ORDINANCE № 1

dated 30 January 2013

on the minimum level of technical and organizational measures and the admissible type of personal data protection

(repealed as of 25 May 2018)

Chapter One
GENERAL PROVISIONS

Article 1. This Ordinance defines the minimum level of technical and organizational measures to be provided upon personal data processing and the admissible type of protection.

Article 2. The Ordinance aims at ensuring adequate level of personal data protection in the maintained registers with personal data against accidental or unlawful destruction or accidental loss, unauthorized access, alteration or dissemination, and against any other unlawful forms of processing.

Article 3. (1) The personal data controller (the controller) shall define the type of personal data, the purposes and means of their processing, unless they are defined by law.

(2) Upon implementing the activity referred to under para. 1, the controller shall structure a set of personal data for the purposes of the respective register.

(3) The controller shall process personal data in the registers maintained in accordance with the principles under Article 2, para. 2 and 3 of the Personal Data Protection Act.

Article 4. (1) The controller shall take the necessary technical and organizational measures to protect personal data in order to ensure an adequate level of protection corresponding to the personal data being processed and the impact in case of violation of their protection.

(2) The measures under para. 1 aim to ensure confidentiality, integrity and availability of personal data.

Chapter Two
TYPES OF PROTECTION

Article 5. The types of data protection are physical, personnel, documentary protection, protection of automated information systems and/or networks and cryptographic protection.

Article 6. (1) Physical protection of personal data is a system of technical and organizational measures to prevent unauthorized access to buildings, premises and facilities, where personal data is being processed.

(2) The basic organizational measures of physical protection are:

1. identifying the areas with controlled access;

2. determining the premises where personal data are to be processed;

3. determining the premises where the elements of the communication and information systems for personal data processing are to be located;

4. determining the organization of physical access;

5. determining the regime of visits;

6. determining the use of technical means of physical protection;

7. appointing a team to respond in case of violations.

(3) The basic technical measures of physical protection are:

1. locks;

2. cabinets;

3. metal safes;

4. equipment of the areas with controlled access;

5. equipment of the premises;

6. devices for physical access control;

7. security guards and/or security system;

8. perimeter protection devices;

9. firefighting devices;

10. fire detection and extinguishing systems;

11. devices detecting substances (metal, explosives, etc.).

Article 7. (1) Personnel protection is a system of organizational measures towards individuals who process personal data upon the instruction of the controller.

(2) The basic personnel protection measures are:

1. knowledge of legislation relating to the protection of personal data;

2. knowledge of policies and guidelines for the protection of personal data;

3. knowledge of threats to personal data processed by the controller;

4. sharing critical information among employees (e.g. IDs, passwords for access, etc.);

5. consent to assume an obligation of non-disclosure of personal data;

6. training;

7. training the employees to respond to events that threaten the security of personal data.

(3) The measures for personnel protection shall guarantee access to personal data only to persons whose official duties or a specific task require such access upon implementing the need-to-know principle.

(4) The individuals may begin to process personal data after having been acquainted with:

1. legislation relating to the protection of personal data;

2. policies and guidelines for the protection of personal data;

3. threats to personal data processed by the controller.

(5) The individuals shall sign a declaration of non-disclosure of personal data to which they have been given access while performing their obligations.

(6) The controller shall maintain the information necessary for the performance of their obligations under Article 2, item 5, 6 and 7.

Article 8. (1) Documentary protection is a system of organizational measures taken in the course of processing personal data in paper copies.

(2) The basic measures of documentary protection are:

1. determining the registers which will be maintained in paper copies;

2. determining the conditions for personal data processing;

3. regulating the access to registers;

4. controlling the access to registers;

5. determining the time-limits for storage;

6. rules for reproduction and distribution;

7. procedures for destroying;

8. procedures for inspection and control of processing.

Article 9. (1) Protection of automated information systems and/or networks is a system of technical and organizational measures to provide protection against unlawful forms of personal data processing.

