



BHAS

AGENCY FOR STATISTICS OF BOSNIA AND HERZEGOVINA

**RULEBOOK
ON PROTECTION OF STATISTICAL DATA
IN THE AGENCY FOR STATISTICS OF BOSNIA AND HERZEGOVINA**

Sarajevo, 2016

Pursuant to the articles 27, 28, and 29 of the Law on Statistics of BiH (“Official Gazette of BiH” No 26/04 and 42/04), and articles 2, 3, and 20 of the Law on the Protection of Personal Data (“Official Gazette of BiH”, No 49/06; 76/11 and 89/11) I hereby issue

RULEBOOK
ON PROTECTION OF STATISTICAL DATA
IN THE AGENCY FOR STATISTICS OF BOSNIA AND HERZEGOVINA

I. GENERAL PROVISIONS

Article 1

This Rulebook shall proscribe procedures and measures for implementation of protection of statistical data, information, IT equipment, software support, as well as the premises where the equipment and installations in the Agency for Statistics of Bosnia and Herzegovina (hereinafter Agency) are placed, as well as the method for production of backup copies and archiving data and products of official statistics.

Article 2

Particular terms and expressions used in this Rulebook have the following mean:

1. “*statistical unit*” is the basic unit of observation for which the data are ultimately collected or derived by different method. Statistical unit is subject of statistical surveys and holder of statistical characteristic, where statistical unit may be: a person, household, enterprise, group of enterprises, etc;
2. “*aggregated statistical data*” are data produced by grouping information into the categories and aggregation of the values within categories;
3. “*confidential data*” are data that enable indirect or direct identification of statistical units where particular information could be revealed. In order to determine if the identification of statistical units is possible all relevant means that third party would reasonably use for identification of statistical unit shall be taken in account.
4. “*micro data for survey purposes*” are statistical data that enables only direct identification of statistical unit that data refer to;
 5. “*statistical protection of confidential data*” is the process of removing or modification of information, or compression within the data set, in order to ensure that no statistical units cannot be identified, directly or indirectly, within the data;
 - 6 “*indirect identification*” represents the identification of statistical unit based on its name or address, or based on publically available ID number;
- 7 „Direct identification“ represents the identification of statistical unit based on any other way except indirect identification;

- 8 „*identifier*“ is the part of individual number (e.g. name, address, PIN, number of ID card) that directly determines identity of statistical unit, i.e. identifies the link between data and statistical unit, where the data describes the precise and specific unit;
- 9 „*passive confidentiality*“ means that no appropriate measures are taken for data protection, except in the case where the explicit request from statistical unit exists due to consideration that their interests could be threatened and published data damaged;
- 10 „*users*“ are all persons (including individuals and legal persons, institutions and government bodies, namely all other business subjects) that use statistical data;
 - 11 „*protected room*“ is the room in the Agency where the carriers of the protected data are or the room where the hardware for access to the data is placed, that is, the workspace of the Agency where is allowed the access and use of micro data to registered science and research institutions and registered researchers, and authorized persons from government bodies and international organization,
- 12 „*Protected room with limited access*“ is the place in the Agency where the access is allowed under special conditions that are proscribed by this Rulebook;
- 13 „*data carrier*“ is each media containing data written in classical or computerized way.
- 14 „*material for archiving*“ considers all statistical data, corresponding programmes, meta data, and other statistical products produced by official statistics.

II. PROTECTION OF STATISTICAL DATA

Article 3

Protection of statistical data includes technics, rules, and procedures in order to prevent unauthorized access to protected data.

Article 4

Protection of statistical data (as one of the key obligations of the Agency), follows three basic aims:

1. *Data confidentiality* (protection against unauthorized access and processing),
2. *Data integrity* (protection against unauthorized changes) and
3. *Data availability* (protection against destruction).

