INSTRUCTION

No. 47, dated 14/09/2018

ON

"DETERMINING RULES ON SAFEGUARDING PERSONAL DATA PROCESSED BY LARGE ENTITIES"

Pursuant to Article 31/1/f and Article 27 of the Law No. 9887, dated 10.03.2008 "*On personal data protection*", as amended, the Information and Data Protection Commissioner (hereinafter the Commissioner).

INSTRUCTS:

1. Determining of organizational and technical security measures also in relation the staff, for the protection of personal data processed by large processors, referred below as large Processors of personal data, as well as the rules of their cooperation with the Commissioner.

2. For purposes of this Instruction, the following definitions mean:
   a) "*Large processing entities"* are the controllers or processors, which process personal data, electronically or manually, with 6 or more persons carrying out the processing, either directly or by processors;
   b) "*Assessment report*" is the report of the latest inspection of security carried out in the storage system;
   c) "*Information Security Policy*" (referred below as "ISP") is the document through which the data processor notifies its employees and contractors (processors) the means of establishment, enforcement and operation of the Management System of Information Security (referred below as "MSIS") on data protection;
   d) "*contact person*" is the person to whom, the data processing subject has provided access to personal data

3. The main categories of users that are obliged to safeguard personal data are the following:
   a) Administrators of Information and Communication Technology Systems (hereinafter as ICT) and their security, who enforce this requirement, when the data processing entity has in place an ICT system either internal or external in order to fulfill this purpose.
   b) Personal data operators (employees, contractors, etc.), whom process personal data aiming at fulfilling their tasks when they work for the data processing entity.
   c) All individuals assigned by the processing entity to process data manually.

4. Except as provided for in the Instruction on controllers' obligations prior to the processing of personal data, the processing entities shall process personal data in accordance with the rules set forth in this Instruction as well.

5. Provision related to the security of ICT system are obligatory to entities who process personal data electronically. As per those that process personal data manually, the respective provisions on physical security, premises and personnel security will be applicable.

6. The Commissioner may, at any time, request the data processing entity to demonstrate the level and content of the technical and organizational measures, and also in relation to the personnel through an assessment report. The assessment report shall be compiled by the data processing entity for a period of no longer than 2 years, prior to the request of the Commissioner. The data processing entities shall submit the assessment report within fifteen days since the day of request. If the assessment report is not sent within the deadline, the Commissioner asks the data processing entity to carry out a new inspection under its expenses, and submit it within a three months period.

7. The inspection of security system of the data processing may be performed only by an independent and impartial and professionally qualified auditor, who has not been part of the development, implementation and controlling of the Information Security Management System of the storage system.

Chapter I

Information Security Management System (ISMS) on data protection

8. The establishment and maintenance of the ISMS on data protection is binding to all processing entities. This system is based on identification, analysis and mitigation of risks against the security of personal data taking into account the imperfection of:
   a) ICT systems used for the processing of personal data;
   b) All forms of manual processing of personal data;
   c) Physical security, both inside and outside of the premises, personnel security and electronic or portable devices.

9. In cases when the controller uses more than one processor, every processor shall put in place an ISMS. The division of responsibilities among the parties should be explicitly expressed in the contract regulating their relation. All these requirements shall be met without prejudice on the contractual relation of outsourcing. When the controller uses a processor, the latter will be notified only for the applicable parts of ISMS, which will be legally binding in a contract on data processing.

10. ISMS will be defined taking into consideration the following standards of information security:

    a) "*Confidentiality*", ensuring that the data are accessible only for authorized persons;
    b) "*Integrity*", ensuring that the data are accurate, complete and by maintaining methods of their processing;
    c) "*Availability*", ensuring that the authorized user accesses data and processing systems;

    ç)"*Trust*" of ICT systems that are used to process data and of the personnel having used them, ensuring that every action/activity performed by them on data is traceable and verifiable.

11. ISMS shall particularly include:
    a) Data Protection Impact Assessment. Prior to the processing of personal data, the controller or processor shall carry out a likely impact of the data protection activities in the protection of personal data identifying where these processing activities present particular risks on the rights and freedoms of data subjects due to the nature, the extent or their purpose;
    b) Information security policy, including the security of personal data processing;
    c) The inspection of storage system security of personal data;
    d) Detailed instructions on security covering specific areas;
    e) The personnel security and electronic devices either portable or not.

12. ISMS should operate in accordance with legal and sub-legal acts in force, technical standards on ICT security systems, rules of good practice in the field of information security, and recommendations drafted by professional industrial organizations, including banks, telecommunication sector, insurance companies, social insurance and healthcare sector. ISMS should be adapted to the level of risks and weaknesses of the data processing systems.

