Unofficial translation

Approved by
Government Decision
No. 1123 of 14.12.2010

Requirements
for the assurance of personal data security at their processing within the information systems of personal data

I. GENERAL PROVISIONS

1. The Requirements for the assurance of personal data security at their processing within the information systems of personal data (Requirements) have the main purpose to lay down minimum rules for the development and implementation by the personal data holders/persons empowered by personal data holders with necessary technical and organizational measures for the security, confidentiality and the integrity of personal data, processed in the information systems of personal data and/or kept in a manual register, in accordance with Law no.17-XVI of 15 February 2007 on personal data protection (Official Gazette of the Republic of Moldova of 27.07.2007, no.107-111, art.468) and Law no. 71-XVI of 22.03.2007 on registers (Official Gazette of the Republic of Moldova of 25.05.2007, no.70-73 art.314).

2. These requirements create necessary framework for the application of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data entered in Strasbourg on 28 January 1981, published in the European Treaty Series, no.108, ratified by the Republic of Moldova through Parliament Decision no. 483 - XIV of 02.07.1999.

3. According to these Requirements, the following definitions can be defined:

Authentication: verifying the identifier assigned to the subject of access, confirmation of authentication;

Security control: - actions taken by the personal data holders or the National Center for Personal Data Protection (hereinafter- Center), in order to verify and/or ensure an adequate security level of the personal data processed within information systems and/or kept in a manual register, in accordance with these Requirements;

Temporary files: a set of data or digital information created for a period of time before the initiation of tasks they were assigned;

Identification: allocation of an identifier to subjects and objects of access and/or comparing presented identifier with a list of assigned identifiers;

Integrity: certainty, non contradictoriness and actuality of the information containing personal data, protecting it from damage and unauthorized modification;

Means of cryptographic protection of information containing personal data: technical means, software and technical applied ones, systems and complex systems making the conversion of cryptogrammic algorithms information containing personal data intended to ensure information integrity and confidentiality in its processing, storage and transmission through communication channels;

Protection level: security level proportional to risk that involves the processing to these personal data, as well as human rights and freedoms, established according to Requirements, set up and updated to the level of technological development and implementation costs of these measures (N-1 or N-2);

Security policy of personal data: document worked up by personal data holder which provides an accurate description of security strategies and protection features selected for data security, taking into account potential threats to processed personal data and real risks to which they are exposed;

Security perimeter: area that is in itself a cross barrier for access provided with physical and/or technical control means;

The person responsible for security policy of personal data: responsible person for the proper functioning of the complex system of protection of information containing personal data, as well as elaboration, implementation and monitoring compliance with security policy of personal data holder;

Information protection against unintended actions: set of measures aimed at preventing unintended actions, caused by user errors, technical means defects, natural phenomena or other causes that are not directly aimed at modification of information, but which lead to the distortion, destruction, copying, blocking of access to information, as well as the loss, destruction or damage of material support of information containing personal data;

Personal data carrier: magnetic, optic, laser, paper or other support of information, on which the document is created, attached, transmitted, received, maintained or otherwise used, that allows its reproduction;

Restoring data: procedures on restoring personal data in the state they were up to the moment of their loss or destruction;

Informational Technology (IT): all the methods, procedures and means of processing and transmitting of information containing personal data and its implementing rules;

User: a person that acts under the authority of personal data holder with an acknowledged access to information systems of personal data;

Working session: Period, lasting since the computer and application of informational resource is turned on and is in usage, or from the moment of start-up of information resource, until their turn off;

Information system of personal data: all interrelated information resources and technologies, methods and personnel, intended for storage, processing and provision of personal data information;

Storage: keeping on any type of support the personal data.

II. GENERAL REQUIREMENTS

4. The measures to protect personal data, is a part of work of creation, development and operation of information system of personal data that will be carried out continuously by all personal data holders.

5. Personal data protection in information systems of personal data will be ensured by a complex of technical and organizational measures for the prevention of unauthorized processing of personal data.

6. Measures of personal data protection processed in information system of personal data will be accomplished taking into account the need to ensure confidentiality of such measures.

7. Implementation of any measures and works with the use of information resources of personal data holder would be prohibited in cases when will not be adopted and implemented appropriate measures for personal data protection.

8. All information resources of personal data holders, containing personal data will be protected, including:

1) magnetic, optical, laser or other electronic information support, mass information and data bases;

2) information systems, networks, operating systems, databases management systems and other applications, telecommunication systems, including both means of producing and copying documents and other technical means of information processing.

