Instruction

No. 22, Date 24.09.2012

Official translation of the text published
in the Official Journal No. 136, date 18.10. 2012[1]

On

"Determining the rules for safeguarding the personal data processed by small controllers"

Pursuant to letter "f", point 1 of Article 31, and pursuant to the obligations defined under Article 27 of the Law No. 9887, dated 10.03.2008 "On the protection of personal data", *as amended* the Commissioner for the Protection of Personal Data gives the following

INSTRUCTIONS:

1. Provision of fundamental organisational and technical measures for protection of personal data processed by small data Controllers, or Processors, hereinafter referred as personal data processing entities, and the rules of their co-operation with the Commissioner.

2. Small controllers or processors are considered all personal data processing entities which:

a) process personal data, electronically or manually, engaging less than 6 persons to carry out such processing, either directly or through Processors,

b) do not process sensitive data.

3. The main categories of users, in charge of the duty to safeguard personal data are:

a) Administrators of Information, Communication Technology (hereinafter ICT) systems and of

[1] The translation was commissioned by the EU funded Project "Strengthening of the Data Protection Commissioner office in Albania, for alignment with EU standards"

their security, which are subjected to this obligation when the entity which processes personal data has an internal and/or external ICT system established for such purpose.

b) Personal data operators (employees, contractors, etc.) which process personal data for the purpose of fulfilling their tasks while working for the personal data processing entity.

4. Besides to what is provided under Instruction No. 2, date 25.02.2010 "On the obligations of the controllers and processors prior to processing personal data", the data processing entities, as defined above, shall process personal data also in compliance with the rules defined in this Instruction.

5. The processing entities are responsible for the security of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and making them available to unauthorized persons, and against any other unauthorized form of processing. For this purpose they shall take adequate technical and organizational measures appropriate to the processing manner, while they shall take into account, above all:

a) the existing technical means,
b) the level of potential risk that could violate the security or functioning of personal data processing system.

6. The processing entities have to prove the level and content of the technical and organizational measures taken according Paragraph 5.

7. Any processing entity may authorize, in writing, a person in charge of supervision of safeguarding personal data.

8. Minimal standards for the security of personal data shall include:

a) **Risks analysis**:

1) The risk analysis identifies the threats affecting individual parts of the filing system, which are able to breach its security or functioning. The outcome of risk analysis is a list of threats which can endanger the confidentiality, integrity or availability of personal data processed, whereas it states the level of potential risk, proposals of measures to eliminate or minimize the risk impact and a list of residual risks;

2) The risk analysis is carried out periodically in order to identify the major risks the systems are exposed to, and documenting thereof comprehensibly for data processing entities' business practice;

b) **Physical and environmental security**:

1) The information processing systems, programs or ICT equipment where a database is kept are accessed by means of a password. Backup of data (security copy) is always made in another safe premise.

2) Physical access to personal data ICT processing equipment is granted to authorised persons only and records of their identity are kept.

3) All physical media containing personal data are destroyed when they have fulfilled the purpose for which they were collected or processed for ,and in particular, printouts, including photocopies, photographs, and other data carriers, CD ROM, DVD ROM, TAPE (backup recording tape), forms, physical registries.

4) In the case of portable electronic equipment storing personal data as well as other memory tools, the destruction shall be in content in a manner that restoring of information is no more possible.

5) A "*clean desk policy*" is implemented in case of contracting service providers which are allowed to enter your premises on your absence such as office cleaning and maintenance, building security, technical services, etc.

c) Logical security of personal data processing ICT equipment:

1) If you own ICT equipment for processing personal data:

a. Possess legally personal data processing software which enables security updates for eligible users.

b. Install security measures to:

- Grant individual access to enable each user to work on his personal account using authentication means, such as “user name” and “password”,
- Limit the possibility to attach external media depending on the scope for which it is required, and continuous controlling thereof by blocking other access routes.

c. If case of using an external service contracted to maintain your ICT equipment for processing personal data:

- treat as your employee the employee of the contracted party who may have access to your personal data while carrying out their duties:

- include the corresponding personal data processing security in the contract with such a party, to guarantee the latter to have formal access to personal data or to the systems which contain personal data.

d) In case of using external service renting ICT equipment for your personal data processing:

- use the security components advised by the service provider;
- upon the termination of the rental contract, destroy personal data from the systems and equipment to be returned to the ICT equipment’s owner, so as restoration of previous information is no more possible.

2) Public networks access:

a) If possible, contract Internet access service providers offering the network security components, and install them, if necessary, on the ICT equipment used.

b) In case of renting personal data processing equipment from a professional third party, contract the service that offers up-to-date network security components.

c) In case of using wireless internet connection, do not use non-encrypted access point and comply with security standards for such access.

ç) Personnel’s security:

1) The employees shall be informed of the major security risks they are exposed to.

2) In case of new recruitments, training shall be organized correspondingly to the risks identified, and on personal data related to employment are kept confidential.

3) Instruct the respective personnel to keep confidential all authentications, identification means available for accessing the ICT equipment available used for processing personal data.

4) Revoke access immediately after the employee is no longer required to process personal data.

9. For entities processing personal data manually, the provisions provided in point 22, Chapter III of Instruction No. 21, date 10.09.2012, "On determining the rules for safeguarding of personal data processed by Large Entities" are applicable:

All private and public controllers, in the territory of the Republic of Albania, as defined under point 2 herein, are in charge for applying this Instruction.

Non-fulfilment of requirements of this instruction constitutes a violation of personal data protection law and is sanctioned under article 39 of the Law on protection of personal data, as amended.

This Instruction enters into force 6 months after its publication in the Official Gazette.

COMMISSIONER

FLORA ÇABEJ(POGAÇE)