Article 5

Protection of statistical data includes technical and organizational measures as well as procedures that are listed in the Rulebook, used for:

- Determining the authorization and responsibilities of the Agency's staff regarding data protection,
- Protection of collection, processing and data transfer,
- Protection of facilities, equipment and documents,

- Prevents the unauthorised persons access to equipment for processing or storing data,
- Preventing intentional unauthorized destruction or loss of data, its change, and
- Registration of access, use, processing, and publication of data.

Article 6

Units of statistical protection of data in the Agency are:

- Individual data with the identifier (confidential data collected within the frame of implementation of the Statistical Programme of Bosnia and Herzegovina and Working Plan of the agency),
- Individual data without the identifier (micro data) and
- Aggregated statistical data (macro data - tables) from which it is possible to recognize statistical units, i.e. individual micro data.

Article 7

Within the process of providing data to a user, it is obligatory to respect the principle of confidentiality. The principle of statistical confidentiality means that the data that could be attributed to the specific statistical unit must not be forwarded to the user outside the official statistical system, or data that would directly enable it.

Exceptionally, confidential data collected for statistical purposes may be published and provided in the following cases:

- If there is written approval from statistical unit to which the data refer to,
- If the data are taken from publically available collection of data,
- If the data are published by the statistical unit itself, and
- Statistical data on trade in goods statistics with foreign countries, for which, based on international standards, the principle of passive confidentiality is applied.

III. COLLECTION AND PROCESSING OF DATA

Article 8

In order to implement the Statistical Programme of Bosnia and Herzegovina and the Work Plan of the Agency, the Agency in cooperation with the Entity Statistical Institutes collects data from all existing primary and secondary sources.

Primary sources are natural and legal persons, and secondary sources are carriers of official and other administrative data bases.

Statistical units are familiar with the fact that the confidentiality of statistical data is guaranteed, and that the data must not be provided to other users of the data, in the form and way that enables the identification of the statistical unit to which the collected data refer.

Article 9

Data from primary sources shall be collected through questionnaires – forms. In this way, the individual data with identifier shall be collected, i.e. individual data with identifying characteristics.

Collected individual data with identifier shall be stored separately from the original identification data on individual or business subject to which the data refer to, i.e. name and surname or name of business subject shall be removed, and year of birth or age and phone number shall be retained / stored.

In the data collection process the Agency introduces data respondents with the purpose, scope and method of data collection, and with the rights and obligations of the persons who collect data, meaning and content of register and other identification characteristics.

Article 10

Secondary data collected by the Agency for statistics purposes from administrative data bases, shall be taken over in accordance with specific procedure that shall be agreed with the respondents and adjusted to their and Agencies abilities.

Procedure of taking over shall be recorded and documented for every secondary source in particular.

The procedure for take over shall be organized in a way to:

1. Appoint authorised persons for data handover in the Agency and with the respondents;
2. Agree the way, time and completion of handover;
3. After the handover to the authorized person, fill out and sign the "TRANSFER LIST" (one copy for the Agency and a copy for respondents);
4. Under the procedure of processing activities in the Agency, all important elements shall be recorded in the document "PROCESSING LIST";
5. Removable media (which contain data) shall be stored and recorded in the protocol of data holders.

Written request for data delivery shall be submitted to the responder with the following information: legal ground from the law for taking over the data and legal ground from the Statistical Programme of Bosnia and Herzegovina and Work Plan of the Agency, purpose for data use and names of the persons in the Agency who are responsible for taking over, use and protection of overtaken data.

Upon the receipt of data the replacement of data identifiers from administrative sources into the statistical identifiers shall be done in a way that enables subsequent reverse connection of data for statistical purposes.

Data from administrative sources shall be stored under specific organizational, physical and computing programme conditions on the server that are not visible in the computer net. Data protection from secondary sources shall be organized in the way that for the data processing

in the Agency the right to access to data shall be assigned to a particular administrator who is responsible for the work with these databases.

Article 11

Data transmission by information, telecommunication, and other means is possible only after the implementation of all measures and procedures that prevent access of unauthorized personnel as well as change and destruction of data.