9. Personal data protection in information systems of personal data will be ensured in order to:

1) prevent the flow of information containing personal data through exclusion method of unauthorized access to it;

2) prevent personal data unauthorized destruction, modification, copying, blocking in telecommunication network and information resources;

3) compliance with regulatory framework for using information system and software for personal data processing;

4) ensure personal data completeness, integrity and correctness in telecommunication systems and informational resources;

5) preserve management options of personal data processing and storage.

10. Personal data protection processed in information systems will be accomplished through such methods as:

1) preventing unauthorized connections to telecommunication networks and interception using technical means of personal data transmitted through this networks;

2) exclusion of unauthorized personal data processing;

3) prevent special technical and program actions which make possible personal data destruction, modification or other damages during technical and program work;

4) prevent indented and/or unintended actions of domestic and/or external users, as well as other employees of personal data holders that make possible personal data destruction, modification or other damages during technical and program work.

11. Prevention of leakage of information containing personal data, transmitted through liaison channels, will be provided using methods of ciphering this information, including organizational, technical and regime measures.

12. Prevention of unauthorized access to personal data information that circulates or is kept in technical means will be provided by the use of special technical and program means, their ciphering, including organizational measures and regime ones.

13. Preventing personal data destruction, modification or software failure in operation for personal data processing, will be ensured by using methods of special technical and program means, including use of licensed programs, antivirus programs, organizing control systems of software security and regular backup execution.

14. The order of access to personal data information processed in information systems will be determined by personal data holder, in accordance with the law.

III. SECURITY POLICY OF PERSONAL DATA

15. Each personal data holder, based on the specific activity, will elaborate and organize the implementation of document provisions which establish security policy of personal data, including the procedures and measures related to implementation of this policy by applying practical solutions with a level of proportional complexity and detailing, for users identification and authentication; the reaction to security incidents, IT and communication protection; to ensure personal data and IT information integrity; access management; audit and evidence insurance, taking into account:

1) category of processed personal data and processing operations performed onto them (as to the appendix no.1 and no.2 of these Requirements);

2) dimension of personal data holder, depending on the number of employees, number of administrative subdivisions, geographical location of subdivisions or subsidiaries, etc., including the number of people who can access personal data;

3) forms for keeping Registers in which personal data are processed (manual, electronic or mixed);

4) the complexion of personal data information systems and application programs involved in data processing;

5) risks to which are exposed personal data holder or people with processed personal data, the state of play of technological development in this field and the cost of implementing measures.

16. Security policy of personal data will be reviewed at least once a year, as a result of changes or reassessment of its components and approved at the highest level of hierarchy of the responsible persons of the personal data holder.

In order to ensure awareness to everyone the security policy of personal data, this document will be made aware to users and other employees of personal data holders, within functional skills and level of granted access.

17. Personal data holder will nominate a responsible person for elaboration, implementing and monitoring compliance with the provisions of security policy of personal data, directly subordinated to the head of institution that will not have other responsibilities incompatible with the functional tasks of policy implementation.

18. The person responsible for security policy of personal data will have sufficient resources (time, human resources, equipment and budget) and will have free access to necessary information to perform his functions at the extent he does not operate outside the framework of this policy.

19. The person responsible for security policy of personal data will ensure that different responsibilities regarding security policy of personal data will be clearly defined (prevention, surveillance, detection and processing), as well as operating with them, outside pressure as a result of personal interests or other circumstances.

20. Personal data holders shall take the following actions:

1) will clearly define the responsibilities and management process of personal data security, with their proper integration into the overall organizational and functional structure;

2) will allocate sufficient financial, technical and organizational resources necessary to organize management process of personal data security;

3) will elaborate procedures for classifying information containing personal data so that it would be possible to draw up a classification catalogue and all processed personal data would be located there, no matter of the type of data carrier;

4) will train people involved in personal data processing in order to meet the functional duties and responsibilities for security of personal data, including on their confidentiality.

21. Documentation on security policy of personal data will be centralized, comprehensive, regularly updated and will contain at least the following elements:

1) identity of the responsible person for security policy;

2) security measures;

3) mechanism for security measures implementation;

4) classification catalogue of processed personal data, their localization and performed operation onto them;

5) a nominal list of users, authorized for personal data access;

6) personal data information system and network configuration;

7) detailed description of criteria under which processed personal data are accessible in the manual register;

8) technical documentation on security controls;

9) schedule of planed security controls;

10) measures to detect cases of access and/or unauthorized personal data processing;

11) Reports of security incidents.

