Renor

26.8.2024

PRIVACY POLICY FOR CAMERA SURVEILLANCE AND ACCESS CONTROL

The purpose of this Privacy Policy is to inform the users of the properties owned by Renor Oy about the camera surveillance and access control on the property.

We take seriously our compliance with the EU General Data Protection Regulation as well as other applicable personal data processing legislation when processing personal data. We also ensure that processing is secure and that our data protection practices allow for the full exercise of data subjects' rights.

Should there be any changes to the data processing policies of Renor Oy or to relevant legislation, this privacy policy may be updated. For our privacy policy valid at each time, please visit our website at www.renor.fi.

CONTROLLER

Renor Oy (business ID 2343526-9)

Any communication related to data protection should be addressed to Renor Oy / Data Protection, Askonkatu 9 B, 15100 Lahti, Finland or by e-mail to legal@renor.fi with the header ”Matters concerning data protection”.

NAME OF DATA FILE

Camera surveillance and access control data file (“Kamera- ja kulunvalvonnan rekisteri”)

THE PURPOSE OF THE PROCESSING OF PERSONAL DATA, THE DATA PROCESSED AND THE LEGAL BASIS AND SOURCE OF THE DATA

The purpose of camera surveillance and access control is to protect the controller’s, employees, tenants and other users of the controller’s property, prevent vandalism and crime, provide assistance in the investigation of any criminal activity and increase safety.

We process video and image data of people moving around the CCTV area. The date and time of the events are also recorded in the footage. Camera surveillance is carried out in the corridors and public areas of the property (in and outside the building). The crime detection system for properties is part of the camera surveillance system. As a general rule, those being filmed are informed by "recording camera surveillance" signs or stickers displayed at the filming locations.

The purpose of access control is to manage the personal access rights and keys of the users of the controller’s property. Users' first and last name, company, e-mail address, telephone number, access event with dates and times (including log data) are stored. The contents of the data file are used to investigate and identify the access-related activities of individuals.

The processing of personal data is based on the controller’s legitimate interest.

DATA DISCLOSURE

As a rule, the controller will not disclose the contents of the data file to outsiders. The personal data will be disclosed to the police or other competent authorities, for example to solve crimes. The disclosure is always based on a specific request from the authorities.

In processing the personal data referred to in this document, the controller may use external processors that are assigned by the controller to process the data on behalf of the controller and in accordance with the controller's instructions on the basis of a data processing agreement.

We have outsourced our camera and access control management partly to an external service provider.

The data will not be processed or transferred outside the European Union or the European Economic Area.

A GENERAL DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL MEASURES

The data is collected in files protected by firewalls, passwords and other technical means. The physical databases are located in locked and controlled premises.

Personal data may be stored in a service provided by a third party selected by the controller if said service is considered secure and in compliance with generally accepted data protection policies. The controller and the third party in question shall ensure the confidentiality and security of the personal data and its processing.

Only the employees of the controller and such persons of the service provider authorised due to their work and/or duties to process the data in this data file may access the system containing the personal data.

RETENTION PERIOD OF PERSONAL DATA

The retention period of the camera surveillance recordings varies depending on the technical solution in each property but will not exceed three (3) months from the date of creating the image, unless a longer time is required for investigating damage or criminal offences.

The retention period of the access control data also varies depending on the technical solution in each property. As a rule, access control data is deleted immediately after the person has no longer had a need for personal access. In any case access control data is deleted in two (2) years after the person has returned the (access) keys.

We regularly assess the necessity of data retention in the light of applicable law. In addition, we will take reasonable steps to ensure that no personal data relating to data subjects is kept that is incompatible, outdated or inaccurate for the purposes of the processing. We will correct or destroy such data without undue delay.

Personal data may be kept for longer than the above-mentioned retention periods if there is a specific reason to do so, such as in connection with suspected criminal offences and the related investigation.

RIGHTS OF THE DATA SUBJECT

In accordance with the applicable data protection legislation and under the stipulated preconditions, the data subject has the right to:

Right	In which situations
Access the information stored about yourself	Always
Request the correction of incorrect or outdated data	Always
Request the erasure of data	Where one of the grounds set out in Article 17 of the GDPR is met.
Object to the processing of data	Where the processing is based on a legitimate interest and involves a particular personal situation

Request restriction of processing (e.g. until requests for data are resolved and settled)	If the accuracy of the data is contested or one of the other grounds set out in Article 18 of the GDPR is met.
File a complaint about the processing of your personal data with the Data Protection Ombudsman	Always

Any requests related to exercising the rights of the data subject should be sent to the address mentioned above under the section Controller.

If necessary, the controller may ask the data subject to specify their request in writing and verify the data subject's identity before processing the request. The controller may also refuse the request on grounds stipulated in data protection legislation. We will respond to requests and enquiries from the data subject concerning the exercise of data subjects' rights within one month.