INSTRUCTION

No. 48, dated 14/09/2018

ON

"CERTIFICATION OF INFORMATION MANAGEMENT SYSTEMS, PERSONAL DATA AND THEIR PROTECTION"

Pursuant to Article 31/1/f and Article 27 of the Law No. 9887, dated 10.03.2008 "On personal data protection", as amended, and in alignment with the EU Regulation 2016/679 of the European Parliament and Council, dated 27 April 2016 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), the Information and Data Protection Commissioner;

INSTRUCTS:

Article 1

Object

The object of the Instruction is the certification of information management systems, personal data and their protection, in accordance with personal data protection legislation, as well as defining of the certification mechanism and its validity.

Article 2

Scope

This Instruction is applicable to all entities that are subject to implementing the Law No. 9887 dated 10.03.2008 "On personal data protection", as amended, (hereinafter "the controllers") which shall apply with the accredited body for certification of information security management systems of personal data and their protection.

Article 3

Definitions

1. Terms and definitions used according the Law No. 9887 dated 10.03.2008, as amended, shall apply and have the same meaning for the purposes of this Instruction

2. "Accredited body" means an accredited body certified by the responsible accreditation entity and authorized by the Information and Data Protection Commissioner (hereinafter the Commissioner) in the quality of the supervisory authority, according the criteria set forth in Article 7, which performs the assessment of compliance of personal data processing with the relevant legislation, through the independent exercised control.

3. "Conformity/compliance certificate", is the document issued by the accredited body to/for controller/s that fulfilling legal requirements to processing of personal data, without prejudice to the activity of the Commissioner.

4. For the purpose of this Instruction, the terms and definitions defined in the International Standard ISO/IEC 27001 apply.

Article 4

Certification and controllers' obligation

1. The certification is required by the controller and is carried out in a transparent process.

2. The certification is issued for a period up to three years eligible for renewal where the accredited body finds that the respective requirements are still being fulfilled.

3. The certification is cancelled, as appropriate, by the Accredited Body when the requirements for certification are not met or not being fulfilled.

4. The controller which subdues the processing that carries out to the certification mechanism, makes available, to the Accreditation Body, information and provides full access to its processing activities, which are necessary for performing the certification procedure.

Article 5
The security management system

The controller establishes, maintains and improves constantly a management system of information security, in line with the requirements of International Standard ISO/IEC 27001, according to the last version.

Article 6

The register of certified subjects

1. The Commissioner's Office establishes a Register of certified controllers for the management system of information security, personal data and their protection.

2. The Accredited Body notifies to the Commissioner on a case-by-case basis on the certified controllers.

3. The Accredited Body informs the Office of the Commissioner on the reasons of providing or either cancelling of the requested certification, aiming to demonstrate the appropriate security measures in place.

4. The Register of the certified controllers on the management system of information security, personal data and their protection, is published on the official website of the Commissioner.

Article 7

The Accredited Body

1. The Accredited Body is the authorized subject by the Commissioner for carrying out independent controls on certification of information security management systems, personal data and their protection.

2. The Accredited Body exercises its activity pursuant to and in line with the principle of transparency in relation with the Commissioner and stakeholders.

3. The Accredited Body exercises independently the inspection activity with controllers.

4. The Accredited Body exercises the control activity with controllers, aiming at supervising the conformity of their information security management systems, personal data and their protection under the personal data protection legislation.

5. During the control operation, the Accredited Body also considers the application of requirements of the Instruction No. 47 dated 14/09/2018 of the Commissioner "On Determining Rules for Safeguarding Personal Data Processed by Large Controllers".

6. The Accredited Body issues the certificate of compliance to controllers, according to the adopted model by the Commissioner, attached to this Instruction.

7. Concerning the processing of personal data according to Article 7/2/c of the Law on Personal Data Protection and personal data as per Article 9, paragraph 1, the issued certificate by the Accredited Body, has influence on issuing/providing of authorization by the Commissioner.

Article 8

Criteria for authorization

1. Every subject that requires authorization by the Commissioner in order to certify controllers, in accordance with this Instruction, should:

   a) The association (partners, experts or its auditors) should have experience in the certification field under the ISO/IEC 27001 Standard for at least a period up to 10 years.

   b) The association should be accredited by the responsible accreditation body in the Republic of Albania in accordance with ISO/IEC 17021-1:2015 Standard "Conformity assessment – the requirement for bodies carrying our assessment and certification of management systems" as a certifying body of information security management systems in conformity with ISO/IEC 27001 Standard.

   c) Successfully implement the legislation on personal data protection, in case of an investigation from the Commissioner's Office;

   d) Appoint the responsible person for the protection of personal data;

   e) Demonstrate independence and its expertise in relation to the scope of certification;

   f) Have determined procedures and structures to administer complaints on breaches of certification or on the manner how the certification has been handled, or is being implemented by the controller or processor and make transparent these procedures and structures for the data subjects and the public;

   g) File with the Commissioner's Office the procedures with regard to avoiding conflict of interest during the exercise of the its task and functions in accordance with this Instruction;

gj) The certifying bodies with adequate level of expertise regarding data protection, should provide and renew the certification, without prejudice to functions and powers of the

Commissioner's Office, after notifying the latter, so as to have his authorization in order to exercise their functions.

2. The Commissioner revokes authorization provide to the Accredited Body when conditions have not been met or where actions taken by the Accredited Body result in a violation of personal data protection legislation.

3. The Commissioner revokes certification for the controller (when the Accredited Body does not exercise this requirement) or orders the Accredited Body to not issue the certificate if the criteria for certification is not met.

Article 9

The Register of Accredited Bodies

The Office of the Commissioner registers all Accredited Bodies on a record and makes them public on its official website.

Article 10

The model of management of the information security, personal data and their protection

1. The model of management of certified controllers by the Accredited Body according to this instruction, shall be considered as compliant with the requirements of the legislation in force on personal data protection.
2. The inspection bodies depending on the Commissioner, to the effect of scheduling their controls, shall take into account the certification compliance owned by the subject as object of control, issued by the Accredited Body according to this Instruction.

Article 11

Final provisions

1. Failure to implement this instruction will be subject to sanctions of the Law No. 9887/2008 "On Personal Data Protection', as amended.
2. Controllers are bound for the implementation of this instruction.

Article 12

Entry into force

This Instruction enters into force after the publication on the Official Gazette.

COMMISSIONER

Besnik Dervishi

Annex 1

{Logo of the Accredited Body}

Conformity/Compliance Certificate

Issued to:

[the Certified Controller]

Headquarter: St….. no. – Albania

USIN: 000000000000

[The Accredited Body] certifies that the Information Security management System, personal data and their protection, is verified and results as compliant with the requirements of the Law No. 9887/2008 “On personal data protection” and sub-legal acts in implementation of this law, as well as meeting the requirements of the Standard

ISO/IEC 27001…

On the included activities in the Enforcement Declaration

Certification No.____ Code/s IAF: ____

Date of issue:

Date of expiry:

On the Accreditation Body

[Name/Surname of the representative]

[Signature]

Address of the Accrediting Body: _____

For clarifications regarding the implementation and the authenticity of this certificate you may contact the following number

(.....)