On the basis of the second paragraph of Article 42 of the National Statistics Act (Ur.l.RS, no. 45/1995 and 9/2001) and Article 14 of the Personal Data Protection Act (Ur.l.RS, no. 59/1999 and 57/2001) the Director-General of the Statistical Office of the Republic of Slovenia hereby issues

Rules on procedures and measures for the protection of data collected through programmes of statistical research at the Statistical Office of the Republic of Slovenia

I. General Provisions

Article 1

By means of these rules, the Statistical Office of the Republic of Slovenia (hereinafter: the Office) regulates the internal organisation of work in a manner that ensures protection of data collected through programmes of statistical research (hereinafter: data), in order to prevent unauthorised access, processing, use, destruction, modification or transmission of the data.

Article 2

Terms used in these rules shall have the following meaning:

1. personal data are data that describe the characteristics, circumstances or relations of an individual;
2. individual data are data that describe the characteristics, circumstances or relations of an individual or legal entity and are part of the overall data about a reported unit;
3. confidential statistical data are individual data that is communicated to the Office by respondents for the purpose of carrying out programmes of statistical research;
4. micro-data or de-individualised data are individual data which have been changed in such a way that it is not possible to identify the entity to which they refer;
5. identifier is the part of individual data that uniformly identifies the link between the data and the respondent in such a way that the data describe a specifically defined entity;
6. identification data are the part of individual data that uniformly identifies the link between the data and the respondent (data on birth, address, telephone number etc.);

7. primary data are data that the Office obtains directly from respondents;
8. secondary data are data that the Office obtains from holders of official and other administrative databases;
9. a carrier of data is any medium containing data entered in a classical or computerised manner
10. protected data are all individual data collected through implementation of programmes of statistical research, aggregated statistical data prior to the time of publication and aggregated statistical data from which it is possible to infer individual data;
11. protected premises are all premises of the Office in which carriers of protected data are located or premises in which equipment is located through which it is possible to access this data;
12. protected premises with restricted access are premises within the Office to which access is only allowed under special conditions determined by these rules.
13. users means anyone who uses data from the Office.

Article 3

(1) Protection of data shall cover techniques, rules and procedures for preventing unauthorised interventions into protected data.

(2) The regulation of data protection specifies data protection during its exchange with authorised implementers of programmes of statistical research (hereinafter: authorised implementers) and with international organisations, during the collection and processing of data and during transmission of data to users.

(3) Protecting data shall cover measures of a technical or organisational nature and procedures specified in these rules, by which:
- the authorities and duties of staff of the Office in connection with protecting data are specified;
- collecting, processing, mediation and transmission of data is protected;
- premises, equipment and documents are protected;
- access by unauthorised persons to equipment in which data are processed or stored is prevented;
- intentional unauthorised destruction or loss of data, its modification or unauthorised processing is prevented;
- access to data and use, processing and displaying data are recorded.

Article 4

(1) These rules shall specify protection in the Office:
- of individual data collected through implementation of programmes of statistical research and
- aggregated statistical data prior to the time of publication, and
- aggregated statistical data from which individual data may be inferred.

(2) The same provisions shall apply for the protection of data in collecting secondary and primary data.

(3) In communicating or use of data in the manner referred to in Article 18 of these rules, statistical aggregates, micro-data and individual data shall be protected.

Article 5

In communicating data to users, the principle of statistical confidentiality shall be respected. The principle of statistical confidentiality means that no data may be communicated to users outside the system of national statistics, which can be ascribed to a particular observation unit or which could indirectly enable this.

II. Exchange of Data with Authorised Implementers of Programmes of Statistical Research

Article 6

The principle of statistical confidentiality shall not apply to the communicating of data within the system of national statistics. In communicating data within the system of national statistics, in compliance with the provisions of the National Statistics Act, individual data with identification for the needs of implementing programmes of statistical research may be exchanged. The exchange of data shall take place according to previously adopted procedures.

III. Exchange of Data with International Organisations in the Field of Statistics

Article 7

(1) In meeting international obligations, data shall be communicated to and exchanged with other countries and international organisations. In meeting international obligations, the Office shall cooperate with authorised implementers of national statistics, with state bodies and local government bodies.

(2) The procedure for communicating and exchanging data for meeting the international obligations of the Office shall be designated by special instructions, which shall regulate in particular the field of exchange of data with Eurostat and other institutions of the European Union.

Article 8

The exchange of data shall be carried out through organisational units responsible for communicating data.

IV. Collecting and Processing Data

Article 9

(1) Data for implementing programmes of statistical research shall be collected from all existing sources, primary and secondary.

(2) Primary sources shall be natural persons or legal entities, and secondary sources holders of official and other administrative databases.

(3) In collecting data, respondents shall be acquainted with the fact that the confidentiality of the collected statistical data is guaranteed.

