DECISION

No 6, dated 05.08.2013

ON DETERMINING EXPLICIT RULES FOR PERSONAL DATA SECURITY

Pursuant to paragraph 5 of article 27 of law no. 9887, dated 10.3.2008 "On the protection of personal data" as amended, the Personal Data Protection Commissioner

DECIDED:

Defining various mandatory rules to be applied by public and private controllers during the processing of personal data, as follows:

The controller is obliged to:

1. Define the categories of personal data and sensitive data that are processed.
2. Define the levels of access to data in accordance with the work profile, in terms of data processing and protection.
3. Draft and approve regulations "On the protection, processing, storage and security of personal data", based on the draft project/regulation drafted by the Personal Data Protection Commissioner.
4. Take the necessary steps and ensure that staff are aware and trained on the need for security and its reinforcement.
5. Draft and implement the privacy policy.
6. Each employee who mainly processes sensitive data must sign the "Declaration of confidentiality", according to the model attached to this decision.
7. Draft and implement rules for the security of access to the premises in which it operates.
8. Draft and implement rules for *"Clean desktop"*
9. Make inventories for electronic devices such as computers, photocopiers, servers, laptops, etc.
10. Design and implement written procedures for removing electronic equipment outside the controller premises.
11. Draft and implement written procedures for keeping records related to modifications, destruction and data transfers during their processing. Procedures should provide for the processing of data manually and electronically.
12. Draft and implement written procedures "For Business Continuity" in case of incidents and security breaches. The system should guarantee integrity, availability and reliability on an ongoing basis.
13. Failure to comply with the obligations set out in this instruction will be sanctioned under Article 39 of the Law on Personal Data Protection, as amended.

All public and private controllers are responsible for the implementation of the requirements of this decision, which during their work activity must also implement the legal provisions set out in Instruction no. 21, dated 24.09.2012 "On determining the rules for maintaining the security of personal data processed by large controllers", as amended and Instruction no. 22, dated 24.09.2012 "On determining the rules for maintaining the security of personal data processed by small controllers", as amended.

Decision No. 1, dated 04.03.2010 “On determining explicit rules for personal data security” is repealed.

This instruction enters into force immediately and is published in the Official Journal.

COMMISSIONER

Flora Çabej (Pogaçe)

CONFIDIALITY DECLARATION

Subject

This statement is addressed to all _____ staff, as well as temporary staff, volunteers and other parties who have access to the information held by _____.

Purpose

This statement must be signed by all employees who have access to _____ personal data. It sets out the requirements and responsibilities of those who have access to such information and ensures that all stakeholders understand their confidentiality obligations.

Scope

The scope of this statement extends to all personal data and confidential information known while working on _____. Relevant provisions apply even after the employment relationship with _____ has ended.

Statement of confidentiality

1. By this statement I undertake not to use or transmit to unauthorized persons personal data or confidential information in connection with or obtained from _____, unless expressly authorized by _____, or required by law. I understand that this obligation applies during the term of employment as well as after its termination.
2. I understand that the use and disclosure of personal data related to individuals, is addressed by law no. 9987, dated 10.03.2008 on “Personal Data Protection”, as amended. I will not use or disclose any personal data I become aware of during my work for any purpose that is inconsistent with the purposes of this work.
3. I understand that I am obligated to maintain the confidentiality of personal data and to keep it secure, taking all appropriate organizational and technical measures.
4. I take full responsibility that if it is found that I have acted contrary to the instructions regarding the confidentiality of personal data or in case of non-storage of them, immediate action will be taken against me. I understand this move as a need to maintain high professional standards in _____.

Employee’s signature Superior signature

_____ _____

Dated Dated