**REPUBLIC OF MACEDONIA**

**DIRECTORATE FOR PERSONAL DATA PROTECTION**
Samoilova 10, 1000 Skopje, Tel:+389 2 3230-635 www.privacy.mk

# M A N U A L

## ON THE MANNER OF PERFORMING EXTERNAL CONTROL

(Unofficial translation)

**No. 02 – 904 / 1**
**18.05. 2012**

Based on the article 41 paragraph 1 line 1 and article 41-a line 4 from the Law on Personal Data Protection („Official gazette of Republic of Macedonia" no. 7/05, 103/08, 124/10 and 135/11) and articles 25 and 35-d from the Rulebook on technical and organizational measures for providing secrecy and protection of personal data processing („Official gazette of Republic of Macedonia" no. 38/09 and 158/10), director of the Directorate for Personal Data Protection has adopted

# MANUAL

# ON THE MANNER OF PERFORMING EXTERNAL CONTROL

## I. GENERAL PROVISIONS

**1**. This Manual was set up in order to describe the manner of performing external control of the information system and information infrastructure and of manual processing of personal data by the controllers (hereinafter: control) by the independent third legal subject (hereinafter: body performing control).

**2**. This Manuel shall provide:

- assessment of the level of compliance of the organization system introduced by the controller with the regulations on personal data protection,
- assessment of the adequacy of the controls on the system of personal data protection regarding the risk assessment by the controller,
- identifying the potential gaps and weaknesses of the data protection system,
- providing information for data protection system review,
- increasing the level of data protection awareness among management and staff and
- improving the personal data protection of natural persons, by reduction of the possibility of accidental or unlawful destroying of personal data, or their loss, modification, unauthorized disclosure and access, especially when processing includes transfer of the personal data through electronic communication network.

**3**. Specific terms used for this Manual have the following meaning:

1) **Control Plan** is a systematic and structured representation of the activities that should be performed by the person performing control in order to give his opinion.

2) **Control Opinion** The overall assessment of the control object against a set of technical and organizational measures for providing secrecy and protection of the processing of the personal data according the regulations on personal data protection.

3) **Person performing control** is an external independent and qualified person who performs control over the system of personal data protection.

4) **Body performing control** is legal person which fulfills the conditions determent in this Manual for performing control over the system of personal data protection.

5) **Compliance** is fulfilling the requirements for personal data protection in accordance with the regulations for personal data protection.

6) **Personal Data Protection Control** is a systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with the documentation for technical and organizational measures of the controller and whether this processing meets the data protection requirements.

7) **Data Protection Requirements** are the requirements which reflect obligations of controller for applying of proper technical and organizational measures for providing secrecy and protection of personal data processing in the process of introducing the personal data protection system.

8) **Data Protection System** is a set of documented policies, codes of practice, guidelines and procedures adopted by the controller, that contribute for enforcing technical and organizational measures for providing secrecy and protection of personal data processing, in accordance with the personal data protection regulations.

Terms used in this Manual whose meaning is not defined in paragraph 1 of this point, are determinate by personal data protection regulations.

## II. CRITERIA FOR PROVIDING INDEPENDENCY AND IMPARTIALITY OF THE BODY PERFORMING THE CONTROL

**4**. Body performing control its responsible persons and staff (persons performing control) responsible for performing control over the system of personal data protection shall not be the processor, third party, user, designer, manufacturer, supplier or maintainer of software programs for personal data processing, that are checked by that body, nor the authorized representative from any parties, or natural and legal person promoting the software programs on the market.

Body performing the control, its responsible persons and staff (persons performing control) shall not be involved directly or indirectly or as authorized representatives in designing, manufacturing, construction, marketing, maintenance or working with software programs for personal data processing, except in exchange of technical information between the manufacturer and that body.

Body performing control shall not perform control over the system of personal data protection in duration of three years from the date of ceasing the business relations mentioned in paragraphs 1 and 2 of this point.

**5**. Body performing control and staff (persons performing control) are obliged to perform the control over the system of personal data protection with highest level of professional integrity and technical competence and to be released from any pressure and influence, especially financial, which may reflect the results of the control, especially from persons or groups that have interest for the control results.

**6**. Body performing control is obliged to have the required professional staff (persons performing control) to be able to properly execute the administrative and technical tasks related to personal data protection system control activities.

Body performing control is obliged to have at least three permanently professional employees (persons performing control), who can be included in the process of personal data protection system control and to be awarded with one or more of the following certificates:

1. CISM (Certified Information Security Manager),
2. CRISC (Certified in Risk and Information Systems Control),
3. IS0 27001 Lead Auditor,
4. CISA (Certified Information Systems Auditor),
5. CISSP (Certified Information Systems Security Professional)
6. Positive opinion from the Directorate for Personal Data Protection regarding the compliance with the regulations for personal data protection.

**7.** Professional staff (persons performing control) who is responsible for control of the system of personal data protection shall own:

- quality technical and professional training,
- appropriate knowledge of the requests for personal data protection that are determinate in the regulations for personal data protection, and need to be proven by certificate from successfully attended training organized by the Directorate for Personal Data Protection and
- ability for compiling minutes and reports to prove that control was conducted.

**8.** Body performing control shall compulsory act in the field of information security or IT revision and to be certified according to the international standard ISO/IEC 27001.

Body performing control is obliged to guarantee impartiality of its professional staff (persons performing control) for performing control over the system of personal data protection and their salaries shall not depend of the number of performed controls or the results from those controls.

