Camera surveillance register

Privacy policy

Registrar

Riihimäen kotikulma Oy (0592797-2)

Hämeenkatu 20

11100 Riihimäki

Contact person for matters concerning the register

Sanna Eskelinen

sanna.eskelinen@riihimaki.fi

Registrar

Camera surveillance register

Date of preparation

2025-04-29

Legal basis for processing

Legitimate interest

Purpose of processing personal data

The legal basis is the legitimate interest of the register holder.

The data is processed if necessary, in connection with the investigation of possible security incidents at the register holder's premises and in criminal cases by the authorities if necessary.

The purpose of camera surveillance is to protect property, prevent crimes and assist in the investigation of crimes that have already occurred. In addition, the purpose of surveillance is to ensure and increase the safety of the register holder's personnel and visitors.

Persons specified by the controller are entitled to process personal data obtained from camera surveillance (e.g. viewing and listening to recordings) based on their job duties or position, as well as administrative service personnel and individual persons who may investigate the matter.

In addition, the employer also has the right to use the information in the register in the situations specified in Section 17, subsection 2, paragraphs 1-3 of the Act on the Protection of Privacy in Working Life (759/2004) to prove grounds for termination of employment, to investigate and prove harassment or bullying as referred to in the Act on Equality between Women and Men (609/1986) or harassment and inappropriate conduct as referred to in the Occupational Safety Act (738/2002), and to investigate an occupational accident or other situation that caused a danger or threat as referred to in the Occupational Safety Act.

Legitimate interest ground

The legal basis for processing personal data is the legitimate interest of the controller (Article 6.1(f) of the EU General Data Protection Regulation “GDPR”). The controller must process personal data in order to perform business-related tasks. In this context, the processing of personal data cannot necessarily be justified by a legal obligation or a contract with an individual.

In the balancing test, the controller has determined that legitimate interest is the most appropriate processing ground for the nature, scope and protection of the rights and freedoms of the data subjects.

The controller has assessed that the legitimate interest does not result in a serious harm to the rights and freedoms of the individuals concerned (data subjects).

Personal data groups in question

The register contains the following personal data in the form of images of all persons moving within the camera surveillance area of the controller's property:

1) The person's appearance and identifying marks

2) The time and exact location of movement within the property

The register stores information whenever a person moves within the camera surveillance area, as the camera surveillance works with motion detection. Recording camera surveillance is indicated by markings. The cameras are placed at the entrances, public areas, walkways and courtyards of the property owned/managed by the controller, as well as at certain locations that are particularly vulnerable due to operational reasons due to a special need for surveillance.

Recipients and recipient groups

The controller's own personnel. The data is not routinely disclosed to anyone without a legal basis (Act on the Protection of Privacy in Working Life 759/2004). Data is only disclosed to the police in special situations through the crime reporting procedure in cases where a crime has occurred or is suspected to have occurred, or to the insurance company if necessary in cases of damage.

Data may also be disclosed to persons in a supervisory position in the controller's organization in order to investigate and prove an occupational accident, harassment, bullying or other inappropriate behavior.

Data content of the register

The register contains the following personal data in the form of images of all persons moving within the camera surveillance area of the controller's property:

1) The person's appearance and identifying marks

2) The time and place of movement within the property

Information is stored in the register whenever a person moves within the camera surveillance area, as camera surveillance works with motion detection. Recording camera surveillance is indicated by signs. The cameras are placed at the entrances, public areas, walkways and courtyards of the property owned/managed by the controller, and due to a special need for surveillance, at certain locations that are particularly vulnerable for operational reasons.

Biometric identification: is it in use? If so, please state it here

Instruction:

In addition, it should be noted that if the photographed persons are analyzed using special technical methods, this may result in the recordings being converted into biometric data. Biometric data is sensitive data under the Data Protection Regulation, the processing of which generally requires anonymization.

Regular data sources

Regular data sources are surveillance cameras, from which the register data is collected from the areas they capture, which are the image material transmitted by the cameras belonging to the recording surveillance system.

Retention period of personal data

The data collected in the register are only stored for as long and to the extent as is necessary in relation to the original or compatible purposes for which the personal data were collected. The personal data are stored on the server of the camera surveillance contract partner. The data is deleted when there is no longer a need for processing, for example for legal proceedings or the like.

After this, the data is deleted. If a report of damage or other crime is received during the storage period, the recording is stored for the time necessary to investigate the crime. The controller deletes the stored personal data when there is no longer a legal basis for their processing. The controller regularly assesses the necessity of storing the data in accordance with its internal code of conduct.

Regular data transfers

Data is not transferred outside the controller or the processor of personal data in a contractual relationship with it, except in criminal cases.

Data transfer outside the EU or EEA

Data in the register is not regularly transferred outside the EU or EEA. However, it is possible that service providers outside the EU/EEA are used in the processing or that the service providers' clouds are located outside the EU/EEA, in which case the SCC standard clauses are used as the basis for data transfer and additional safeguards have been implemented in

data transfers, such as internal instructions (on pseudonymisation of personal data and the like) and possibly a TIA analysis if the situation requires it.

When an organisation processing personal data has committed to the EU-US Data Protection Framework (DPF), the transfer basis is used for the duration of its validity.

Principles of register protection A: Manual data

Manual data is not stored anywhere.

Principles of Register Protection B: Electronic Material

Personal data is kept confidential. The data is collected in databases located on a secure server. The databases are protected by passwords and other technical means. The user names and passwords required to use the register are only granted to persons authorized to use the register.

Right of inspection, i.e. the right to access personal data

The data subject has the right to check what information about him or her is in the register. The inspection request must be made from an identifiable email address to the contact point of the data controller.

Right to transfer data from one system to another

The data subject does not have the right to transfer his or her own data from one system to another.

Right to demand correction of data

Personal data in the register that is incorrect, unnecessary, incomplete or outdated in terms of the purpose of the processing must be corrected, deleted or supplemented.

The request for correction must be made from an identifiable email address to the controller's contact point.

The request must specify what information is requested to be corrected and on what basis. The correction will be carried out without delay, if technically possible.

The person from whom the incorrect information was received or to whom the information was disclosed will be notified of the correction of the error. If the request for correction is denied, the person responsible for the register will issue a written certificate stating the reasons for the denial of the request for correction. The person concerned may refer the denial to the Data Protection Ombudsman for resolution.

Right to restriction

The data subject has the right to request the restriction of data processing, e.g. if the personal data in the register are incorrect. Contacts must be made from an identifiable email address to the controller's contact point.

Right to object

The data subject has the right to request personal data concerning him or her and the data subject has the right to request the correction or deletion of personal data. Requests must be made from an identifiable email address to the controller's contact point.

Right to lodge a complaint with a supervisory authority

If you consider that the processing of personal data concerning you has infringed the General Data Protection Regulation, you have the right to lodge a complaint with a supervisory authority.

You can also lodge a complaint in the Member State where you have your habitual residence or place of work.

The contact details of the national supervisory authority are:

Office of the Data Protection Commissioner

Visual address: Lintulahdenkuja 4, 00530 Helsinki

Postal address: P.O. Box 800, 00531 Helsinki

Telephone switchboard: 029 566 6700

Library: 029 566 6768

tietosuoja@om.fi

www.tietosuoja.fi

Other rights related to the processing of personal data

The data subject has the right to prohibit the disclosure and processing of his or her data for direct advertising and other marketing purposes, to demand the anonymization of the data where applicable, and the right to be completely forgotten.