Renor

16 August 2019

PRIVACY POLICY

This is a combined privacy policy, in accordance with valid data protection legislation, and an informative document for the users of property owned by Renor Oy and our subsidiaries.

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/en.

CONTROLLER

Renor Oy (business ID 2343526-9)
Kiinteistö Oy Lahden Askotalot (business ID 2877517-4)
Kiinteistö Oy Lahden Liesitehdas (business ID 2604806-1)
Kiinteistö Oy Lahden Teollisuuskeskus (business ID 0719369-3) Kiinteistö Oy Tikkurilan Silkki (business ID 2877518-2)
Each as a respective controller

Any communication related to data protection should be addressed to Renor Oy / Tietosuoja-asiat, Askonkatu 9 E, FI-15100 Lahti, Finland or sent via e-mail to legal@renor.fi with the header *"Tietosuoja-asiat"* ('Matters concerning data protection').

NAME OF DATA FILE

Kamera- ja kulunvalvonnan rekisteri ('Video surveillance and access control data file')

PURPOSE OF, AND GROUNDS FOR, PROCESSING PERSONAL DATA

The purpose of video surveillance and access control is to protect the possessions of 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.

The individuals subject to video surveillance are primarily informed with signs or stickers reading *"Tallentava kameravalvonta"* ('Recording video surveillance') placed in the monitored locations.

The purpose of access control is to manage the access rights and keys of the users of the controller's property. 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 TO BE PROCESSED

The access rights of the users of the property are specified individually. The information stored in the data file consists of the individuals' first and last name, employer, e-mail address and telephone number.

The access control system also forms a data file based on the use of the ID. The access control data file records any access-related activities and their dates and times.

The burglar alarm systems of the properties form a video-format record data file by using surveillance cameras.

DATA SOURCES

The data subject provides the data when communicating in writing and when registering with access control and/or accessing various locations in the property area.

DISCLOSURE OF DATA

As a rule, the controller will not disclose the contents of the data file to outsiders. However, the controller may disclose personal data to authorities or other parties as allowed and obligated by legislation. Data is disclosed to the police or other competent authority to, for example, investigate

criminal activity. 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 and, for this purpose, disclose data to its cooperation partners that are assigned by the controller to process the data on behalf of the controller and in accordance with the controller's instructions. The controller always ensures the appropriate processing of personal data and makes certain that the processors have implemented the appropriate technological and organisational measures to enable confidential processing of the data and a sufficient level of data security. There is a valid personal data processing agreement between the controller and the external processor.

The data will not be processed or transferred outside the European Union or the European Economic Area unless required by the technical implementation of the processing.

PROCESSING OF DATA

The personal data of the data subjects will not be processed for purposes other than those for which the personal data was originally collected. In addition, the controller aims to ensure that no personal data that is unnecessary, expired or inaccurate, having regard to the purposes for which it is processed, is stored.

The personal data is stored for as long as is necessary for the purpose of processing the personal data. Primarily, the data is stored for six (6) months after the termination of the employment or contractual relationship, unless otherwise allowed or required by legislation. The recordings of the video surveillance system are primarily stored for 2–3 weeks.

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 data security of the personal data and its processing.

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

The data is collected into databases protected by firewalls, passwords and other technical means. The physical locations of the databases are locked and monitored.

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:

- be informed of the processing of their personal data
- access their personal data stored in the data file
- request rectification of inaccurate personal data
- request restriction of processing or the erasure of their personal data
- object to processing of their personal data
- refuse the use of their personal data for direct marketing

Any requests related to exercising the rights of the data subject should be sent, in writing and signed, to:

Renor Oy,
Askonkatu 9 E
FI-15100 Lahti, Finland

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.

The data subject has the right to lodge a complaint with a competent data protection supervisory authority regarding the controller's processing of personal data.