Pursuant to the Article 11 of the Law on Personal Data Protection ("Official Gazette of BiH", No. 49/06) and the Article 17 of the Law on the Council of Ministers of Bosnia and Herzegovina ("Official Gazette of BiH", No. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 and 24/08) the Council of Ministers of Bosnia and Herzegovina, at its 93rd session held on 2 July 2009, passed the

RULEBOOK
ON THE MANNER OF KEEPING AND SPECIAL MEASURES OF PERSONAL DATA TECHNICAL PROTECTION

CHAPTER I - GENERAL PROVISIONS

Article 1

(Subject of the Rules)

The Rules on the manner of keeping and special measures for personal data technical protection (hereinafter: the Rules) sets forth the manner and special measures of technical protection of personal data.

Article 2

(Terms)

The terms used in this Rules bear the following meanings:

a) “Personal data filing systems administrator” is a natural person empowered and responsible for managing the personal data filing system and ensuring privacy and protection of the personal data processing.

b) “Executer” is a natural person, employed or engaged with the controller, who executes the activities in connection with the personal data processing.

CHAPTER II - MANNER OF PERSONAL DATA KEEPING

Article 3

(Manner of keeping)

The manner of personal data keeping involves undertaking of organizational and technical measures of personal data protection and drafting the personal data safety plan.

Article 4

(Organizational protection measures)

(1) The controller shall ensure organizational measures of personal data protection which include: informing and training of personnel working on the personal data processing, physical measures of protection of working premises and equipment related to personal data processing, prevention of unauthorized duplication, copying or transcribing of personal data, destroying of personal data etc.

(2) After being employed, and prior to starting to perform his/her duties, any person who will perform personal data processing in the scope of his/her duties is briefed on the measures of personal data protection.

(3) Prior to commencement of immediate performing activities related to personal data processing, the controller additionally briefs the employee with his/her specific obligations regarding personal data protection.

Article 5

(Measures of technical protection)

(1) The controller shall ensure adequate technical protection of the premises and equipment where processing of personal data shall be performed.

(2) Special measures of technical protection of personal data shall prevent unauthorized access to and processing of personal data.

(3) The technical measures of personal data protection include, among other, the control of access to premises and equipment for personal data processing, protection from destroying and damaging of personal data etc.

Article 6
(Personal data security plan)

(1) The personal data security plan contains technical and organizational measures that shall ensure that:

a) Only authorized persons can know personal data - confidentiality;

b) Personal data remain unchanged, full and accurate during the processing - integrity;

c) Data are constantly available and at disposal and can be properly processed - availability;

d) The origin of personal data can be determined at any time - authenticity;

e) It can be verified who processed personal data, when, which personal data and in which manner – possibility of revision;

f) The procedure of personal data processing is complete, up-dated and correspondingly recorded - transparency.

(2) Personal data security plan must include the categories of processed data and a list of instruments for protection, i.e. organizational and technical protection measures.

(3) Personal data security plan must be prepared in writing, up-dated and

continuously available to the Personal Data Protection Agency in Bosnia and Herzegovina.

CHAPTER III - PERSONAL DATA PROTECTION IN AUTOMATIC PROCESSING

Article 7
(Technical measures)

(1) Personal data automatic processing controller should ensure technical measures of personal data protection such as:

a) Unique user name and password containing combinations of a minimum of six characters, numbers or letters;

b) Automatic password change per agreed time period which may not be longer than six months;

c) The user name and the password shall allow access only to the parts of the system necessary for the executer to carry out his/her work duties;

d) Automatic log-off from the system after agreed period of inactivity, not longer than 15 minutes, and re-activation of the system requires new log-in of the user name and password;

e) Automatic ban to access the system after three failed system log-ins with automatic warning to the executer to ask the personal data filing systems administrator for instructions;

f) Efficient and reliable antivirus protection of the system that shall be continuously updated for prevention of unintended or unknown risks of new viruses;

g) Computer, software and other necessary equipment connected to electric power network by means of continuous power supply device.

(2) In case from item (1) of this Article the personal data filing systems administrator grants further access to the system.

(3) The human resources officer shall report to the personal data filing systems administrator on the employment or engagement of each executive authorized to access the information system in order to be assigned user name and password, as well as on termination of employment or engagement in order to erase user name and password and forbid further access.

(4) The reporting referred to in paragraph (3) of this Article is also done in case of any other change of working status of the executer that affects the level or extent of access to personal data filing systems.

Article 8
(Organizational measures)

Controller of the personal data automatic processing should ensure organizational measures to protect personal data such as:

a) Complete confidentiality and security of passwords and other forms of identification to access personal data;

b) Organizational rules for Internet access of the executer relating to downloading and recording the documents by means of electronic mail or other sources;

c) Destroying documents that contain personal data after the deadline for processing;

d) Any taking of any media containing personal data outside the working premises must be done with special permission and control in order to avoid loss or illegal use;

e) Physical measures for protection of working premises and equipment for personal data processing; and

f) Keeping to technical instructions at installation and use of equipment for personal data processing.