(4) Collected data may not be transmitted to other users of data in a form or in a manner that allows the identification of the respondent to which the collected data refer. The Office may use the obtained data for the elaboration of samples, for carrying out statistical research and for statistical analysis.

(5) Collected individual statistical data shall be stored separately from original identification data on the individual or business entity to which the data refer.

(6) Transmission of data by computer, telecommunications or other means shall only be possible by carrying out procedures and measures that prevent the appropriation or destruction of data or improper access to the data by unauthorised persons.

Article 10

(1) Secondary data that the Office obtains for statistical needs from administrative databases on the basis of Article 32 of the National Statistics Act, shall be received in compliance with special receipt procedures which shall be agreed with the providers of the data and shall be adapted to their capacities and the capacities of the Office. A receipt procedure shall be recorded and documented for every secondary source of data individually.

(2) The receipt procedure shall be organised in such a way that:
1. authorised persons for handover of data are designated at the Office and at the data provider;
2. the method, time and place of handover is agreed;
3. at the time of handover the authorised persons complete and sign a “RECEIPT NOTE” (one copy for the Office and one copy for the data provider);

4. during handling of data after receipt, technological activities and technological events are concurrently recorded in a document "TECHNOLOGICAL NOTE";
5. at the time of returning the data carrier to the data provider, the authorised persons agree on the method, time and place of the reverse handover;
6. at the time of the reverse handover the authorised persons complete and sign a “DELIVERY NOTE” (one copy for the Office and one copy for the data provider);
7. in the case of storage of a received data carrier with data, it is filed and noted in the entry archive of the physical data carrier.

(3) A written request shall be sent to the data provider for the communication of data and in it stated the statutory basis for obtaining the data and the legal grounds from the programme of statistical research, the intended use of the data and the names of persons that will be responsible in the Office for the receipt, use and protection of the communicated data.

(4) After receipt of the data, the source identification code shall be replaced by a statistical identifier in a manner that enables subsequent reverse linkage of the data for statistical and scientific and research purposes.

(5) Data shall be stored under special organisational, physical and computer programme conditions on servers that are not visible in the computer network of the Office. Concealing data from secondary sources shall be arranged in such a way that the right to access data for the purpose of processing data within the Office shall be granted to individuals (trustees).

Article 11

(1) Primary data shall be collected by means of questionnaires.

(2) Individual data with identifiers or individual data with identification data shall be collected in the manner referred to in the first paragraph. In the case of individual data with identifying data, the name and surname shall be removed, but the year of birth or age or telephone number shall be retained.

(3) When collecting data, data providers shall be acquainted with the purpose, extent and method of collecting data, with the rights and obligations of persons that collect the data, with the meaning and content of registration and other identification marks and with the confidentiality of the statistical data used.

(4) The same provisions apply for the protection of data from primary sources as for data from secondary sources.

Article 12

(1) Staff of the Office may not remove protected data carriers from the premises of the Office without permission, which shall be issued by the director or a person so authorised by the director.

(2) Protected data that is transmitted electronically shall be protected with an electronic signature or in another suitable manner.

Article 13

(1) Measures and procedures for protecting data specified in these rules must be carried out by staff of the Office and other persons who cooperate in the process of producing statistics. Staff shall carry out measures and procedures for protecting data in compliance with these rules and other regulations that govern the protection of data.

(2) Staff of the Office and providers who occasionally perform specific tasks for the Office on the basis of contract, must protect as an official secret the content of the data of which they become aware in their work. The responsible person in the personnel service shall acquaint them with this when they start work.

(3) The duty to protect official secrets referred to in the previous paragraph shall continue after the cessation of employment.

(4) If the direct collection of data from natural or legal persons is required for the implementation of individual statistical research, those carrying out the poll have the same obligations in relation to data protection, mutatis mutandis the same position as staff of the Office.

(5) Staff of the Office, polling personnel and operators that perform specific tasks for the Office on the basis of contract, must sign the declaration on data protection, which is attached to these rules, prior to the commencement of work.

Article 14

(1) The authority by which staff of the Office, contract operators and those who occasionally cooperate are allowed access to protected data or to premises, machinery and programmes through which it is possible to access protected data, shall be issued by the director of the Office on the basis of a written proposal by the head of the organisational unit.

(2) Forms for authority are annexed to these rules.

(3) The personnel service of the Office shall prepare authorities and keep and maintain records of authorities issued.

(4) The same provisions shall apply for revoking authority as for issuing authority.

Article 15

The method of guaranteeing the protection of statistical aggregates from discovery shall by regulated by special methodological instructions.

V. Access to Data for Research Purposes

Article 16

(1) For purposes of polling, only the follow personal data shall be communicated to research institutes and registered individual researchers: name and surname of an individual, residence, date of birth, sex and profession.