Both, personnel of the Agency, and other stakeholders who participate in the statistical production process must implement measures and procedures for data protection regulated by this Rulebook.

Article 12

Director of the Agency issues permission for access to premises, devices and software, and by that the access to protected data.

Department for Legal, Personnel, and General Affairs of the Agency prepares the permissions and keeps records on issued permissions.

Article 13

Employees of the Agency must not bring out of the Agency the carriers of protected data without the permission issued by Director or other authorised person who is appointed by the Director.

Protected data that are transmitted electronically are protected by electronic signature or in any other appropriate way.

Article 14

Both, personnel of the Agency, and other stakeholders who participate in the statistical production process must implement measures and procedures for data protection regulated by this Rulebook.

Persons who, based on signed agreement, perform certain tasks for the Agency are obliged to keep confidential the official secrets, and content of data that are at disposal during their work. A responsible person from the Department for Legal, Personnel, and General Affairs shall inform them about it when signing a contract.

If for a certain statistical surveys a direct collection of data from natural and legal persons through interview is needed, the interviewers, in the sense of data protection, have the same responsibilities and obligations as employees of the Agency.

Employees from the Agency, interviewers, and other contracted personnel for carrying out certain tasks for the Agency, before starting the work are obliged to sign a declaration on data protection that is an integral part of this Rulebook.

Article 15

Based on written proposal of the head of organizational unit the Director shall issue the permission for employees of the Agency and other contracted persons for contingent work by which the access to protected data, premises, and devices is allowed.

Department for Legal, Personnel, and General Affairs of the Agency shall prepare permissions and keep records on already issued permissions.

The same rules for issuing permission apply for the revocation of the issued permission.

IV. DATA EXCHANGE WITHIN STATISTICAL SYSTEM OF BOSNIA AND HERZEGOVINA

Article 16

Transmission of data within statistical system of Bosnia and Herzegovina shall not be subject to limitations related to data confidentiality.

Confidential data within the statistical system of Bosnia and Herzegovina could be exchanged for the purpose of production of statistical data of BiH, implementation of Statistical Program of BiH and Work Plan of the Agency.

Exchange of confidential data between entity statistical institutions shall be done under already agreed procedure.

V. DATA EXCHANGE BETWEEN INTERNATIONAL INSTITUTIONS IN THE AREA OF STATISTICS

Article 17

Regarding the fulfilment of international obligations in the area of statistics, the Agency submits and exchange data between Eurostat and other EU institutions.

The process of submitting and exchange of data concerning the fulfilment of international obligations of the Agency shall be determined by specific instruction that primarily regulates the area of exchange between Eurostat and other EU institutions.

Data exchange shall be done through organizational unit within the Agency that is in charge for submitting and exchange of data between Eurostat and other EU institutions.

VI. ACCESS TO MICRO DATA FOR RESEARCH PURPOSES

Article 18

The access to micro data for research purposes is allowed to registered scientific-research institutions and registered researchers.

The access to micro data for research purposes shall be approved exclusively after:

- Filling in the *Form for Access to Micro data for Scientific Purposes* (Annex 1 to Rulebook), or *Form for Access to Micro data for Analytical purposes in the Government Bodies* (Annex 1 a. to Rulebook),
- Signing the *Declaration on Data Protection* (Annex 2 to the Rulebook), and
- Conclusion of *Agreement for Access and Use of Data* (Annex 3 to the Rulebook).

Micro data for scientific purposes are available on *removable media*, by access to data in *the secured room*, or *online access*.

Prior to approval for access to data for scientific purposes, it is necessary that research institution or registered researcher presents confirmation on registration.

Article 19

Prior to conclusion of the contract the commission for statistical confidentiality and data protection, scrutinizes the proposal of the contract.

The contract must contain the status of the user, purpose of use of data, method for data protection, method, and deadlines of publication of data.

The obligation of data protection does not stop after the contract expires.

The agreements shall be archived in the Agency, in Department for Legal, Personnel, and General Affairs.