IV. PHYSICAL ENVIRONMENT AND INFORMATION TEHNOLOGY SECURITY USED IN PERSONAL DATA PROCESSING

Section 1

Authorization of physical access

22. For N-1 category:

Access to premises/offices/ bureaus or spaces where personal data information systems are placed will be restricted, being allowed only for people who have necessary authorization and only during office hours as listed and appropriate signs (signs, badges, identification cards, chip cards).

The head of personal data holders will elaborate and approve the access lists, which will be reviewed monthly, and signs that allow access.

23. Additionally, for N-2 category:

Access will be based on identification cards, chip cards or other similar technologies.

Section 2

Administration and monitoring of physical access

24. For N-1 category:

Administration and monitoring of physical access will be carried out in all access points of personal data information system, including the fact that there will be reaction to the access regime infringement;

Prior to granting physical access to personal data information system, there will be checked the access competences.

Monitoring registers will be kept for at least a year, after which they are liquidated, and the data and the documents contained in the register under liquidation will be transmitted to the archive.

25. Additionally, for N-2 category:

The areas where personal data systems information is placed will be equipped with access control systems and video supervision, for monitoring the access of persons in these areas.

During the monitoring process will be used supervision means and alarm in real time of all authorized and/or unauthorized access cases.

Automated means will be used to provide unauthorized identification access cases and initiate actions to block access.

Section 3

Security of premises/offices/bureaus and of means of personal data processing

26. For N-1 category:

Security perimeter will be determined concretely and clearly. The building or room perimeter in which are placed means for personal data processing will be physically upright.

Exterior room walls will be resistant, entrances equipped with locks, access control means, signal, etc.

If the room location is on the ground floor or/and the top floor of the building, and in case of balconies, fire stairs, the windows of those rooms will be equipped with grating bars.

Computers, servers, other access terminals will be located in places with limited access for strangers.

Doors and windows should be locked in the room when employees are missing.

Agendas and/or phone books which contain clues about the location of the means of personal data processing will not be accessible to strangers.

Location of means of personal data processing will meet their need for security against unauthorized access, theft, fire, flood and other possible risks.

The use of photo, video, audio techniques or other means of security perimeter recording will be allowed only in the presence of a special permission of the head of personal data holder.

Information carriers and resources of personal data processing removed from the premises of the security perimeter will not be left unauthorized in public places.

27. Additionally, for N-2 category:

Intrusion detecting systems will be implemented for exterior doors and windows located in accessible places.

Reserve equipment and carriers of information containing personal data will be stored in places to avoid destruction or damages as a result of main premise/office/bureau disasters.

Section 4

Visitors` control

28. For N-1 category:

Physical access of the visitors will be controlled in the rooms where information systems of personal data are located.

Visitors' access will be recorded in registers, which will be kept for a period not less than one year. After the expiry of one year, the registers are liquidated, and the data and the documents contained in the register under liquidation will be transmitted to the archive.

29. Additionally, for N-2 category:

Visitors of personal data information systems will be accompanied by persons empowered for such purposes, while exercising, in parallel, control over their actions.

Section 5

Power security

30. For N-1 category:

Security will be ensured of the electric equipment used to maintain information system of personal data functionality, electrical cables, including their protection against damages and unauthorized connections.

In case of exceptional situations, emergency or force majeure the possibility of electricity disconnection to personal data information system will be ensured, including the possibility of disconnection of any IT component.

Autonomous sources of short power supply will be provided, to be used for proper completion of work session of the system (component) in the event of the disconnection from the main power source.

31. Additionally, for N-2 category:

There will be provided and assured sources of long term electricity supply, which will be used for long periods of disconnection and for the need to continue carrying out the functional tasks set in front of personal data information systems.

Section 6

Cable network security

32. For all personal data information systems:

Network cables, which carry out operations of personal data processing, will be protected against unauthorized connections or deterioration.

Power cables will be separated from communication ones, in order to exclude electromagnetic interference.

Personal data holders will make monthly controls in order to verify cases of unauthorized connection to the network cables.

Section 7

Providing fire safety of personal data information systems

33. For N-1 category:

Means of ensuring fire safety of premises/offices/bureaus where personal data information systems and means of personal data processing are located will be provided.

34. Additionally, for N-2 category:

Automated systems will be implemented to detect/signalize and fire extinguishing on the premises/offices/bureaus where personal data information systems and means of personal data processing are located.

Section 8

Installation control and removal of IT components

35. For all components of personal data information systems:

Control and evidence will be realized on program and technical resources installation and removal, as well as other technical software used in personal data information system.