(2) Before communicating data referred to in the previous paragraph, the research organisation or registered individual researcher shall sign the declaration on data protection which is annexed to these rules.

(3) A registered research organisation or registered individual researcher may use micro-data and individual data for research purposes. Access to individual data shall only be possible in a secure room within the Office.

(4) Evidence of the registration of individual researchers may not be older than 30 days.

Article 17

(1) Data for research purposes may only be used by a registered research organisation or registered individual researcher that has concluded an appropriate contract with the Office, which must contain the status of the user, the intended use of the data, protection of data and the manner and time of publication of the data.

(2) A proposal for concluding a contract shall be discussed by the Committee for Data Protection before the contract is concluded. Contracts shall be kept by the legal affairs service.

Article 18

(1) A secure room is working premises in the Office in which access and use of micro-data is made possible to registered research organisations and registered individual researchers and access and use

of micro-data and individual data to researchers and authorised persons from international organisations.

(2) The cooperation of researchers or authorised persons from international organisations and the Office in work using micro-data and individual data shall only be possible on the basis of a written request for access and use of data. The contract or agreement on cooperation shall specify the agreed participating and authorised persons, the content, purpose, extent and duration of the cooperation and the obligations of participating individuals and participating organisations and the conditions and measures for ensuring the protection of data.

(3) The following shall be provided for each cooperation:
1. working premises,
2. agreed equipment,
3. communication,
4. documentation on the content,
5. documentation on applications,
6. documentation on equipment,
7. access to data, in accordance with the contract or agreement,
8. programme equipment,
9. training in the use of the equipment and applications,
10. maintenance of communications, applications and equipment.

Article 19

The obligation to protect data shall not cease with the cessation of validity of the contract or agreement.

Article 20

Users who access data in accordance with Articles 16 and 18 shall be entered in a register of data users. The following data shall be entered in the register: name and surname or title, code of the researcher, institution, research project, description of the micro-data used, where the aggregated data will be published and the name of the authorised person on the part of the Office.

VI. Archiving and Destroying Data

Article 21

(1) Production of archive copies shall take place annually in accordance with standard procedures, unless otherwise specified for an individual case.

(2) Two archive copies shall be produced, of which one shall be stored in a secure place within the Office where the copy shall be made, and the other in another secure place within the Office.

Article 22

(1) After the procedure of archiving is complete, the data shall be erased. For erasing data from computer media, the method used shall prevent restoration of all or part of the erased data.

(2) Data on documents or other forms of classical media shall be destroyed in a manner that prevents reading all or part of the destroyed data.

(3) All auxiliary material must also be destroyed in the manner referred to in the first and second paragraph of this article. Material containing protected data may not be discarded into a rubbish bin.

(2) Procedures and instructions for destroying data shall be regulated by special instructions.

VII. Right of Access to Protected Premises, Data and Documents

Article 23

Protected premises within the Office shall be divided into three categories in relation to the functions that they perform:

- category A premises,
- category B premises and
- category C premises.

Article 24

(1) Category A premises shall be premises in which staff of the Office carry on the regular working process at workstations. Access to such premises shall be regulated within the framework of office rules and secure access to the premises of the Office.

(2) Staff who work in the premises permanently or temporally shall be responsible for protecting the premises, equipment and access to data. They must respect in this the general rules by which the security of premises, data, material and equipment is ensured (locking premises in absence, care for passwords to work stations and similar, suitable storage of working material).

Article 25

(1) Category B premises are premises in which equipment or material (servers, network equipment, fax, telephone exchange, documentation,

archives, goods and similar) and working posts of special importance (working stations with access to protected data under special conditions).

(2) Category B premises shall be marked with a sign »CATEGORY B PREMISES, RESTRICTED ACCESS, Authorised person: NAME AND SURNAME«. Access to category B premises shall only be permitted to authorised persons, and other persons only when accompanied by an authorised person.

(3) The director shall issue more detailed instructions on behaviour in category B premises in accordance with the provisions of these rules.

Article 26

(1) Category C premises are premises in which equipment or material and working positions of special importance are located, or the highest level of protection.

(2) Category C premises shall be marked with a sign »CATEGORY C PREMISES. ACCESS PROHIBITED TO UNAUTHORISED PERSONS«. Access to category C premises shall only be permitted to authorised persons, and to other persons only accompanied by an authorised person.

(3) Every entry to category C premises shall be recorded with the following data: date and hour of entry, name and surname of person who entered the premises, title of task in the premises, date and hour of exit from the premises and signature of the authorised person.

(4) The director shall issue more detailed instructions on behaviour in category C premises in accordance with the provisions of these rules.