(2) The basic measures for protection of the automated information systems and/or networks are:

1. policy to protect personal data, protection guidelines and standard operating procedures;

2. defining roles and responsibilities;

3. identification and authentication;

4. registers management;

5. session controls;

6. external links/connections;

7. telecommunications and remote access;

8. monitoring;

9. virus protection;

10. accidents/contingency planning;

11. maintenance/operation;

12. configuration management;

13. copies/backups for recovery;

14. information media;

15. physical environment/surroundings;

16. personnel protection;

17. training the employees to respond to events that threaten the security of data;

18. determining time-limits for personal data storage;

19. procedures for destruction/removal/deletion of media.

Article 10. (1) Cryptographic protection is a system of technical and organizational measures applied to protect data from unauthorized access during transmission, dissemination or provision.

(2) The basic cryptographic protection measures are:

1. standard cryptographic capabilities of the operating systems;

2. standard cryptographic capabilities of the database management systems;

3. standard cryptographic capabilities of communications equipment;

4. systems for distribution and management of cryptographic keys;

5. systems for electronic signature.

Chapter Three
IMPACT ASSESSMENT AND LEVELS OF IMPACT

Article 11. (1) In order to define the adequate level of technical and organizational measures and the admissible type of protection the controller shall carry out an impact assessment on the personal data processed.

(2) The impact assessment is a process of determining the levels of impact on a particular individual or a group of individuals, depending on the nature of the personal data processed and the number of affected individuals in case of violations of the confidentiality, integrity or availability of personal data.

(3) The impact assessment shall be carried out periodically every two years or upon a change of the nature of the personal data processed and the number of individuals affected.

Article 12. When carrying out the impact assessment, the controller shall consider the nature of the personal data processed as follows:

1. systematization and evaluation of personal aspects of a particular individual (profiling) for analyzing or forecasting in particular their economic situation, location, personal preferences, reliability or behavior based on automated processing and which are considered the basis to take measures which create legal consequences for the individual or affect the individual to a significant extent;

2. data that reveal racial or ethnic origin, political, religious or philosophical beliefs, membership in political parties or organizations, associations with religious,

philosophical, political or trade union purposes, or data concerning health, sex life or human genome;

3. personal data by creating video records from video surveillance in publicly accessible areas;

4. personal data in large-scale registers of personal data;

5. data, the processing of which as determined by decision of the Commission for Personal Data Protection threatens the rights and legitimate interests of the individuals.

Article 13. The following levels of impact are determined:

1. "Extremely high" – where unlawful processing of personal data could give rise to significant harm or identity theft of a particularly large group of individuals, or permanent health damage or death of a group of individuals;

2. "High" – where unlawful processing of personal data could give rise to significant harm or identity theft of a large group of individuals or senior government officials, or permanent health damage or death of a single individual;

3. "Medium" – where unlawful processing of personal data could pose a risk of infringement of interests, revealing racial or ethnic origin, political, religious or philosophical beliefs, membership in political parties or organizations, associations with religious, philosophical, political or trade union purposes, health, sex life or human genome of a single individual or a group of individuals;

4. "Low" – where unlawful processing of personal data would threaten privacy and personal life of a single individual or a group of individuals.

Article 14. (1) The controller shall carry out an impact assessment of all maintained registers in accordance with Annex 1.

(2) Each one register shall be assessed on the basis of the criteria of confidentiality, integrity and availability.

(3) The highest level of impact, determined on the basis of each criterion referred to in para. 2 shall determine the level of impact of the respective register.

(4) For a group of jointly stored or processed registers, the level of impact shall be the highest one among all levels determined for each registers within the group in accordance with Annex 2.

Chapter Four
LEVELS OF PROTECTION

Article 15. (1) The appropriate level of protection shall be determined depending on the level of impact.

(2) The level of protection is a combination of technical and organizational measures for the physical, personnel, documentary protection and the protection of automated information systems and/or networks and cryptographic protection of personal data.

Article 16. (1) The levels of protection are classified as low, medium, high and extremely high.

(2) The levels of protection are as follows:

1. at low level of impact – low level of protection;

2. at medium level of impact – medium level of protection;

3. at high level of impact – high level of protection;

4. at extremely high level of impact – extremely high level of protection.

