of personal data protection. The data protection impact assessment shall be carried out for processing operations that cause high risk, in accordance with ISO/IEC 27701, paragraph 7.2.5, and article 31 of the Law. The results of the risk assessment shall be integrated into the *Privacy Information Management System "PIMS"* and be subject to assessment by the governing body(ies).
7. The Client shall plan and carry out internal audits of the *Privacy Information Management System* "PIMS" in accordance with ISO/IEC 27701, paragraph 5.7.2, to verify compliance with data protection requirements. In the event of non-conformity, the Client shall take corrective measures.
8. The Client shall demonstrate the continuous improvement of the *Privacy Information Management System* "PIMS" and ensure that it is effective, up-to-date and at a level that responds to changes in processing operations or the legal framework.

Article 16
Suspension of certification

1. The certifying body may suspend the certification granted in accordance with this Guideline for a specified period of time if:
a) periodic monitoring or reassessment reveals non-conformities that have not been corrected within the specified period;
b) the client does not make available to the certification body the information, documentation or access requested in the framework of the monitoring activity;
c) significant changes occur in the processing operations, in the organizational structure or in the management system that may affect compliance and that have not been notified to the certification body;
ç) there are investigations concluded by the Commissioner or other competent authorities that may affect compliance with the certification criteria.
2. During the period of suspension, the client must not use the data protection seal or mark in relation to the processing operation(s) affected.
3. The certification body shall document the reasons for the suspension and notify the client and the Commissioner without delay.

Article 17
Revocation of certification

1. The certifying organization shall revoke the certification in cases where:

a) it is found that the client no longer meets the certification criteria, including the requirement to maintain the functionality of the Information Security Management System (ISMS) and the *Privacy Information Management System* "PIMS";

b) serious or repeated violations of the Law have been confirmed;

c) the client results in misuse of the data protection seal or mark or provides false or misleading information;

ç) the certified processing process has been completed, significantly changed or replaced without a prior reassessment.

2. After revocation, the certifying body shall immediately notify the Commissioner in writing, setting out the reasons and shall update the public register of certified entities.
3. The client shall immediately cease using any reference, seal or certification mark and remove them from public communications and the official website.

Neni 18
Re-certification process

1. A client whose certification has been suspended or revoked under this Guideline may re-apply for certification, only after it has established that the reasons for the suspension or revocation no longer exist or have been corrected.
2. The re-certification process follows the same assessment and verification procedures as the initial certification.

Article 19
Transfer of certification

1. In case the client requests the transfer of certification, the certifying body shall act in accordance with the certification scheme and ensure that:

   a) the client has a valid certificate at the time of application;

   b) the certifying body shall receive a copy of the existing certificate, the latest assessment report and documents on the complaints submitted;

   c) the certification body shall assess the existing non-conformities, the findings of the latest assessment, the complaints and the corrective measures;
2. The certifying body shall make a decision on the transfer of certification within one month. In case of missing documents or doubts about the client's conformity, the certifying body shall not transfer it and shall start the certification process from the beginning.

HEADING IV
TRANSITORY AND FINAL PROVISIONS

Neni 20
Transitory provisions

Certifications issued before the entry into force of this Guideline, under the Commissioner's Guideline no. 48, dated 14.09.2018 "*On System of Certification of Information Security Management, Personal Data and their protection*" will remain valid until their expiration.

Article 21
Final provisions

1. All public and private controllers/processors in the territory of the Republic of Albania shall be responsible for respecting and implementing this Guideline.
2. Failure to comply with the requirements of this Guideline constitutes a violation of the Law and is sanctioned, according to article 94 thereof.

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

COMMISSIONER

Besnik Dervishi