Privacy Notice: Video-surveillance (CCTV)

Last update: 21 July 2023

This Privacy Notice provides you with information about the personal data that may be processed through the video-surveillance system installed at the premises of the Commissioner of Communications (the "**Controller**"). This Privacy Notice is intended to help you understand why and how we may use your personal data.

The Data Controller operating the video surveillance system is the **Commissioner of Communications** who according to:

a) article 6 (1) of the Information Systems Security Law (L.89(I)/2020) is the head of the Digital Security Authority· and

b) article 10 (3) of the Electronic Communications and Postal Services Law (L.112(I)/2004) is in charge of the Office of the Commissioner for Regulation of Electronic Communications and Posts (OCECPR).

What personal data is being processed by us?

The personal data that are processed by the video-surveillance system are as follows:

Categories of personal data	Types	Grounds for processing
Data from video-surveillance systems	Images and video clips of all persons entering the Controller's premises at Andrea Chaliou 1, 2408 Nicosia, Cyprus	The Controller's legitimate interest in controlling security and access to its premises pursuant to Article 6 (1) (f) of the Regulation (EU) 2016/679.

For what purposes do we process your data?

The Controller collects data from the CCTV system for the following reasons:

1. To control access to the building and to ensure the security of the building, the safety of the Controller's employees and visitors, as well as property and information located or stored on the premises;

2. To prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information;

3. To prevent, and possibly assist in the detection and investigation of theft of equipment or assets owned by the Controller, visitors or employees or threats to the safety of personnel working at the office (e.g. fire, physical assault).

The CCTV system is not used for any other purpose other than the purposes specified above, such as to monitor the work of employees or their attendance. The location and positioning of the video-cameras are such that they are not intended to cover the surrounding public space.

The CCTV system is not used as an investigative tool or to obtain evidence in internal investigations or disciplinary procedures unless a security incident is involved. The CCTV cameras are installed at the entrances placed and focused in a way that only people who want to access the site or the annexed facilities including parking areas property are recorded.

The CCTV system covers the area of entry and exit points of the building including emergency exits, entry points inside the building, elevators, staircases, secure premises and protected rooms, parking and outer area of the building.

How long do we keep your personal data?

Personal data collected by the CCTV system are stored for a period of 150 days. After the expiry of that period, the personal data are deleted automatically.

Who can see my data?

The images can be accessed by a limited number of employees of the Controller who have access on "a need to know basis". Access to the hard-disc recorder is highly limited, being protected by a password and recording any log or action from the employees of the Controller.

Can we share your personal information with third parties?

We respect and maintain the confidentiality of your personal information. The Controller will not disclose your personal information obtained through the video-surveillance systems to third parties, unless national law or European regulation requires such disclosure. In such a case, the Controller may disclose your personal data to the competent authorities authorized by applicable law.

Your rights regarding your personal data

Pursuant to the provisions of Regulation (EU) 2016/679 ("GDPR"), you have the following rights to your personal data processed by the Controller:

1. Right of access: access your personal data that the Controller processes and obtain a copy thereof;

2. Right of rectification: in case of incompleteness or inaccuracy in the data that the Controller processes, your personal data will be corrected;

3. Right of erasure: request that your data be deleted when the conditions are met. Such cases are if the purpose for which the data is collected is achieved, there is no other legal basis for processing, your data is being processed unlawfully and others;

4. Right to restriction of processing: in the cases specified by the GDPR, you may require limitation of the processing of your personal data;

5. Right to object: in the cases specified by the GDPR, you may object to the processing of your personal data;

6. Right to data portability: exercise your data portability rights and request that your data be provided in a structured, widely used and machine-readable format;

7. Withdraw your consent when processing your personal data is based on consent.

8. You also have the right to file a complaint with the Commission for Personal Data Protection when the relevant prerequisites are in place (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/2FBD2ACD407DEFE8C22582B9002E7019).

How to contact us

For any questions, you may have concerning the protection of your personal data, or to submit a complaint or to exercise your legal rights you may contact us at:

Data Protection Officer:

Andrea Chaliou 1, 2408 Nicosia, Cyprus

Tel.: 22693000

Email: contact@dsa.ee.cy

Data Protection Officer

Tel.: 22693000

Email: dpo@ee.cy