Joint UNECE/Eurostat work session on statistical data confidentiality
(Skopje, 20 to 22 September 2017)

Topic (III): Confidentiality of big data and special types of data

Data confidentiality and statistical registers in the Macedonian statistical system

Mirjana Boshnjak
mirjana.bosnjak@stat.gov.mk
State Statistical Office of the Republic of Macedonia (SSO)

Abstract: The State Statistical Office of the Republic of Macedonia (SSO) is fully in line with the sixth United Nations Fundamental Principle of Official Statistics, which refers to statistical confidentiality - "Individual data collected by statistical agencies for statistical compilation, whether or not they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes".
The SSO is authorised to establish and maintain databases and statistical registers in the country, based on a prescribed statistical methodology. The use of administrative sources is becoming increasingly important for establishing and maintaining statistical registers.
All necessary administrative, methodological, technical and organisational measures are taken to ensure the confidentiality of statistical data in registers. Confidentiality embraces the responsibility for both protecting data from unauthorised access and ensuring its beneficial use for statistical purposes. The measures are aimed at assisting the Departments in the SSO in implementing systems and procedures that ensure, as much as possible, that individual data in statistical registers are kept safe, secure and available for statistical compilation.
A number of general procedures have been established at the SSO with respect to storing, handling and protecting individual data, and measures have been put in place to monitor the implementation of the general procedures for data confidentiality.

1. Introduction

State statistics is an independent professional activity, which conducted on a scientific basis, provides users (legal and natural persons) with data on the economy, demography, social life, environmental protection and other areas.
The SSO is authorised to establish and maintain databases and statistical registers in the country, based on a prescribed statistical methodology. The use of administrative sources is becoming increasingly important for establishing and maintaining statistical registers.

***Article 25-a* of the Law on State Statistics**
The Office shall use data from data sets, censuses, surveys and statistical data collected by observation and monitoring, for organising and maintaining statistical registers.

***Article 25-c* of the Law on State Statistics**
Data from statistical registers shall be used exclusively for statistical purposes.
Statistical purpose in terms of paragraph 1 of this Article shall mean use of data from statistical registers for conducting statistical surveys, and publication of statistical data.

The State Statistical Office of the Republic of Macedonia (SSO) is fully in line with the sixth United Nations Fundamental Principle of Official Statistics, which refers to statistical confidentiality - "Individual data collected by statistical agencies for statistical compilation, whether or not they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes".
It is clearly stated in the Law on State Statistics that the activities of state statistics shall be performed according to the principles of professional independence, impartiality, objectivity, reliability, statistical confidentiality and cost-effectiveness.

***Article 4-a* of the Law on State Statistics**
"statistical confidentiality" shall mean that data collected from reporting units through statistical surveys or indirectly, from administrative or other sources, are confidential and shall be used for statistical purposes only, which prohibits the use of data for non-statistical purposes and their unlawful disclosure.

2. Administrative, methodological, technical and organisational measures

All necessary administrative, methodological, technical and organisational measures are taken to ensure the confidentiality of statistical data in statistical registers. Confidentiality embraces the responsibility for both protecting data from unauthorised access and ensuring its beneficial use for statistical purposes. The measures are aimed at assisting the Departments in the SSO in implementing systems and procedures that ensure, as much as possible, that individual data in statistical registers are kept safe, secure and available for statistical compilation. A special article in the Law on State Statistics is dedicated to ensuring the protection of confidential data.

