

VIDEO SURVEILLANCE

PRIVACY STATEMENT

The Privacy Statement herein shall elaborate the type of personal data which Makedonski Telekom AD – Skopje (hereinafter referred to as: the Controller or MKT) collects from you by means of conducting video surveillance when visiting the official or business premises thereof, as well as the manner in which the Controller uses such data.

1. Why do we collect (process) personal data?

(1) The Controller collects personal data via the video surveillance system due to the following reasons:

- For the purposes of controlling the access to the official facilities thereof (building, entrance, premises) and the business premises – shops, for the purposes of ensuring safety of the facility, as well as safety of the employees, the visitors and the customers;
- In order to prevent, deter and, if necessary, investigate any unauthorized physical access, including unauthorized access to security-related and protected premises, IT infrastructure, operational information and equipment for information access and storage, located in the premises controlled by MKT;
- In order to prevent, detect and investigate any thefts, other illegal acts or harmful actions aimed at the equipment or the assets possessed by the Controller or at the visitors, the employees or the customers located in the official or business premises of MKT;
- For the purposes of preventing and controlling any threats upon the security of the staff working in the premises or the visitors at the Controller's premises (e.g. fire, physical attack, etc.).

(2) The video surveillance system is not being used for any other purposes or as a means for monitoring the work of the employees or controlling their presence.

(3) Video surveillance cameras are installed at the access points to a particular facility (e.g. entrance/exit, hallways, staircases, elevator lobbies, etc.) or premises where technical equipment and communication infrastructure are being kept. If necessary, cameras are also installed for the surveillance of other areas around the facilities across which the property is accessed (e.g. parking lot, garages, unloading access points, warehouse space, etc.). The Controller positions the video surveillance devices in such a manner so that the surrounding public space is not being recorded, except for the space in the immediate vicinity of the official and business premises thereof.

(4) The purpose of the cameras is to provide a general overview of everything that takes place in the areas which are under video surveillance, but, principally, they are not used to detect the identity of natural persons by means of video surveillance. Nevertheless, under conditions when from the video surveillance recordings it is established that a criminal or other type of an act which is illegal or harmful has been committed at the Controller's premises, the data obtained via video surveillance may be used for establishing the identity and the manner of perpetrating such illegal act in the course of a formal disciplinary or criminal investigation and handed over to the competent state authorities within a legally prescribed procedure.

2. What type of data does the Controller collect?

The controller collects only the visual images that are recorded by the video surveillance cameras. The Controller does not make any audio recordings.

3. Who is responsible for the data processing?

MKT, as the Controller, performs the processing of the personal data and it determines the purposes of such processing activity. Said purposes are in accordance with the Law on Personal Data Protection. Your corporate

security specialist from the Corporate Security Unit shall be the person responsible for the video surveillance, as well as the appointed contact person.

4. What is the legal basis for the personal data processing via the video surveillance system?

(1) The Controller uses video surveillance equipment for the purposes of achieving the following objectives which are in accordance with Article 90 of the Law on Personal Data Protection:

- property protection
- protection of human life and health
- provision of control over the entry and exit from the official or business premises for security purposes

(2) In addition, at the entrance of any official facility or business premises – shops, a notice has been placed indicating that video surveillance is being performed, which enables the personal data holders to become acquainted with the basic data pertaining to such video surveillance, the title of the Controller undertaking the video surveillance and the manner in which information may be obtained as to where and for how long the footage is kept in the video surveillance system.

5. Who may view my personal data?

Access to the video footage is only allowed to the persons authorized for video surveillance by the Controller, whereas access to live recordings from the video surveillance is also allowed to the authorized personnel of the commissioned security agency. The access to the digital video recorders and the related technical equipment on which the video footage is kept is restricted and protected by means of applying technical measures aimed at data security (password and log related to each event or action taken by the employees, i.e. the authorized persons). Access to the data, i.e. the video footage, is not permitted without an authorization by MKT.

6. How can you exercise your rights related to your personal data from video surveillance?

(1) As a personal data holder, you are entitled to request to exercise your rights prescribed in the Law on Personal Data Protection in terms of your personal data that were processed by means of video surveillance.

(2) In order to exercise your right, you are required to submit a written request wherein you shall state your name and surname, contact information and an explanation as to the circumstances and all the required information related to your request. MKT shall be entitled to verify your identity and request additional information in order to act upon such request.

(3) You may submit the request to the main archives of MKT, located in Skopje at Kej 13 Noemvri No. 6 Skopje, with the designation – attn. Personal Data Protection Officer – or in an electronic format to the following e-mail address – dpo@telekom.mk

7. Can I access my data?

You are entitled to request access to your data at any time, free of charge, by sending a request to the Controller pursuant to item 6 above.

8. Can I modify my data?

Modification of the video surveillance footage is not allowed.

9. Can I request a restriction of the processing of my personal data?

You are entitled to request a restriction of the processing of your personal data by sending a request to the Controller pursuant to item 6 above in cases when you are contesting the accuracy of your personal data or when the Controller no longer needs the data for the performance of the tasks thereof. You may also block the processing when the operation is illegal and you are opposed to the deletion of the data. Nevertheless, such blocking is impossible in the event of an official investigation.

10. Can I delete my own data?

You are entitled to request the deletion of your data by sending a request to the Controller pursuant to item 6 above when you consider the processing to be illegal.

11. Are my personal data being shared with any other parties?

As a rule, the video surveillance data are kept by the Controller and they are not shared with any third parties, unless requested or allowed by you for us to share them.

In the event of sharing your data with any third parties, at your request, you will be informed to whom your personal data have been disclosed, what was the purpose for it and on which legal grounds it was done.

12. Am I entitled to a complaint?

Yes, you are entitled to a complaint and to contesting the processing at any time by sending a request to the Controller pursuant to item 6 above, provided that you have legitimate reasons relating to your particular situation. The Controller shall respond to your request within 15 days as of the day of the submission of the request.

13. What can I do in the event of a problem?

a) The first step is to notify the Controller by calling the telephone number 02/32 42 908 of the Corporate Security Unit, where you may obtain information as to the video surveillance and request for adequate actions to be taken.

b) If you do not receive an answer or you are dissatisfied with the answer provided, you may contact our Personal Data Protection Officer at dpo@telekom.mk

c) If you consider that the measures taken by the Controller are insufficient, you may file a request to the Personal Data Protection Agency www.azlp.mk

14. When will the processing of your personal data via the video surveillance system commence?

The processing commences at the moment of visiting the Controller's premises.

15. Personal data safety

The Controller is dedicated to protecting your personal data. While conducting the video surveillance, security technologies and procedures are applied by means of which your personal data are protected from any unauthorized access, use or disclosure. Your data are kept on a computer system with restricted access and in a controlled environment.

16. How long do we keep your data?

(1) As a rule, the Controller shall keep your personal data obtained by video surveillance for a period of 30 days, whereupon any recorded video footage shall automatically be deleted.

(2) As an exception, certain video surveillance footage may be kept for a longer period, if a request has been issued by a competent authority to the Controller in a legally stipulated procedure (e.g. conducting an official investigation or identifying the perpetrator of a criminal act), or if the video surveillance footage is required for conducting other procedures pursuant to the law or with a view to pursuing a legitimate interest of the Controller, until the completion of such procedures.

Translated by Lingva Ekspert