Information containing personal data and stored on the carriers will be physically destroyed or transcribed and destroyed by secure methods, avoiding the use of standard functions of annihilation.

Section 9

General measures of information security administration

36. For all personal data information systems:

Temporary unused information carriers on paper support or electronic (digital) one containing personal data will be kept in locked metallic safes or cases.

Computers, access terminals and printers will be disconnected at the end of work session.

Security for points of received/sent mail, and security against unauthorized access to fax and copy machines will be ensured.

Physical access to the resources of representation of information that contains personal data will be under administration, in order to prevent its viewing by unauthorized persons.

Means of personal data processing, information that contains personal data or software for personal data processing, will be removed from security perimeter only on grounds of written permission of head of personal data holder.

Removing and placing the means of personal data processing from/into security perimeter will be recorded.

V. IDENTIFICATION AND AUTHORIZATION OF PERSONAL DATA INFORMATION SYSTEM USER

Section 1

User identification and authentication

37. For N-1 category:

Will be identified and authenticated users of personal data information system and processes executed on behalf of these users.

All users (including staff that provides technical support, network administrators, programmers and database administrators) will have a personal identifier (user ID), which must not contain signs of users level of accessibility.

To confirm user ID passwords will be used, special memory physical means of access (token) or microprocessor cards, biometric means of authentication, focused on unique and individual characteristics of the person.

If the employment contract/ user`s work relationships finished, suspended or modified and new tasks do not require personal data access, or user right of access was modified, or the user abused on received codes in order to commit a harmful act, was absent for a

long time, identification and authentication codes will be revoked or suspended by personal data holder.

38. Additionally, for N-2 category:

Multifactor (complex) authentication will be used, which will include passwords and special memory physical means of access or microprocessor cards, biometric means and passwords of authentication.

Section 2

Equipment identification and authentication

39. For all personal data information systems:

Will be provided the opportunity to identify and authenticate used equipment in the personal data processing.

Section 3

Administration of user identifiers

40. For all personal data information systems:

Administration of user identifiers will include:

1) univocal identification of each user;

2) user authentication;

3) authorization acquirement from the responsible person issuing user ID;

4) ensuring that the user ID is issued to specifically determined person;

5) disabling user account after inactive period whiciis set in time (maximum inaction - two months);

6) making archive copies of ID of the users.

Section 4

Administration of authentication means

41. For all personal data information systems:

Personal data holders will determine administrative procedures that will govern the process of distribution and lifting the means of authentication for users, including actions in cases of lost/compromising or their defection.

The standard user authentication information will be changed after system installation.

Section 5

Providing bilateral connection in case of information insertion for user authentication

42. For all personal data information systems:

Will be provided bilateral connection of personal data holder to the user when performing the authentication procedures, that will not compromise authentication mechanism.

Section 6

Using passwords during the process of ensuring information security

43. For all personal data information systems:

Will be observed the rules to ensure information security for choosing and using the passwords, which will include:

1) keeping the password confidentiality;

2) prohibiting inscribing password on paper support, if it is not ensured its security preserving;

3) changing passwords every time when there are possible compromises of the system or password;

4) choice of quality passwords with a minimum size of eight symbols, which are not related to the user's personal data information, will not contain consecutive identical symbols and will not be entirely composed of groups of numbers or letters;

5) changing passwords in more than three months intervals;

6) disabling automated registration process (using saved passwords).

Section 7

Managing user passwords

44. For all personal data information systems:

Individual identifiers and individual passwords will be used for each user in order to ensure the possibility of establishing accountability.

Will be provided the possibility for users to choose and change individual passwords, including the activation of procedure for filing their wrong introductions.

Blocking access will be provided after three incorrect login attempts.

Keeping previous history of passwords of the users will be assured in hash form (for the period of one year) and preventing their repeated use.

When logging in, the passwords will not be clearly reflected on the monitor.

Password will be stored in ciphered form, using the unilateral cryptographic algorithm (hash function).

VI. USER ACCESS MANAGEMENT

Section1

Access management

45. For all personal data information systems:

Recording and evidence mechanisms of persons that have access or participate in operations of personal data processing will be implemented, and if it is necessary will allow to identify cases of unauthorized access or illegal personal data processing.

Section 2

Administration of access accounts

46. For all personal data information systems:

The administration of access accounts will be made of users, who process personal data, including their creation, activation, modification, revision, deactivation and deletion. Automated means of support will be used in order to administrate access accounts.