Article 20

Pursuant to the Article 18 of the Rulebook, the users shall have access to micro data for research purposes and shall be recorded in the *Data Users' Register*.

The following information shall be recorded in the Data Users' Register: name and surname of the researcher (i.e. name of scientific research institution); address, telephone, e-mail; code of researcher / scientific research institution; name of research project; short description of used micro data (used variables from statistical research); where and when the results from statistical analysis i.e. research will be published.

VII. RIGHT TO ACCESS PROTECTED PREMISES, DATA AND DOCUMENTS

Article 21

Protected premises in the Agency, according to the function, are divided into three categories:

- *Premises for regular work*,
- *Premises for special purposes and*
- *The highest protection level premises.*

Article 22

Premises for regular work are premises where employees from the Agency perform regular work on working stations. House Rules regulate the access to these premises and protection of entrance in the premises of the Agency.

Employees who permanently or temporarily work in these premises are responsible for the protection of premises, equipment, and access to data. The employees must respect general rules for ensuring protection of premises, data, documents, and equipment (locking the premises during the absence, adequate storage of documents and other measures).

Article 23

Premises for special purposes are the premises where the equipment or documents are placed (servers, network equipment, documents, archive, cash register, etc.) and working places where the working stations with the access to protected data under special conditions are placed.

Entrance to these premises shall be allowed only to authorised personnel and to others only with the presence of authorised personnel.

Pursuant to provisions of the Rulebook the Director issues more detailed instructions on conduct in these premises.

Article 24

The highest protection level premises are the premises where the equipment and documents are placed, and working place of special importance.

Entrance to these premises shall be allowed only to authorised personnel and to others only with the presence of authorised personnel.

Each entry to these premises is recorded and the following information are entered: date and time of entrance, name and surname of the person who entered, name of task that is to be done in the premise, date and time of leaving the premises and signature of authorised person.

Pursuant to provisions of the Rulebook, the Director issues more detailed instructions on conduct in these premises.

VIII. PROTECTIONS AND MAINTENANCE OF HARDWARE, SOFTWARE, AND PREMISES

Article 25

Access of authorised personnel for maintenance of hardware within regular working hour is allowed exclusively in the presence or under written authorisation of the employee who is the user of hardware or authorised person allowed to access the protected premises with limited access.

Article 26

The access to the premises and computer equipment outside of working hours, as well as in the cases when the Agency's employees are not present in the workplace, is allowed to maintainers of computer equipment and premises only under written authorization of the Director of the Agency.

Article 27

External contractors can maintenance the computer equipment and software in the Agency only under appropriate contract with clearly indicated provisions related to data protection.

If the maintenance of computer equipment is awarded to external contractor, it is mandatory to be performed in the presence of maintainers from the Agency. The external maintainers shall enter or leave the premises of the Agency only in the presence of employees from the Agency.

Article 28

All interventions on hardware and software, and on working stations that enable the access to protected data, shall be recorded and described.

Repair, replacement, or update of software is exclusively allowed to the maintainer of computer equipment and authorised contracted external maintainers.

IX. PRODUCTION OF DRAFT BACKUPS AND PASSWORDS

Article 29

In order to prevent data loss, authorised personnel shall regularly produce daily, weekly and monthly draft backups of data basis (draft BACKUPS).

Two copies shall be produced and one of them will be stored on the external magnetic media until the professional DATA STORAGE is purchased.

Article 30

Authorised person responsible for certain statistical survey shall write the application for material ready for archiving to be included in production of backup copies.

Article 31

Backup copies will be stored in a fireproof closet in the Agency.

Usability of copies shall be regularly monitored. The copies shall be destroyed 12 months after the moment of their production.

Article 32

The user usually once a month changes the password that allows access to protected data.

Only authorised person with corresponding explanation may directly change the passwords of each user, user group or all users in the Agency.

Article 33

User password is confidential and shall not be provided to unauthorised personnel.