Article 9
(Firewall)

The controller is obliged to ensure adequate protection – a firewall between his system and Internet network, or any other form of external network, as protection against unauthorized logging to the system.

Article 10
(The right of access)

(1) Access to data stored in the personal data filing systems is allowed to authorized persons employed with the controller or data-processor and to authorized persons tasked to maintain and develop systems for managing personal data filing systems.

(2) Personal data filing systems controller nominates the persons referred to in paragraph (1) of this Article.

(3) Data-processor does not have powers to nominate the persons referred to in paragraph (1) of this Article.

(4) The request for access or processing and the request for termination of the authorization to access the personal data filing systems or personal data processing are submitted by the personal data filing system controller who issues or revokes the authorization for access to the filing systems.

Article 11
(Backup)

(1) The controller is obliged to carry out backups or archiving the data stored in the system on a regular basis in order to avoid their loss or destruction.

(2) The controller is obliged to inspect the usability of the filing systems backups through the verification procedure of restoring the filing systems stored on devices with removable storage to make sure that the restored data are fully available for use upon inspection, without any information loss.

(3) Each copy of data stored on devices with removable storage must be marked by number, type, date of storage and the name of the person who did the storage.

(4) It is prohibited to multiply the devices with removable storage containing data from the special categories of the personal data filing systems without supervision and approval of the filing system controller.

Article 12
(Access to telecommunication, computer and application system)

(1) Access to the information system for maintenance of the personal data filing systems or processing the filing systems data is allowed with the use of appropriate user names and accompanying passes.

(2) The controller shall record and inspect any right of the employees to access external networks as well as the right of access to computer systems or local networks to users outside the computer system.

(3) The modem plug-ins and their numbers used to access the system, which keep stored the personal data filing systems are not to be listed in telephone directories and may not be available through the telephone customer service.

Article 13
(Mandatory use of unique user names and pass to access the system)

(1) Access to data stored in the personal data filing systems is allowed by use of allocated unique user names and passes.

(2) The revoked user name must not be allocated to another person.

(3) The user name and accompanying pass must not be disclosed or given to another person.

(4) The manner of allocation and the obligation of change of passes is designated by the personal data filing system controller.

Article 14
(Records, monitoring of access and attempt of unauthorized access to the system)

(1) Any access to the information system for maintenance of the personal data filing systems must be automatically recorded by user name, date and time of registration and check-out.

(2) Each case of unauthorized access to the system must be automatically

recorded by user name, date and time, and if it is possible by place from which the access was tried.

(3) The data-processor, personal data filing system administrator and executer shall inform the responsible person with the personal data filing system controller on all attempts of unauthorized access to the system.

Article 15
(Person responsible for personal data protection)

The personal data filing system administrator is responsible for due implementation of measures of personal data insurance, storage and protection.

Article 16
(Person authorized for allocation of user names and passes)

The personal data filing system controller designates the person authorized for allocation and removal of user names and issuance of passes to persons authorized to work with the system, who are allowed to access the personal data filing systems.

Article 17
(Protection for special categories of personal data)

(1) The controller shall indicate that the processing concerns the special categories of data during all stages of the processing of special categories of personal data.

(2) The Controller shall undertake additional technical and organizational measures during the processing of special categories of personal data.

(3) Additional technical and organizational measures in the processing of special categories of personal data provide:

a) The possibility to recognize each individual authorized access to the information system;

b) The work with the data during normal working hours of the controller; and

c) Crypto-protection of the data during transfer of data over telecommunications systems with appropriate software and technical measures.

Article 18
(Weekly, monthly and annual checking of the system)

The personal data filing systems controller conducts checking of operation of all parts for the system on weekly, monthly and annual basis.

IV. TRANSITIONAL AND FINAL PROVISIONS

Article 19
(Supervision)

Supervision of the implementation of these Rules is conducted by the Personal Data Protection Agency in Bosnia and Herzegovina.

Article 20
(Harmonization with the provisions of the Rulebook)

(1) Within six months from coming into force of this Rulebook the personal data filing systems controllers and data-processors shall harmonize measures, means

and conditions of insurance, storage and protection of personal data with provisions hereof.

Article 21
(Entry into force)

(1) By entry into force of this Rulebook the Rules on Data Security ("Official Gazette of BiH" No. 39/02) ceases to be valid.

(2) This Rulebook shall enter into force eight days after publication in the "Official Gazette of BiH".

VM No. 176/09
2 July 2009
Sarajevo

Chairman of the
Council of Ministers
PhD Nikola Spiric, S. R.