The action of access accounts of temporary users, who processes personal data, will automatically terminate on expiry of a fixed time period (for each type of access account in part).

Access accounts of inactive users that process personal data will be automatically disabled, after a maximum of three months.

Automated means will be used for registration and information about creating, modifying, disabling and stopping of access account`s action.

Section 3

Granting access

47. For all personal data information systems:

Will be authorized the access to personal data information system in accordance with established administration policy by personal data holder.

Access to security functions of personal data information system and their data will be granted only to responsible persons expressly indicated in security policy of personal data holder.

Section 4

Review of user access rights

48. For all personal data information systems:

User access rights to personal data information systems will be regularly revised in order to ensure that no unauthorized access rights were granted (over every six months) and after any change of user`s status.

Section 5

Managing information flows

49. For all personal data information systems:

There will be authorized by personal data holders the realization of the information flows during the transmission of these within and beyond personal data information systems.

Section 6

Obligations distribution and investment with the minimum rights and competences

50. For all personal data information systems:

Obligations distribution to subjects, who provide functioning of personal data information systems, will be made through investing with rights/appropriate competences of access through an administrative act of the head of personal data holder.

Personal data information systems users will be invested only with those rights/competences that are necessary to achieve the settled targets.

Section 7

Warning information

51. For all personal data information systems:

Before granting access to the system, users will be informed that the use of personal data information system is checked and their unauthorized use is prosecuted in accordance with legislation.

Section 8

Blocking of the working session

52. For all personal data information systems:

The working session in information system for personal data processing will be blocked (at user`s request or automatically after a maximum of 15 minutes of user`s idle time) which will make impossible further access until the moment when the user will unlock the session by repeated method of identification and authentication procedures.

Section 9

Control of access administration

53. For all personal data information systems:

The control of user`s actions will be performed to assess accuracy and compliance of the operations and undertaken activities using personal data information system.

Section 10

Marking documents

54. For all personal data information systems:

The information that went out of the system, containing personal data, will be marked with indication of prescriptions for its further processing and wide spreading, including the indication of the unique identification personal data holder number.

Section 11

Distance access

55. For all personal data information systems:

All methods of access from the distance to personal data information system will be secured (using VPN, encryption, ciphering, etc.), and shall be documented, monitored and controlled.

Each method of access from the distance to personal data information system will be authorized by responsible persons of personal data holders and allowed only to users, to whom it is necessary for the set objectives.

Section 12

Limitation of wireless technologies usage

56. For all personal data information systems:

Limitations and rules for the use of wireless technologies that provide the access to personal data information system will be established.

Wireless access to personal data information system will be documented, monitored and controlled.

Wireless access to personal data information systems will be allowed only when cryptographic means of information protection are used.

The use of wireless technologies will be authorized by the relevant responsible persons of personal data holder.

Section 13

Managing access of mobile and portable equipment

57. For all personal data information systems:

Limitations and rules for the use of portable and mobile equipment which enable access to personal data information systems will be established.

Access to information systems of personal data using portable and mobile equipment will be documented, monitored and controlled.

Use of portable and mobile equipment will be authorized by relevant responsible persons of personal data holder.

VII. Protection of information systems and communications where personal data are processed

Section 1

Division of application programs

58. For all personal data information systems:

Separation of user functional opportunities from the functional possibilities of personal data information system management will be ensured.

Section 2

Isolation of security functions

59. For all personal data information systems:

Isolation of security functions from those that are not assigned to the security of personal data information system will be ensured.

Section 3

Residual information

60. For all personal data information systems:

Disclosure of unauthorized or unintended attempts of residual information containing personal data will be prevented through generally accessible information resources.

Section 4

Protection against denial of service

61. For all personal data information systems:

Protection of personal data information systems will be ensured or limited the possibilities for different types of attacks “denial of service”, including DOS.

Section 5

Resources priorities

62. For all personal data information systems:

Possibility for limitation will be ensured by means of mechanisms of setting the priorities, of using information resources in which personal data are processed.

Section 6

Protection of the perimeter of information system in which personal data are processed

63. For all personal data information systems:

Permanent monitoring and communication control at the outer perimeter of personal data information system will be made, including at the most important contact points within the perimeter of these information systems.

Location of generally accessible resources will be ensured in spaces specifically designed for computing network with network physic interfaces.

Impossibility of outside access for users to internal network of personal data processing will be ensured.

Section 7

Ensuring the integrity of transmitted personal data

64. For all personal data information systems:

Integrity of transmitted personal data using cryptographic means of protection and digital signature will be ensured.