Article 17. The minimum level of technical and organizational measures which are to be provided by the controller (Annex 3) is as follows:

1. at low level of protection – the measures under Article 6, para. 2, item 2 - 4,

para. 3, item 1, 2, 5 and 9, Article 7, para. 2, item 1, 3 and 5, Article 8, para. 2, item 1 - 3, 5 and 7, Article 9, para. 2, item 3, 4, 6, 9, 13, 14, 16, 18 and 19;

2. at medium level of protection – the measures under item 1, as well as the measures under Article 6, para. 2, item 1 and 6, Article 7, para. 2, item 2, 4, 6 and 7, Article 8, para. 2, item 4 and 6, Article 9, para. 2, item 7, 11 and 15, Article 10, para. 2, item 1, 2 and 3;

3. at high level of protection – the measures under item 2, as well as the measures under Article 6, para. 2, item 5 and 7, para. 3, item 4, 6 - 8, 10 and 11, Article 8, para. 2, item 8, Article 9, para. 2, item 1, 2, 5, 8, 10, 12 and 17, Article 10, para. 2, item 4 and 5;

4. at extremely high level of protection the controller shall take the measures referred to under item 3, as well as the measures derived from international security policies or acts of international nature.

Chapter Five
OBLIGATIONS OF THE CONTROLLER

Article 18. (1) The personal data controller or a data protection officer designated by the controller shall implement the necessary technical and organizational measures for personal data protection.

(2) The controller may designate one or more data protection officers that shall be responsible for coordinating and implementing the measures referred to under para. 1.

Article 19. The controller shall have the following responsibilities:

1. to determine the personal data protection policy in the organization;

2. to adopt instruction as per Article 23, para.4 of the Personal data Protection Act;

3. to arrange the maintenance of the registers;

4. to undertake specific protection measures depending on the specific of the registers;

5. to exercise control on the observance of the requirements for protection of registers, to ascertain circumstances relating to violations of their protection and to take measures to eliminate them;

6. to update the registers with personal data maintained;

7. to perform periodic impact assessment under Article 11;

8. to assist in the implementation of the control functions of the Commission for Personal Data Protection.

Article 20. (1) The instruction referred to under Article 19, item 2 includes:

1. identification of the data controller;

2. general description of the registers maintained - categories of personal data and reasons for their processing;

3. technological description of maintained registers - data media, processing technology, period of storage life and services rendered;

4. determining the positions associated with processing and protection of personal data, their rights and obligations;

5. impact assessment and determination of the respective level of protection as per Chapter Three;

6. description of the technical and organizational measures taken;

7. actions for protection in case of accidents, incidents and disasters (fire, flood, etc.);

8. provision of personal data to third parties – reasons, purposes, categories of personal data;

9. time-limit for conducting periodic reviews of the need for data processing and deletion of data;

10. determining the procedure for the implementation of the obligations under Article 25 of the Personal data Protection Act;

(2) The information referred to under item 2 to 10 of the preceding paragraph shall be described for each of the registers maintained.

Additional Provision

§ 1. Within the meaning of this Ordinance:

1. “Data protection officer” shall be an individual with the necessary competency, who is authorized or designated by the controller by a respective written instrument regulating the rights and obligations of this individual relating to the provision of the necessary technical and organizational measures for protection of personal data during their processing.

2. “Personal data medium” shall mean a physical object capable of recording data or restoring data stored therein.

3. “Backups for recovery” shall mean copies of data stored on the medium that may be used for data restoration.

4. “Confidentiality” shall mean the requirement for non-disclosure of personal data to unauthorized persons in the course of their processing.

5. “Integrity” shall mean the requirement that data may not be changed/replaced in an unauthorized manner during their processing and the requirement to avoid alteration and unauthorized manipulation of the function concerning data processing.

6. “Availability” shall mean the requirement for provision of uninterrupted possibility for personal data processing by authorized persons and for the implementation of the functions of the processing system or their quick recovery.

7. “Particularly large group of individuals” shall mean a group of over 1,000,000 individuals;

8. “Large group of individuals” shall mean a group of over 10,000 individuals;

9. “Group of individuals” shall mean a group of over 2 individuals;

10. “Senior government officials” shall mean the persons referred to under Article 2, para. 1 of the Public Disclosure of the Property of Senior Government Officials Act.

