



Camera surveillance register

1. Data controller

Northern Finland Student Housing (business ID: 0210156-9)
Mannenkatu 6 A
90130 Oulu
Tel. +358 (0)8 3173 110

2. Data processor

Eerik Junnikkala
Mannenkatu 6 A
90130 Oulu
Tel. +358 (0)8 3173 110
tietosuoja@psoas.fi

3. Name of the register

Camera surveillance register

4. Purpose and legal basis for the use of personal data

Personal data is being processed on the grounds of legitimate interest to investigate any crime and vandalism or other misconducts occurring at premises owned by the data controller.

5. Data content of the register

Video images of persons, vehicles etc. at the sites. Video surveillance is used around the clock and video is recorded on a hard drive located on own server. Sound or speech is not recorded.

6. Regular data sources

Video cameras. Stickers and signs are used to inform tenants of video surveillance.

7. Regular release of data

As a rule, no data is released outside PSOAS. In cases of suspected crime, data can be released to the police.

8. Data transfer outside the EU or the European Economic Area



No data is transferred outside the area of European Union member states or outside the European Economic Area.

9. Right to access, restriction and rectification

The data subject has the right, in accordance with the Personal Data Act, to inspect which data concerning them has been recorded in the register.

The data subject can exercise their rights by an access request submitted in person or in writing. Written requests to implement rights are to be sent to customer service by email: asuntotoimisto@psoas.fi. To locate the data, the data subject shall notify the place and time of filming as accurately as possible. The subject shall attach their photo in the data access request. The data subject has the right to file a complaint to the supervisory authority if they believe that their personal data are being processed in violation of the EU General Data Protection Regulation or national legislation and regulations on data protection.

10. Data protection principles

Any electronically processed data in the register are protected with firewalls, passwords and other necessary technical means generally accepted within the data security field at the time. Any manually maintained data are located in spaces with restricted access for outsiders.

Any data in the register is only accessible by designated employees of the data controller and companies working for and on behalf of the data controller, who have signed a confidentiality agreement, with an individual access right granted by the data controller.

The data retention period is 1 month.