Section 8

Ensuring the confidentiality of transmitted personal data

65. For all personal data information systems:

Confidentiality of transmitted personal data, using the means of cryptographic protection of the information, will be ensured.

VIII. SECURITY AUDIT IN PERSONAL DATA INFORMATION SYSTEMS

Section 1

Generating audit registering in personal data information systems

66. For all personal data information systems:

Personal data holders will generate audit registering for personal data information systems security for the events specified in a corresponding list, subject to audit.

Section 2

List of events registered in the security audit system of personal data information system

67. For all personal data information systems:

1) The registration of user`s attempts of entry/exit in the system will be realized according to the following parameters:

a) date and time of attempted entry/exist;

b) user ID;

c) result of attempted entry/exit - positive or negative.

2) Attempts of start/end work session of the applicative programs and processes, designed for personal data processing, will be registered, as well as changes to users' rights of access and status of accessed objects under the following parameters:

a) date and time of the start attempted;

b) name/identifier of application program or process;

c) user ID;

d) result of starting attempting - positive or negative.

3) Will be registered attempts of obtaining access (execution of transactions) for applications and processes designed for personal data processing in accordance to the following parameters:

a) date and time attempting to obtain access (operation implementation);

b) name (identifier) of the application or process;

c) user ID;

d) specifications of protected resource (identifier, logical name, file name, number, etc.)

e) type of requested operation (reading, registration, deletion, etc.);

f) result of attempting to obtain access (operation implementation) - positive or negative.

4) Registration will be made of modifications for user right of access (competences) and status of accessed objects in accordance to the following parameters:

a) date and time of competences modifications;

b) Administrator ID which carried out modifications;

c) User ID and competences or the specification of accessed objects and their new status.

5) Will be made registration of exit from the information system containing personal data (electronic documents, data, etc.), registration of modifications of subject`s access rights and the status of accessed objects in accordance to the following parameters:

a) date and time of issue;

b) information name and ways of access to it;

c) equipment specification (device) that issued the information (logical name);

d) ID of the userwho requested information;

e) volume of the issued document (number of pages, fillets, copies) and the outcome of the issue - positive or negative.

Section 3

Processing the results of security audit in personal data information systems

68. For all personal data information systems:

In case of disturbance of security audit in personal data information system or completing the entire memory volume allocated for the maintaining of audit results, the responsible person for security policy of personal data will be informed and measures will be taken in order to restore working capacity of the audit system.

Section 4

Monitoring, analysis and generating reports on security audit of personal data information systems

69. For all personal data information systems:

Permanent monitoring and analysis of security audit registrations in personal data information systems will be made in order to detect unusual or suspicious activities for use of these information systems, with appropriate reports in cases of detecting such activities, stored in electronic means of calculation and undertaking pre-established actions in security policy in such cases.

Section 5

Protecting the data of security audit in personal data information systems

70. For all personal data information systems:

Security audit results in personal data information systems, which are operations of processing personal data and means of conducting the audit, will be protected against unauthorized access by setting appropriate security measures, including ensuring their confidentiality and integrity.

Section 6

Storage of data of security audit in personal data information systems

71. For all personal data information systems:

The duration of security audit in personal data information systems results storage will be justified in security policy of personal data but, in any case it shall not be less than two years, for their use as evidence for security incidents, or of any investigations or judicial processes.

If the investigations or judicial processes are extended, the audit results will be kept throughout their duration.

IX. ENSURING INTEGRITY FOR PERSONAL DATA INFORMATION AND INFORMATION TECHNOLOGIES

Section 1

Elimination of the software deficiencies designed for personal data processing

72. For all personal data information systems:

Identification, noting and removal of deficiencies of the software, designed for personal data processing, will be provided, including the software installation for their corrections and package of its updating.

Section 2

Ensuring protection against malware programs (viruses)

73. For N-1 category:

The protection against malware programs infiltration in software designed for personal data processing will be ensured, a measure that would ensure the possibility of automatic and timely renewal of means providing protection against malicious programs and viruses' signatures.

74. Additionally, for N-2 category:

Will be ensured centralized management mechanisms against malicious programs in software designed for personal data processing.

Section 3

Technologies and means of finding the intrusions

75. For all personal data information systems:

Will be used technologies and means of finding the intrusion that will allow event monitoring in personal data information system and finding attack, including ensuring identification of attempts of unauthorized information systems usage.

