

Privacy Notice for Access Control and CCTV Surveillance Register

This Privacy Notice has been prepared by Ab Stormossen Oy in accordance with the EU General Data Protection Regulation (2016/679), outlining the processing of personal data and the rights of the data subject.

1. Register Name

Ab Stormossen Oy's Access Control and CCTV Surveillance Register

2. Data Controller

Ab Stormossen Oy, business ID 0586634-8

Stormossenintie 56, 66530 Koivulahti, FINLAND

Tel. 010 320 7600

E-mail: info@stormossen.fi

3. Contact Person for Register Matters

Kristiina Kuosma, Operating Manager

Tel. 010 320 7661

E-mail: kristiina.kuosma@stormossen.fi

4. Purpose and Legal Basis for Processing Personal Data

The purpose of **CCTV surveillance** is to protect property, prevent crimes, and assist in the investigation of crimes that have already occurred.

The purpose of the CCTV surveillance register is to ensure and increase the safety of staff and customers. Register data is used for the investigation of criminal and damage incidents, identification of individuals in the premises if necessary, verification of waste batch reception information, and monitoring compliance with environmental permits.

- Access control
- Ensuring personal safety
- Preventing situations that endanger security
- Investigating situations that have posed a threat to general security
- Investigating work accidents or situations that have posed a threat to work safety
- Protecting property
- Preventing misconduct
- Investigating misconduct
- Ensuring the rights and interests of employees
- Verifying waste batch reception information and monitoring compliance with the environmental permit as per the Privacy Notice.

The purpose of **access control** is to prevent unauthorized access at Stormossen or the premises of other entities using the same gates. The access control register is used to check the access rights to the premises.

- Access control/tags
- Key registers
- Access rights (gates)
- Other access rights granted by Stormossen
- Visitor lists, contractor lists

5. Register Content

The image material captured by the cameras within the surveillance system at Stormossen's premises, including the recording time and location. No audio is recorded.

- the register also includes reports prepared based on the material, if necessary;
- information may be combined with other access control or security-related register data (e.g. electronic door openings with access rights) if necessary, such as in investigations of suspected crimes.

The access control registers may contain information about individuals or businesses/partner entities:

- name
- address
- phone number
- e-mail
- profession
- vehicle registration
- general contact details of the business/partner entity, business ID
- timing movements in the area

6. Regular Sources of Information

- The image material transmitted by cameras within the recording surveillance system.
- Access control collects information on the movements of employees and other authorized individuals at Stormossen's premises.
- The gate register collects information on individuals and businesses authorized for access.
- The key register collects information on individuals who have received keys from Stormossen.
- Necessary information is collected on individuals who have been granted access rights.

7. Recipients of Information

No routine disclosure.

Register data is not disclosed to anyone other than the police or another competent authority who, for a legally specified purpose, requests specified information from the register. Information can be shared and processed between Stormossen's own premises and other entities using the gate in the area as necessary.

Stormossen may use subcontractors to implement the CCTV surveillance. These may process personal data only for tasks related to managing or maintaining the customer relationship on behalf of Stormossen. Stormossen always ensures that partners and subcontractors do not process the transferred personal data for any other purposes.

8. Transfer of Data Outside the EU or EEA

No routine disclosure.

9. Retention Period of Personal Data

Data collected in the register is retained only as long as and to the extent necessary in relation to the original or compatible purposes for which the personal data was collected. The personal data described in this Privacy Notice is kept for as long as the data controller utilizes the data for the purposes described in Section 4.

The data in the register is stored for a maximum of three (3) months depending on the storage capacity of the recording device, unless there is a specific reason related to the purpose of the CCTV surveillance to retain the data for a longer period. Data is deleted by overwriting or recording new data over it. Access to the data is by browsing the data on a computer.

10. Principles of Register Protection

The information security of the register and the confidentiality, integrity, and availability of personal data are ensured with appropriate technical and organizational measures.

Only individuals with authorized access can view the recordings and other register data.

11. Right of Access and Rectification

The data subject has the right to inspect what personal data about them is stored in the register. Access or rectification requests can be made by submitting a written request to the person responsible for register matters.

12. Right to Erasure

The data subject has the right to have their personal data erased without undue delay, provided that:

- the personal data is no longer needed for the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
- the personal data has been unlawfully processed; or
- the personal data must be erased to comply with a legal obligation in Union or national law.

13. Right to Restriction of Processing

The data subject has the right to obtain from the data controller restriction of processing if:

- the accuracy of the personal data is contested by the data subject;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the data controller no longer needs the personal data for the processing purposes, but the data subject requires them for the establishment, exercise, or defense of legal claims.

14. Right to Withdraw Consent

The data subject has the right to withdraw their consent for processing at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

15. Right to Data Portability

The data subject has the right to receive their personal data, which they have provided to the data controller, in a structured, commonly used, and machine-readable format, and have the right to transmit those data to another data controller.

16. Right to Lodge a Complaint with a Supervisory Authority

The data subject has the right to lodge a complaint with a supervisory authority if they consider that the processing of personal data relating to them infringes the applicable data protection regulations.