11. “Large-scale registers of personal data” shall mean distributed personal data which are not possible to be managed using the standard tools for database management.

Transitional and Final Provisions

§ 2. The personal data controller shall provide the minimum level of technical and organizational measures for personal data processing and the admissible type of protection in accordance with this Ordinance:

1. within six months from the entry into force of this Ordinance, the controller shall be bound to determine the level of impact on the registers processed;

2. for registers with personal data kept at the moment of the entry into force of this Ordinance, the measures for protection at low level provided therein must be implemented within six months after the determination of the level of impact;

3. for registers with personal data kept at the moment of the entry into force of this Ordinance, the measures for protection at medium level provided therein must be implemented within nine months after the determination of the level of impact;

4. for registers with personal data kept at the moment of the entry into force of this Ordinance, the measures for protection at high and extremely high level provided therein must be implemented within one year after the determination of the level of impact.

§ 3. This Ordinance is issued pursuant to Article 23, para. 5 of the Personal Data Protection Act.

§ 4. This Ordinance repeals Ordinance 1 of 7 February 2007 on the minimum level of technical and organizational measures and admissible type of data protection (SG, issue 25 of 2007).

Annex 1 to Article 14, para. 1

Assessment of the level of impact of a register

	LEVEL OF IMPACT			
	Confidentiality	**Integrity**	**Availability**	**Total for the register**
Register name				

Annex 2 to Article 14, para. 4

Assessment of the level of impact of a group of "n" registers

	Confidentiality	**Integrity**	**Availability**	**Total for the register**
Register 1				
Register 2				
……				
Register n				
Level of impact for the group of "n" registers:				

Types of protection / Levels of Protection	Physical		Personnel	Documentary	Automated Information Systems and/or Networks		Cryptographic
	organizational measures	technical measures	organizational measures	organizational measures	organizational measures	technical measures	technical measures
Low	* determining the premises where personal data are to be processed; * determining the premises where the elements of the communication and information systems for personal data processing are to be located; * determining the organization of physical access;	*locks; * cabinets; * firefighting devices; * equipment of the premises;	* knowledge of legislation relating to the protection of personal data; * knowledge of threats to personal data processed by the controller; * consent to assume an obligation of non-disclosure of personal data;	* determining the registers which will be maintained in paper copies; * determining the conditions for personal data processing; * regulating the access to registers; * determining the time-limits for storage; * procedures for destroying;	* personnel protection; * determining time-limits for personal data storage; * procedures for destruction/removal/deletion of media;	* identification and authentication; * registers management ; * external links/connections; * virus protection; * copies/backups for recovery; * information media;	
Medium	*** low level +** * determining the use of technical means of physical protection; * identifying the areas with controlled access;	*** low level**	*** low level +** * training; * sharing critical information among employees; * knowledge of policies and guidelines for the protection of personal data; * training the employees to respond to events that threaten the security of personal data;\	*** low level +** * controlling the access to registers; * rules for reproduction and distribution;	*** low level +** * physical environment/surroundings;	*** low level +** * telecommunications and remote access; * maintenance/operation;	* standard cryptographic capabilities of the operating systems; * standard cryptographic capabilities of the database management systems; *standard cryptographic capabilities of communications equipment;
High	*** medium level +** * appointing a team to respond in case of violations; * determining the regime of visits;	*** medium level +** * fire detection and extinguishing systems; * equipment of the areas with controlled access; * security guards and/or security system; * devices for physical access control; * devices detecting substances ; * perimeter protection devices;	*** medium level**	* **medium level +** * procedures for inspection and control of processing;	*** medium level +** * policy to protect personal data, protection guidelines and standard operating procedures; * accidents/contingency planning; * training the employees to respond to events that threaten the security of data;	*** medium level +** * defining roles and responsibilities; * session controls; * monitoring; * configuration management;	*** medium level +** * systems for electronic signature; *systems for distribution and management of cryptographic keys;
Extremely high	*** high level +** * measures derived from international security policies or acts of international nature						