Camera surveillance register - privacy policy

Creation date	07.07.2021
Data controller	
Contact person in matters related to the filing system	
Name of filing system	Camera surveillance register
Purpose of personal data processing	Legal bases of processing data: the legitimate interest of the data controller. Data is processed as required to investigate possible security anomalies at the premises of the data controller and, in the case of criminal cases, by the necessary authorities. The purpose of processing has to do with general safety, such as the investigation and prevention of criminal activity, vandalism, and other types of misconduct on premises owned or monitored by the data controller. The individuals defined by the controller are legitimate on the basis of their duties or position on the processing of personal data on camera surveillance (eg recordings for viewing and listening to records), as well as administrative services personell, and possibly individual persons related to solving current matter. In addition, the employer also has the right to use the registry for the protection of privacy in accordance with Article 17 § 2 of Section 1-3 of the Law on Privacy (759/2004) to conclude the establishment of an employment relationship to the establishment of an employment relationship, disruption or harassment of harassment or harassment in the Act on Equality between Women and Men (609/1986) in order to identify and demonstrate the harassment and inappropriate behavior referred to in the Occupational Safety Authority (738/2002), as well as to identify the risk or threat of occupational safety or other occupational safety.
Legitimate interest basis	The data controller’s legitimate interest for processing collected and used personal data is based on the Data Controller's and it's employee's security needs and the freedom to engage in commercial activity.
Categories of personal data in question	The register contains the following personal data of the following image material from any of the persons moving in the domain of the data controllers property in the domain of the data controllers property: 1) The appearance of a person and the characteristics of the person 2) Exact time and location of movement on property or in the area of surveillance. The register saves information always when a person is moving in the camera monitoring area as camera control works with motion detection. The recording camera control is indicated by labeling. The cameras are placed in the entrances, general premises, paths and yard areas owned / managed by the controller owned / managed by the controller, and for particular control need for certain functional reasons due to particularly vulnerable objects.
Recipients and recipient groups	The controller's own personnel. Information is not regularly disclosed anywhere without a legitimate criterion (the law on the protection of privacy in working life 759/2004). Information is transferred to the police only in special situations through the criminal reporting procedure in cases where there has been or suspected of an offense or in case of damage if necessary

	for the insurance company. Information may also be disclosed to identify and recover the accident at work, harassment or other inappropriate behavior to the supervisor's leadership of the controller's organization.
Concent	
Data content of filing system	The register contains the following personal data of the following image material from any of the persons moving in the domain of the data controllers property in the domain of the data controllers property: 1) The appearance of a person and the characteristics of the person 2) Exact time and location of movement on property or in the area of surveillance. The register saves information always when a person is moving in the camera monitoring area as camera control works with motion detection. The recording camera control is indicated by labeling. The cameras are placed in the entrances, general premises, paths and yard areas owned / managed by the controller owned / managed by the controller, and for particular control need for certain functional reasons due to particularly vulnerable objects. Biometric Detection: If your company is using it, please express it here Guide: In addition, it should be noted that if the individuals described are analyzed by specific technical methods, it may make recordings of biometric data. Biometric data is subject to sensitive information under the Data Protection Regulation, whose processing requires a particularly express consent. Biometric data means personal data obtained by a person with physical and physiological properties or behaviors, such as face images or fingerprint data on the basis of which the natural person concerned can be identified or the identification of that person can be ensured. Before the introduction of video analysis should be evaluated whether the analytics generates information that could be classified as biometric information.
Regular data sources	As a regular source of information, there are surveillance cameras whose registers describe the registry information, which are the image material transmitted by the cameras of the recording control system.
Storage time	Data collected from surveillance cameras is stored for a period deemed necessary if they contain data relevant for on-going investigations. After the investigation has been completed, the data are stored for as long as is necessary for conducting relevant legal procedures. After this the data will be removed. If the retention period becomes a notification of damage or any other offense, the recording is kept in this respect for the period required to determine the crime. The data controller removes the stored personal information when there is no longer any legal basis for their handling. The data controller will regularly evaluate the need for retention of data regularly in accordance with its internal code of conduct
Regular disclosure of data	Data in the filing system will not be disclosed to third parties unless disclosure is required for upholding security. If criminal activity is suspected, data may be disclosed to the police.
Transferring data outside the EU or the EEA	Personal data will not be transferred outside the European Union unless necessary for ensuring the technical implementation of the company’s or its partners’ activities.
Filing system’s principles of protection A: Manual material	Manually processed data are stored in premises that can only be accessed by authorised persons.

	Only identifiable individuals employed by the data controller or companies acting on behalf of or under commission by the data controller who have signed confidentiality agreements have access to data stored in the filing system by means of unique access permissions.
Filing system's principles of protection B: Electronically processed functions	Electronically processed data contained within the filing system are protected with firewalls, passwords and other necessary data security measures in accordance with current methods in the field. Only identifiable individuals employed by the data controller or companies acting on behalf of or under commission by the data controller who have signed confidentiality agreements have access to data stored in the filing system by means of unique access permissions.
Rights of the data subject	According to the General Data Protection Regulation (GDPR), data subjects have the right to obtain information on the processing of their personal data of access to their data to rectification of their data to the erasure of their data and to be forgotten to restrict the processing of their data to data portability to object to the processing of their data not to be subject to a decision based solely on automated processing.
Cookies	
Information source	
Automatic processing and profiling	The results of data processing are not used for profiling or other related purposes.
Right of access	The data subject has the right to inspect what information about them has been stored in the filing system. The request for data access should be sent to the responsible person of the register. The request must be made in writing and it must be signed by the data subject. A request for data access can also be made in person at the data controller's place of business. In order to gain access to the data, the data subject should provide information on the place and time of when the recording would have taken place as accurately as possible. The data subject should attach a photo of themselves with the request for data access.
Right to lodge	If you consider that an infringement of the General Data Protection Regulation has occurred in the processing of your personal data, you have the right to lodge a complaint with a supervisory authority. The complaint can also be lodged in a member state where you are a permanent resident or where you are employed. Contact information for the Finnish national supervisory authority: Office of the Data Protection Ombudsman PL 800, Lintulahdenkuja 4, 00530 Helsinki tel. +358 29 566 6700 tietosuoja@om.fi www.tietosuoja.fi/en/
Right of portability	The data subject has the right to transfer their personal data from one system to another. Request of transfer can be sent to the contact person of the filing system.
Right to rectification	Taking into account the purposes of processing, any data stored in the filing system that is inaccurate, unnecessary, incomplete, or outdated must be erased or rectified.

	The written and signed request for rectification should be sent to the company’s customer service or the personal data filing system’s administrator. The request should specify what information should be rectified and on what grounds. Rectification shall be carried out without delay. Notification of rectification will be sent to the party who provided the inaccurate data or to whom the data were disclosed. If a request for rectification is denied, the responsible person of the filing system will provide a written document stating the grounds for the denial of the request for rectification. The data subject concerned may then pass the matter alongto the Data Protection Ombudsman.
Other rights related to the processing of personal data	Right to restrict processing The data subject has the right to request that the processing of their personal data is restricted for example if data stored in the filing system is erroneous. Requests should be sent to the responsible person of the filing system. Right to object The data subject has the right to request for personal data pertaining to them, and the data subject has the right to request for the rectification or erasure of said data. Request can be sent to the contact person of the filing system. If you are acting as the contact person of a company or organisation, your data cannot be erased during this time. The data subject has the right to prohibit the disclosure of processing of personal data for the purposes of direct marketing or other marketing, the right to demand the anonymization of data where applicable, as well as the right to be completely forgotten.