13. In case when data processing is performed through cloud computing or by means of portable processing, additional security measures will be applied (such as the activations of the antitheft service in the portable computer or on smartphone). All devices serving as data carriers will be encrypted. Storage of personal data in these services shall be carried out in line with the purpose of their collection. The data may be kept out of the deadline retention only by priory notifying the data subject and obtain his consent explicitly as well as by providing the right of withdrawal. The destruction process is carried out irrevocably. Personal data processed through these services should not be transferred out of the European Union member states and Albania, without taking in advance the opinion of the responsible authority on personal data protection.

14. The processing entities determine the steps that should be taken in the event of a data breach. After the risk analysis results, appropriate measures should be taken to mitigate the likelihood and impact of the data breach. ISMS should also include the specific agreements for the continuity of the commercial activity, for which, technical standards and recommendations made available to the public will be applicable.

15. ISMS papers are kept by the data protection officer, appointed by the processing entity of personal data. This documentation should be made available to the Commissioner, upon his request, within the determined deadline from the date of receipt.

Chapter II

Information Security Policy

16. ISP should be developed and implemented respectively by the personal data processing entity.

17. ISP is developed and kept in line with the rules of information security, as stipulated by legal and sub-legal acts in force and the international legislation recommended by the defined security standards, as well as the recommendations of the Commissioner. Risk analysis is an integral part of ISP. The ISP document clearly specifies the objectives of security and determines technical and organizational measures, and also in relation to the staff, for the mitigation of threats and risks affecting storage systems.

18. Regarding the establishment of the ISP, particular attention is paid to the technical standards of information security, codes of good practice, as well as special recommendations and instructions by the Commissioner. ISP shall cover the following aspects on the information security of personal data:

    a) Assessment and handling of the risk through carrying out risk analysis to information security of the processing entity;
    b) The Security Policy which implies the adoption and enforcement of the document testifying the support and commitment of the entity governing structure to information security;
    c) The organization of the information security through undertaking of measures in order to protect information and its systems from unauthorized access and by performing security checks. ;

    ç) Asset management by updating the inventory of all means of processing and classification of security conditions to define what will be protected, why and how;

    d) Human resources security by taking security measures for the employees being recruited, dismissed or fired from the processing entity;

dh) Environmental and physical security through the protection of computer devices;

e) Operation and communication management by technical security checks in the systems and computer networks;

ë) Access control through restrictions of access rights on the web, systems, applications, functions and data;

f) Purchase, development and maintenance of information processing systems by applying security in applications;

g) Management of information security breach (referred to as incidents) through anticipating and provision of the reaction against the information security breach;

gj) Management of the continuation of commercial activity through protection, safeguarding and recovering of critical processes and systems;

h) Ensuring compatibility with special policies of information security, standards, laws and regulations.

19. When implementing provisions of this Chapter, the following are dealt with separately by ISP:
    a) Processing of sensitive data
    b) Management of access rights
    c) Risks deriving by the access on public networks, particularly from the web.

20. ISP specifies core objectives of security that should be achieved for the protection of the storage system of personal data against the breach of its security and in particular it should:
    a) Determine objectives for core security and measures for the minimum security required;
    b) Determine technical and organizational measure, also in relation to the staff for the security of personal data in the storage system and the manner of their use;
    c) Illustrate the storage system and its connection with potential security breach;

    ç) Define boundaries that determine the remained risks.

21. The security analysis of storage system implies a detailed analysis of the state of security, in particular including:
    a) Risk analysis, in which threats affecting individual parts of the storage system are identified, able to breach security or its functioning; risk analysis result will be a list of threats that may threaten confidentiality, integrity and availability of personal data processed, while it will also include the scale of the potential risk, proposals on measures to remove or mitigate the risk impact and a list with remaining risks;
    b) The use of security standards and determining of other methods and means of security proposed by the applied security standards, methods and means shall form a part of security analysis of the storage system.

c) Development of detailed regulations on security which will specify and implement result deriving from ISMS according to the concrete conditions of the storage system activated, which will include, in particular:
   i. Description of organizational and technical measures also in relation with the staff as defined in ISMS and their use in concrete conditions;
   ii. Extension of powers and description of permitted activities of individuals enjoying those rights, means of their identification and verification during the access in the storage system;
   iii. The object of responsibility of persons in charge and the contact person;
   iv. Manner, form and periodicity of performing inspection activities focused on surveillance of the security of storage system;
   v. The procedures during failures, abortions and other extraordinary situations, including preventive measures for restriction of developing extraordinary situations and possibilities for efficiently restoring the state as it was before breakdown.