Section 4

Ensuring software and information integrity

76. For all personal data information systems:

The protection and possibility of detection of unauthorized modification of software, designed for personal data processing, and information that contains personal data will be ensured.

Software designed for personal data processing and information containing personal data, access to which is made through public access system, will be secured through using digital signature method.

Section 5

Testing the functional possibilities of ensuring security of personal data information systems

77. For all personal data information systems:

The proper testing operation of security functions of personal data information systems will be ensured (automatically at system startup and monthly at authorized user request for this purpose).

X. BACKUP COPIES AND RESTORE OF PERSONAL DATA INFORMATION AND INFORMATION TECHNOLOGY

Section 1

Backup copies of personal data information

78. For N-1 category:

Given the volume of processing undertaken individually, the time which will run the information backup containing personal data information and used software for automated personal data processing will be determined by personal data holder, but, in

any case, it shall not be less than one year, which are to be stored in protected locations, outside of the location of that information and basic software.

Backup copies will be tested in order to verify the safety of information carriers and information integrity containing personal data.

Procedures for restoring backup copies need to be updated and tested regularly in order to ensure their effectiveness.

79. Additionally, for N-2 category:

Backup copies will be stored in metallic boxes with applied seal and stored outside of basic software information location containing personal data, or if it is possible in rooms in another building.

Will be identified potential access problems in places of backup copies storage in case of defect or damage and determine concrete actions for restoration of access ways.

Section 2

Reserve telecommunication services

80. For N-2 category:

Will be identified basic and reserve telecommunication services, including solved questions about the use of reserve telecommunication services in order to restore basic service of access of personal data information systems.

In order to avoid being subjected to common dangers, basic and reserve telecommunication services providers will be different.

XI. SECURITY CONTROLS OF PERSONAL DATA INFORMATION SYSTEMS

81. Personal data holders will regularly perform, at least once a year, security controls of technical measures and/or organizational taken, so that if it is possible to detect malfunctions regarding the use of telecommunication systems and/or make improvements where necessary in personal data processing.

82. Security controls will be updated every time when personal data holder/person empowered by the personal data holder will be reorganized or will change their infrastructure.

83. In order to check the level of personal data information systems protection, as well as in order to avert possible cases of illicit or accidental access to such information systems, detection of weak points in their protection mechanisms, the Center will undertake regularly planned security controls, including conducting special technical measures in order to simulate a model of personal data information system access.

84. The results of the control performed by the Center will be immediately made available to the personal data holder, the level of personal data information systems protection of which served the purpose of control, prescribing, where necessary, appropriate actions to be taken in order to ensure the security of personal data processing.

XII. SECURITY INCIDENTS MANAGEMENT OF PERSONAL DATA INFORMATION SYSTEMS

Section 1

Instruction for reaction to security incidents of personal data information systems

85. For all personal data information systems:

Staff that provides exploiting personal data information systems will follow at least once a year instructions regarding the responsibilities and obligations in case of undertaking actions of management and reaction to security incidents.

Section 2

Processing security incidents of personal data information systems

86. For N-1 category:

A prompt information mechanism will be ensured to the head of personal data holder about incidents that infringes the security of personal data information systems.

Processing the incidents will include detection, analysis, and prevention of development, their removal and security restoration.

87. Additionally, for N-2 category:

Will be used automated means in order to support the processing of security incidents of personal data information systems.

Section 3

Monitoring the security incidents of personal data information systems

88. For N-1 category:

Security incidents of personal data information systems will be traced and documented permanently.

89. Additionally, for N-2 category:

Will be used automated means for tracing security incidents of personal data information systems, collection and analysis of information on these incidents.

Section 4

Reporting on security incidents of personal data information systems

90. For all personal data information systems:

Annually, by January 31, reports on security incidents of personal data information systems will be presented to the Center by the personal data holders. Based on this report, the Center undertakes the necessary measures that are compelled by the Law on personal data protection.

XIII. TECHNICAL PROTECTION OF PERSONAL DATA INFORMATION

91. For N-1 category:

Will be excluded uncontrolled presence of persons or transport means, as well as random installation of antennas, in an area of at least 15 meters from the location of the main technical means of personal data information systems (hereinafter - perimeter under control), for security purpose of personal data processing.

Server rooms will be protected against information leakage containing personal data due to electromagnetic emissions through the screening rooms or installation of electromagnetic interference systems, which will be designed, realized and researched by specialized enterprises.

If the rooms where technical means of personal data processing are placed are screened, continuity of electrical connection of all relevant screening material will be ensured: walls, ceiling, floor, windows and doors.