VIII. Protection during Maintenance of Computer Equipment and Programmes and the Premises

Article 27

Access by authorised persons for maintenance of computer equipment (hereinafter: computer maintenance staff) to premises and computer equipment shall be possible during normal working time in the presence or with the consent of the member of staff of the Office who is the user of the equipment or an authorised person with the right of access to protected premises with restricted access.

Article 28

Outside working hours of the Office and when staff of the Office are not present at their working posts, computer maintenance staff and maintainers of the premises shall have the right to access to the premises and computer equipment on the basis of authority referred to in Article 14 of these rules.

Article 29

When maintenance of computer equipment is carried out by an external operator that performs agreed services by contract, a computer maintainer from the Office must always be present. The external maintainer may only enter and leave the premises of the Office accompanied by Office staff.

The provisions of the previous paragraph shall not be used for maintainers of premises and security staff. Maintenance and security staff may have access to protected premises of the Office only if the computers are switched off or programmes closed.

Article 30

Each intervention for maintaining computer equipment and programmes and any work at work stations from which it is possible to access protected data, shall be recorded and described.

Article 31

Maintenance of computer hardware and software in the Office may only be carried out by external operators that have concluded a suitable contract with the Office, which must also contain provisions relating to the protection of data.

Article 32

Repairing, modifying or supplementing computer programmes shall only be permitted by computer maintenance staff and authorised external maintainers that have concluded a suitable contract with the Office.

IX. Back-up Copies, Lists and Passwords

Article 33

Authorised persons shall regularly make back-up copies of computerised data collections. Back-up copies shall be made each working day. At least the last three variants produced shall be kept.

Back-up copies shall be stored in a locked fireproof cabinet in the premises of the Office. The serviceability of copies shall be regularly checked.

Article 34

Uses shall generally change user passwords allowing access to protected data once a month.

Irrespective of the provisions of the previous paragraph, an authorised person may make a suitably reasoned request for the immediate change of user passwords of any individual user, group of users or all users in the Office.

Article 35

(1) User passwords shall be confidential and may not be communicated to unauthorised persons.

(2) Authorised persons and other staff of the Office may only tell the content of user passwords by which access to collections of protected data is protected, to the director of the Office on his reasoned request.

Article 36

(1) User passwords for access to systems, databases and applications on servers and equipment shall be stored in sealed envelopes. Changes shall be recorded by an authorised person (guardian or administrator of databases or systems administrator) in a document »Passwords of equipment or applications« for each item of equipment or application individually.

(2) The document »Passwords of equipment or applications« shall contain in particular the following data:
- Title of equipment and/or application:
- Inventory number of the equipment:
- Location of the equipment:
- Name and surname of trustee:
- Date:
- Signature:
- Password of the equipment and/or application:
- Instructions and warnings for using the password and for starting up the equipment in question:

(3) The following data shall be written on the sealed envelope:
- Title of equipment and/or application:
- Inventory number of the equipment:
- Location of the equipment or application:
- Name and surname of guardian:
- Date:
- Signature:

(4) The sealed envelope shall be stored in a fireproof cabinet.

(5) Several documents relating to the same equipment or application may be stored in an individual sealed envelope.

Article 37

The sealed envelope with passwords may only be used by authorised persons in exceptional circumstances or in urgent cases. Each use of the contents of the sealed envelope shall be documented. The owner of the password shall be informed about the use of the contents of the sealed envelope, and if this is not possible, her or his immediate superior shall be informed.

X. Committee for Data Protection

Article 38

(1) A Committee for Data Protection shall be created in the Office as an advisory body to the director of the Office. Members of the Committee for Data Protection shall be appointed by the director of the Office from among experts in the Office, experts from authorised operators and external experts in data protection.

(2) The tasks of the Committee for Data Protection shall be:
- Ensuring implementation of the provisions of these rules and other regulations in the field of data protection;
- Dealing with cases and advising the director of the Office on questions which cannot be resolved within general rules in the field of data protection;
- Reporting to the director of the Office and the Statistical Council of the Republic of Slovenia on conditions in the field of data protection in the Office, not later than 30 April of the current year for the past year.

XI. Responsibility for Carrying out Security Measures and Procedures

Article 39

Staff of the Office shall have disciplinary responsibility for all behaviour that is in conflict with the provisions of these rules, and other persons on the basis of contract obligations.

Article 40

Possible criminal responsibility, responsibility for violations and responsibility for damages caused to third persons occurring in

connection with protection of data does not exclude disciplinary and damages liability of staff of the Office.

XII. Final Provisions

Article 41

Interpretation of these rules shall be within the competence of the director of the Office.

Article 42

These rules shall enter into force on the day that it is signed by the director of the Office and shall be published on the notice board of the local network server.

No.: 947-05-2/03
Date: 27. 2. 2003

Tomaž BANOVEC
DIRECTOR-GENERAL