Chapter III

Special cases of processing

22. The following provisions are applicable to entities that process personal data manually:

a) All documents processed manually will be safeguarded in order to prevent illegal disclosure, destruction, and loss, as in the workplace and also during their transfer;
b) Making available the requested copies, may be carried out under the condition where it allows further traceability of their use to their destruction or anonymization;
c) Upon the expiration of the retention period, the documents:
   i. Are stored, where there is in place a legal requirement; or
   ii. Are physically destroyed irrevocably; or
   iii. Become anonymous irrevocably.

ç) In case when it is not anticipated by the legislation in force, which regulates the special processing of data, the data retention deadline is defined by the controller in accordance with the purpose of data collection. For any change in the deadline of retention, the controller reconsiders the period of retention and also notifies the data subject. After the expiration of the data retention deadline, the data subject will irrevocably be removed from all active systems of data processing, either automatic, manual or anonymized.

23. Concerning entities that process sensitive data, either manually or electronically, the following additional rules will be applicable, respectively for any manner of processing:

a) Particular attention is paid to preventing of illegal disclosure:
   i. In case of a manual processing, ISMS sets forth additional specific procedures for handling of documents aiming at preventing of access by unauthorized persons to personal data contained in these documents, throughout their lifecycle;
   ii. In case of an electronic transfer of data, transfer channels or documents containing these data will be encrypted, by using encryption methods in accordance with the results of risk analysis carried out in advance;
   iii. In case of the use of portative electronic means as information carriers, the data will be encrypted before transferring them out of the premises of the processing entity. This encryption is also encouraged to be carried as well on non-sensitive data.

Chapter IV

Training of the staff of the Processing Entity on Personal Data

24. The staff of personal data processing entity will be trained on regular basis on the protection of personal data. The training will be held following the instructions listed below:
    a) The staff that processes personal data will be trained at least once per year;
    b) The staff, except for the definition in letter "a", will be trained for all cases as listed below:
       i. After any substantial change of the law on personal data protection;
       ii. After any essential amendment of the EU legal framework on personal data protection, which is published in advance on the Commissioner's official website;
       iii. After the change of the organization of ISMS, in particular ISP;
       iv. After the change of special procedures of the data processing security of the processing entity.

The purpose and the form of training organization should be applied in accordance with provisions of this instruction.

25. The personal data processing entity ensures professional training to the persons in charge. The Commissioner may request the processor to demonstrate proofs on organization of professional trainings.

Chapter V

Control of the information security of the personal data processing entity

26. The control of information security (personal data) will be carried out not less than once per year by the controlling entities.
    The control reports should be made available to the Commissioner upon his request.

Chapter VI
The contact person in the processing entities

27. The data processing entity is responsible for the internal supervision of the protection of personal data processed. Every processor being subject to this instruction shall, at least, provide a written authorization to appoint a person in charge to carry out this supervision. The processing enttiy shall notify the Commissioner for the authorization of only one contact person, even though it may appoint several persons for the internal supervision on data protection. If the subject replaces the contact person, it should notify the Commissioner no longer than 14 days since the day of replacement.

28. The processor being subject to this instruction, may designate one or more persons in charge, whom are responsible for guaranteeing appropriate security of personal data, when acting on behalf of the controller. Small processors contracted by the processing entity which is subject to this instruction, are also advised to appoint a person in charge.

29. The contact person may be any individual that meets the following criteria:

    a) Enjoys full legal capacity to act;
    b) Enjoys integrity;
    c) Has higher legal education or computer science;
    d) Known for professional capability and pure ethical-moral figure;
    e) Has working experience for no less than 5 years as lawyer or IT expert, or has been working for more than 3 years at the Commissioner's institution as a lawyer or IT expert;

    dh) not been convicted with a final decision on any criminal offence.

    He submits an updated certificate of the judicial status, which is obtained by the controller during the performance of his function.

30. Prior to the initiation of personal data processing in the storage system, the contact person makes a risk assessment on potential breach of the rights and freedoms of data subjects. This analysis is an integral part of the data protection impact assessment.

31. In a timely manner, the contact person makes a written notification with the data processing entity for any potential of breach of the data subjects' rights, including thereto the violation of personal data protection legislation.

32. In case that, after the notification of the contact person, the personal data processing entity fails to take appropriate measures for dealing with the problem in a timely manner, the contact person shall notify the Commissioner without delay.