***Article 43 of the* Law on State Statistics**
To ensure the protection of confidential data collected for statistical purposes, measures shall be taken against unauthorised access, transmission or any unauthorised processing, as well as measures to prevent the destruction, loss, modification, misuse or unauthorised use of data.
A number of general procedures have been established at the SSO with respect to storing, handling and protecting individual data, and measures have been put in place to monitor the implementation of the general procedures for data confidentiality.
SSO has established a System for technical and organisational measures for providing security and protection of data in Registers. The SSO is applying technical and organisational measures that are classified at three levels: basic, medium and high level. For all documents, it is obligatory to apply technical and organisational measures that are classified at the basic level. Documents containing a citizen's national identification number are subject to technical and organisational measures that are classified at the

basic and medium level. For documents that are transmitted through an electronic communications network, it is obligatory to apply technical and organisational measures that are classified at the basic, medium and high level.
The measures that are taken are:

- Administrative - policies
- Organisational
- Technical - infrastructure

2.1 Administrative measures - policies

The first stage in establishing policies and procedures to ensure the protection of personal data is to know what data are held, where they are held and what the consequences would be, should these data be lost or stolen.
SSO has a Policy on Statistical Confidentiality - it is a basic policy that serves as a basis for a number of general procedures which describe: user responsibilities, risk management, administration procedures.
The Policy on Statistical Confidentiality aims to lay down the basic principles that are applied in the SSO, arising from the: Law on State Statistics, Code of Practice of European Statistics and Resolution of the United Nations on Fundamental Principles of Official Statistic.
The protection of statistical confidentiality is a complex concept and covers several phases of the statistical business process model: data collection, processing and dissemination.
The main responsibility for security lies with the Owner of the data. However, some security principles have to be clear to the Owner:

- Security is not only based on technical solutions; the organisational framework is equally important
- Security awareness plays an important role
- Security needs to be planned and integrated from the start
- Security measures must be understandable and effective

Besides the responsibilities of the Owner of the data, the most important are the responsibilities of the IT Department. For example: to define the organisational framework, to provide the technical infrastructure needed to ensure security, to provide support and a security awareness programme, to ensure that the safeguards approved are correctly applied. Furthermore, another important factor in the overall administrative system are users of data in statistical registers with their responsibilities: the security of the information in their workstation, correct use of their user ID and the protection of their password, compliance with security rules and procedures, notification of any security incident to administrators.

2.2 Organisational measures

It is necessary to have a good organisational framework for security administration. In SSO, the responsibilities are divided into 3 levels: department/sector level, user administrator level and resource administrator level. At the department/sector level, responsibilities include deciding “how much” security is needed, defining the security organisation at the level of department/sector. The user administrator level decides how many groups for access are needed in the department/sector, provides each person a user

ID, and ensures that each user has only the authorisations needed to perform their work. The resource administrator level reviews the authorisations given and the use of the resources, and ensures that all security authorisations are assigned on a need-to-work basis.

2.3 Technical measures - infrastructure

Within the scope of the IT infrastructure, the main task is to support Systems, Internet Access and Other Systems in SSO. SSO has a general policy for standard files: backup copy of modified files every day and databases: special logs – data recovery at any previous date – time. With regard to confidentiality, SSO has defined a policy for IT privileges for system administrators and access to production data at the network level, the database level and the application level. Special tools are available to manage those authorisations. Access to all server rooms used to host hardware and software on which personal data are stored should be restricted only to those staff members that have access to work there. A very important activity which ensures confidentiality is data transfers – removable media for transportation where such data must be encrypted using the strongest possible encryption method available. Also, the electronic submission of data takes place in a strictly controlled environment with the use of encryption.
The Director of the SSO authorises persons who perform transfer via media and direct transfer, and the activities have to be registered by the Officer for Data Protection.

In SSO, there are monitoring procedures at different levels:
- The administrator of the information system checks the functionality of the system and safety copies on a daily basis.
- The Officer for Data Protection records and monitors the overall process.
- The annual internal audit in accordance with the Audit Plan.