Authorised personnel and other employees from the Agency may provide passwords for protected access to protected database exclusively to the Director of the Agency upon his request.

Article 34

User password for access to system, database, web applications and hardware is kept in sealed envelopes.

The authorised person records the change of user passwords (data base administrator or system administrator) in the document *»Passwords for hardware and application«* for each hardware and each application.

The document *»Passwords for hardware and application«* contain the following information:

- Name of hardware and/or application:
- Inventory number of hardware:
- Location of hardware:
- Name and surname of a person responsible for hardware/application:
- Date:
- Signature:
- Password for hardware and/or application:
- Instructions and notes to use passwords:

The following information shall be written on the sealed envelope:

- Name of hardware or application:
- Inventory number of hardware:
- Location of hardware and application:
- Name and surname of a person responsible for hardware/application:
- Date:
- Signature:

Sealed envelope shall be archived in fireproofed closet. Additional documents that refer to the same hardware or application may be inserted into the sealed envelope.

Article 35

Only in exceptional circumstances, the authorised personnel can use sealed envelope. Any use of content of sealed envelope shall be documented. The owner of user password or his/hers immediate superior shall be noticed on use of content in the sealed envelope.

X. STORAGE, ARCHIVING AND DESTRUCTION OF DATA

Article 36

The Agency is obliged to remove the indicators of statistical units after processing collected data or data taken from administrative sources, and also after using the data for update of statistical registers.

The Agency is obliged immediately to destroy (after entering, coding and processing data) statistical questionnaires and other documents that contain statistical data.

Article 37

The Agency is obliged to archive and store data without identifiers in electronic form organized and coded at the level of statistical unit at least ten years unless otherwise stated by specific regulation.

Article 38

Production of archive copies shall be done annually in line with standard procedures on archiving unless otherwise regulated.

Two archive copies shall be produced. One shall be stored in protected place in the Agency, where the copy is produced, and second in the other protected place in the Agency.

Article 39

Upon the archive expiration, the data shall be deleted. Method of deletion shall be used for deleting data from computer media. This method prevents restauration of all or part of deleted data.

Data on documents or other classical forms of media shall be destroyed in a way that prevents reading of all or part of destroyed data.

All supporting materials shall be destroyed as well. It is forbidden to put media with protected data in the waste bin.

The procedures for the destruction of data shall be regulated by a specific instruction.

XI. COMMISSION FOR PROTECTION OF STATISTICAL DATA CONFIDENTIALITY

Article 40

Commission for Protection of Statistical Data Confidentiality as an advisory body to the Director shall be established in the Agency (hereinafter CPDC). Director of the Agency shall appoint the members of CPDC by separate decision. Number of CPDC members must be odd.

Members of CPDC shall be employees from the Agency who are managers of sectors/departments that are in charge for statistical methodologies, social, business and

economic statistics, statistics of agriculture and environment, dissemination and informatics, and legal advisor.

Chairperson of CPDC is Head of *Sector for Statistical Methodologies and Standards*.

CPDC tasks:

- Consistent implementation of the Rulebook and other regulations related to data protection;
- Scrutinizing the requests for access to confidential data;
- Reporting to Director on situation related to statistical data protection in the Agency.

XII. RESPONSIBILITY FOR IMPLEMENTATION OF PROTECTION MEASURES

Article 41

For all conduct contradicting the regulations of the Rulebook, employees of the Agency are disciplinary responsible and responsibilities of other actors are pursuant to the obligations under the contract.

Article 42

Any kind of criminal liability, minor offence liabilities, and damage caused to third persons shall not exclude disciplinary responsibility or responsibility for compensation of damage of employees of the Agency resulted in reference to data protection.

XIII. TRANSITIONAL AND FINAL PROVISIONS

Article 43

This Rulebook shall enter into force on the day of signature.

Article 44

This Rulebook shall be published on website of the Agency.

No: 01-02-3-603- 1/16

Sarajevo, 19 May 2016

D I R E C T O R

Mr. Sc. Velimir Jukić