Screening constructions will have ground sockets that will be located in the perimeter under control.

Will be provided the protection of personal data information against leakage through the electrical grid, including crossing of the object`s electrical grids with protection filter installation which would block (to jam) the signal.

Will be excluded or limited the unauthorized installation of other electrical devices, radio or other type, in rooms where technical means of personal data processing are placed, in order to ensure personal data security.

The equipment which has output lines outside the perimeter under control will be installed at a distance of at least three meters away from IT means where personal data are processed.

XIV. SPECIFIC FEATURES OF SECURITY REQUIREMENTS IN CASE OF MANUAL FORMS OF REGISTER KEEPING WHERE PERSONAL DATA ARE PROCESSED

92. The provisions of these Requirements, except pct. 11 - 13, 23, 25, 27, 30-32, 35, 37-44, 46, 49, 51-53, 55-68, 72-77, 80, 87-89, 91, will be properly applied by personal data holders/persons empowered by the personal data holders for manual form of keeping the register where structured set of personal data are processed, accessible according to centralized or decentralized criteria, or dispersed on functional or geographic criteria.

93. At the same time, registrations of security audit of manual registers where personal data are processed will include:

1) user name and surname;

2) accessed document name (page and inscription from the register);

3) number of records made;

4) type of access;

5) date of access (year, month, day);

6) time (hour, minute) and access duration.

Appendix No.1
to Requirements for the assurance of personal data security at their processing within the information systems of personal data

CATEGORIES OF PERSONAL DATA

1. Personal data which directly or indirectly identify a natural person, in particular, by reference to an identification number (personal code), to one or more specific elements of his physical, physiological, psychological, economic, cultural or social identity fall into two categories: common and special.

2. Special category of personal data is the information revealing racial or ethnic origin, political or religious believes, personal data concerning health or sexual life, as well as data relating to criminal conviction of a physic person.

3. Common category is the information that reveals:

1) name and surname;
2) gender;
3) date and place of birth;
4) citizenship;
5) IDNP;
6) image;
7) voice;
8) family situation;
9) military situation;
10) geographic location data/ traffic data;
11) nickname/alias;
12) family members' personal data;
13) driving license data;
14) data from matriculation certificate;
15) economic and financial situation;
16) data of owned assets;
17) banking data;
18) signature;
19) civil status data;

20) pension file number;

21) social security number (CPAS);

22) medical insurance code (CPAM);

23) phone/fax number;

24) cell phone number;

25) address (domicile/residence);

26) e-mail address;

27) genetic data;

28) biometric and anthropometric data;

29) finger print identification data;

30) profession and/or work place;

31) professional occupation - diploma - education;

32) habits/preferences/behaviors;

33) physical characteristics.

4. In cases of common personal data processing, personal data holders will include in personal data security policy and will implement the requirements set up for the 1st security level of personal data information systems - (N-1).

5. In cases of special category of personal data processing, personal data holders, additionally to the set requirements for the 1st security level, will include in security policy of personal data and will implement requirements established for the 2nd security level of personal data information systems - (N-2).

Appendix No 2
to Requirements for the assurance of personal data security at their processing within the information systems of personal data

CATEGORIES OF OPERATIONS OF PERSONAL DATA PROCESSING SUSCEPTIBLE TO SPECIAL RISKS FOR INDIVIDUALS` RIGHTS AND FREEDOMS

1. The following categories of personal data processing present special risks for individuals` rights and freedoms:

1) adaptation, modification, disclosure by transmission, diffusion or otherwise of personal data related to racial or ethnic origin, political or religious believes, membership of a political party or religious organization, personal data concerning health or sexual life, as well as data relating to criminal conviction, measures of coercion, disciplinary or contravention sanctions;

2) operations of genetic, biometric data and geographic location data processing through electronic communications network;

3) operations of personal data processing by electronic means having as aim to assess some personality aspects as it is professional competence, credibility, behavior, etc.;

4) operations of personal data processing by electronic means in some evidence systems having the purpose of solvency, economic and financial situation analysis, the facts likely to attract disciplinary, contravention or criminal responsibility of individuals;

5) operations of personal data processing of minors for commercial purposes (direct marketing activities);

6) operations of personal data processing mentioned in the sub points 1) and 2), as well as personal data of minors, collected via internet or electronic messaging.

2. In cases of personal data processing by any operation or set of operations specified in pct.1 of this Appendix, personal data holders will include in personal data security policy and will implement requirements established for the 2nd security level of personal data information systems - (N-2).