3. Graphical view of the organisation for security administration

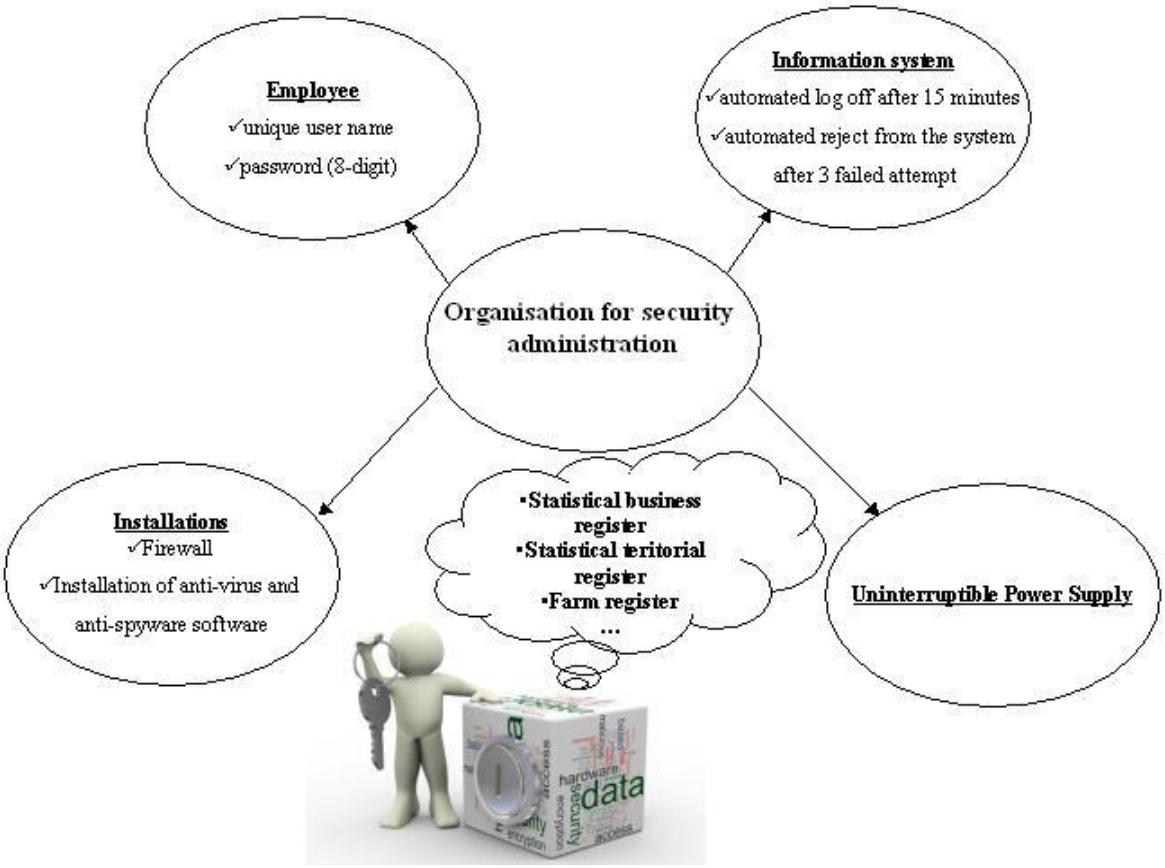

Figure 1. Technical measures for security and protection during data process

4. Conclusions

The confidentiality system in the SSO is established in a way that provides field data protection and protection of the data derived from administrative sources. The institutional image concerning the confidentiality is recognised in our society and also by the feedback from data users and data providers who assessed very highly the SSO's efforts in the field of data confidentiality. The improvement of the confidentiality system is an ongoing process, advancing in line with the development of modern infrastructure and raising staff awareness to the highest possible level.

Continuous efforts are made to educate employees and raise awareness of the importance of statistical confidentiality, its aspects, legal bases, procedures, and above all the fact that the weakest link in the system is always the human factor, rather than the legal and technological measures.

References

- Law on State Statistics - "Official Gazette" No. 54/1997, 21/2007, 51/2011, 104/2013, 42/2014 192/2015 and 27/16
- Policy on Statistical Confidentiality
- Rulebook on procedures and measures for protection of data collected within the Programme for Statistical Surveys in the State Statistical Office
- Internal general procedures in the SSO