## III. MANNER OF PERFORMING CONTROL OVER THE SYSTEM OF PERSONAL DATA PROTECTION

**9.** The scope of the control over the system of personal data protection compulsory shall be defined in the Engagement Letter which according the agreement shall be concluded between the controller and the body performing control. In the Engagement Letter the scope of control over the system of personal data protection is particularly mentioned, targets to be fulfilled required resources, period of control and the report that shall be prepared (appendix no.1).

Controller and the body performing control mandatory concludes confidentiality agreement which defines the protection of secrecy of the data reviewed/disclosed during the control over the system of personal data protection.

**10.** Control over the system of personal data contains the following phases:

- Defining the task of performing control,
- Preparation for control,
- Conducting the control and
- Preparing opinion about the control – compiling Report

## 1. Phase 1- Defining the assignment of the control

11. The person performing control always controls the system of personal data protection for the needs of the controller, and because of this, the two sides should agree for the assignment, which is the starting point of control and the base for the Control plan.

Assignment for performing control should be documented and should, as a minimum, specify:

- The assigner and assignee,
- The objective and nature of the assignment,
- Explanation of the assignment,
- The controller,
- The scope of control, that is:

a) Object (s) (description of personal data processing operation)

b) Aspect (s) (confidentiality, integrity, continuity and controllability)

c) Requirements (which regulations, standards and best practices for personal data protection will be taken into account)

- The period,
- The ability to protect personal data (design, existence, effectiveness)
- Target group / users of control opinion,
- Form and frequency of reporting,
- The required time and budget,
- Limitations regarding the execution of control,
- Access to information
- References to applicable legislation and
- Limitations related to liability.

12. At this phase the person performing controls must be sure that he/she understands the complexity and / or specific features of processing operations of personal data that will be covered by the control of system of personal data protection.

## 2. Phase 2 - The preparation of the control

13. In order to asses efficient and effective approach, person performing control must decide what kind of activities should be executed in order to provide the necessary evidence for his/her opinion on the control in terms of the established system for personal data protection. Therefore, before starting any activity, the person performing control mandatory prepares Control plan (Appendix no. 2).

14. Control plan is a systematic and structured representation of the activities that should be performed by the person performing control, to assess the design, implementation / existence and / or effectiveness / continuous operation of the system of measures and procedures the controller that is processing personal data has taken to properly protect its data processing.

15. During the process of preparation of the Control plan, person performing control in order to correctly define the activities, must prepare a risk analysis in relation to the requirements for personal data protection derived from:

- Personal data protection regulations
- Generally accepted practices and standards for personal data protection
- Nature of processed personal data and
- The risk for their processing.

During the risk analysis, body performing control determines the level of risk (high, medium and low) where controller belongs, following these criteria:

- The number of collections of personal data
- The number of authorized persons performing processing of personal data
- The number of employees in the controller.

### 3. Phase 3 - Performing the control

16. During performing the control over the system of personal data protection, person performing control may use one or more means, as follows:

- Inquires
- Collecting evidences and other documentation,
- Observation, or
- Use of specialized audit software (Computer assisted audit techniques-CAAT's).

In case of using specialized audit software, in the Engagement letter must be precisely determent audit software that will be used while performing control.

Guidelines for performing control over the system of personal data protection are listed in Annex no. 3.

17. During the control over the system of personal data protection, the person performing the control is obliged to record evidence as part of a complete record of the control. This record may contain:

- Reports of interviews and notes from various activities
- Collected information / documentation,
- Findings, observations and decisions concerning the opinion of the performed control.

18. During the control over the system of personal data protection, person performing control must confirm his findings with the controller’s responsible persons.

### 4. Phase 4 – Formulation of the control opinion - compiling of the Report

19. Based on the collected information, person performing control should assess whether more or less material errors have occurred, that may affect the reliability of the established system of personal data protection.

The person performing control is obliged to explain the compiled opinion on the performed control within the Report of performed control, prescribed in provisions of the article 25 of the Rulebook on technical and organizational measures for providing secrecy and protection of personal data processing ("Official Gazette Republic of Macedonia "no. 38/09 and 158/10).

In the Report of the performed control, person performing control is required to give all information and facts on which he has built his opinion on the control and has proposed measures for removing the identified deficiencies in the system of personal data protection. This approach is allowing the user of the Report to gain insight into how the person who performed the control came to his opinion.

20. The controller is obliged to implement the recommended solutions for removal of the identified defaults of the system of personal data protection and to monitor their implementation through its data protection officer.

21. The Body performing control is obliged to submit the Report from performed control to the Directorate for Personal Data Protection.

## IV.SPECIAL PROVISIONS

22. The provisions of this Manual shall be applied for performing the internal control by the controller in accordance with the provisions of the articles 25 and 35-d of the Rulebook on technical and organizational measures for providing secrecy and protection of personal data processing and the verification of treatment by the processor during the processing of personal data in light of the provisions of the article 26, paragraph 3 of the Law on Personal Data Protection.

23. Appendixes from No. 1 to No. 3 are an integral part of this Manual. Content from Appendix No. 1 to No. 3 represents basis for further elaboration of matter concerning the control of the system of personal data protection by persons performing control.

## V.FINAL PROVISION

24. This Manual entries into force on the date of publication on the website of the Directorate for Personal Data Protection, and will be applicable from 1 June 2012.

Director,

Dimitar Gjeorgievski