33. Within 30 days from the date of concluding the internal supervision, the personal data processing entity that has authorized the contact person, shall notify the Commissioner. The notification should contain:

a) The name, address, identification number (BIN) and/or subject legal representative;
b) Generalities of the contact person;
c) The position of the contact person within the processing entity;

ç) Date of appointment of the contact person;

d) Declaration of the processing entity where is defined that the contact person meets the criteria set forth in point 29.

34. The contact person has the following tasks and responsibilities:
a) Is responsible for the internal supervision and for meeting the data protection requirements from the data processing entity;
b) Provides advice to the responsible persons;
c) Is responsible for the implementation of organizational and technical measures, also in relation to the staff, as well as oversees their execution in practice. In particular, he will provide the ISMS documentation demonstrating the development and its appropriate maintenance;

ç) In case when the data processing entity contract a processor, the contact person is responsible for the internal supervision of the processor's activity, for the content and development of the contract with the processor. In the course of contract relation or authorization, the contact person shall verify the fulfillment of the adopted criteria, including the commitment and change of Processors, in case of.

d) is responsible for the internal supervision of international personal data transfers;

dh) is responsible for submitting the documentation of storage system for special registration and announcements of changes and de-registration of storage systems form the special register. He keeps storage system data that are not subject to registration and makes them available to anyone legally entitled to have access on;

e) Is responsible for the necessary co-operation with the Commissioner in order to fulfill the tasks within his responsibilities;

ë) Upon the request of the Commissioner, he is obliged to submit in writing the authorization allowing him to act on, as well as provide information on the level of knowledge acquired in professional trainings.

35. After designating the contact person for the internal supervision of personal data protection, the personal data processing entity is exempt from the obligation to provide for registration on storage systems of non-sensitive data.

36. The contact persons maintains on regular basis, an inventory of storage systems of personal data processed by the processing entity of personal data, including personal data exempt from the obligation for registration under the authority of the Commissioner.

37. The access in this inventory of storage systems of personal data is provided to the Commissioner and data subjects, the data of whom are processed in the special storage system, without delay, on the basis of a request.

38. The data processing entity is obliged to allow the contact person to conduct, independently, the internal supervision of the protection of personal data and accept its legal proposals. The notification of deficiencies or making of a request by the contact person regarding the fulfillment of his obligations, should not be inducement or reason for performing an action by the entity against the contact person.

39. The Commissioner is entitled to communicate and request the data processing entity to authorize another person in charge for the internal supervision on personal data protection, under the condition that the previous authorized person has failed and has not accomplished sufficiently his obligations, or has incorrectly evaluated or applied in practice the rights and obligations of the entity set forth in this act, or does not meet the ethical or professional criteria.

40. The data processing entity is obliged to fulfill the request of the Commissioner in a timely manner and authorize, within 15 days, another person for the internal supervision.

41. If not possible, for objective reasons, to respect the deadline defined in point 40, the Commissioner will provide an additional month to the data processing entity.

Chapter VII

Compliance rules

42. The following rules will be followed to ensure the appropriate compliance with this instruction:
    a) The formal risk analysis approach to the information security shall be approved based on the information security standards, so as personal data protection be an inseparable part of ISMS within the processing entity;

b) If the processing entity has decided to certify its compatibility with technical standards of security, it should make available this certificate to the Commissioner. The certification process on compatibility with information security standards shall include also identification, management and mitigation of weaknesses and risks of personal data security;
c) Serious breaches of personal data security shall be notified immediately to the Commissioner. In case when a contact person is appointed, then it will be his duty to make such notification.

43. The updated control reports may be fully acceptable as proof of compliance with the law on personal data protection, by the processing entity, only when the above steps have been enforced and compliance certifications with information security standards covering also personal data processing have been saved by the entity.

44. Prior to entering into a contract that includes personal data processing, the controller is obliged to inspect the Processor on his compatibility with the law on personal data protection.

45. On this basis, the Commissioner may request the contact person to carry out a part of procedures of inspection, including the control of sensitive data records in advance.

46. Both public and private controllers situated in the territory of the Republic of Albania are subject to this instruction, as determined in letter a) of point 2 in this instruction.

47. Failure to implement requirements of this instruction, consist in violating the law on personal data protection and is sanctioned based on Article 39 of the law on personal data protection, as amended.

48. The Instruction No. 21, dated 24.09.2012 “On determining rules for safeguarding personal data processed by large controllers” as amended, is repealed.

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

COMMISSIONER

Besnik Dervishi