Aalto University

Privacy notice, digital camera surveillance

This privacy notice provides the data subject with the information required under articles 13 and 14 of the EU General Data Protection Regulation (hereinafter GDPR).

Name of personal data file:	Aalto University digital camera surveillance
Date:	12 June 2018
Controller **Unit responsible** **Person responsible**	Aalto University Foundation sr (registered foundation) 2228357-4 P.O. Box 11000, FI-00076 AALTO Otakaari 1, 02150 Espoo Tel.: (exchange) 09 47 001 Aalto University Security and Lobby Services Head of Security and Risk Management Seija Piiponniemi-Lahti, seija.piiponniemi-lahti(at)aalto.fi
Short description of the personal data file	Aalto University digital camera surveillance Notice of the camera surveillance is posted in Finnish, Swedish and English at the entrances to the monitored spaces. The notices indicate that the sites are under recorded video surveillance. At Aalto University, information on the data subject is processed in compliance with the requirements of the Act on the Openness of Government Activities (621/1999) and regulations concerning data protection (the GDPR and national legislation). The register contents are not public information.
A: Is the personal data collected directly from the data subject?	No.
B: Is the personal data collected from another source than the data subject?	Yes.

	Visual material on the individual is transmitted by cameras belonging to the university's recording surveillance system.

1. Controller contact person and his/her contact details

Head of Security and Risk Management Seija Piiponniemi-Lahti,
seija.piiponniemi-lahti(at)aalto.fi

System administrator: Pasi Lehto,
firstname.lastname(at)aalto.fi

2. Data protection officer and contact details

Jari Söderström, Senior Legal Counsel,
tietosuojavastaava@aalto.fi

3. Purpose of the personal data file and legal bases for processing the data

Surveillance cameras are located in the university's:

- IT classroom and instrument spaces
- Lobby spaces
- Entrances to buildings
  Immediate vicinity of buildings.

The purpose of the cameras is to prevent and determine the cost liabilities of vandalism and crimes directed at property located in university classrooms, instrument rooms and general spaces. A purpose of surveillance is also to monitor the security of university spaces, to maintain order, and to ensure and enhance the security of staff and students as well as guests and other persons working in Aalto spaces.

The university as employer has the right to utilise the personal data file in individually specific cases for: substantiating the grounds for termination of an employment relationship as referred to in section 17, subsection 2 paragraphs 1–3 of the Act on the Protection of Privacy in Working Life (759/2004); investigating and substantiating harassment or molestation as referred to in the Act on Equality Between Women and Men (609/1986) or harassment and inappropriate behaviour as referred to in the Occupational Safety and Health Act (738/2002); or investigating an occupational accident or other situation causing a danger or threat referred to in the Occupational Safety and Health Act.

Legal bases for processing the personal data:

- Employees: Compliance with statutory obligations (Occupational safety)
- Students: Compliance with statutory obligations. Under the Universities Act (558/2009) students are entitled to a safe study environment.
- Other persons: Compliance with statutory obligations.

4. Categories of personal data

GDPR category of the personal data for processing that is contained in the personal data file:

Basic information consisting of timestamped video recordings of persons moving in the area monitored by the camera.

5. Groups or individuals receiving the personal data

Live images: Live images may be viewed only by those employees of Aalto University and those of partners who provide security services to Aalto whose job descriptions include security monitory of the properties, and by system administrators for the purpose of installation and maintenance.

Viewing of recordings: Access to the recordings is confined to the system administrator, the deputy system administrator and any security service employees agreed upon separately.
Other individuals may be shown a recording as designated on a case-by-case basis by the person responsible for the data file.

Data may be released to the law enforcement authorities (police) to the extent regarded as necessary if the data relates to or is suspected of relating to a committed crime or act of vandalism.

6. Planned transfers of personal data to third countries or international organisations

The data will be transferred neither to international organisations nor to parties outside of EU or EEA borders.

7. Personal data retention times and the criteria determining them

The video recordings are retained for thirty (30) days from the date of the recording. After the 30 days, the recordings are deleted automatically. If an act of vandalism or other

crime is reported to have occurred during the retention period, the relevant part of the recording will be retained as long as necessary for investigation of the incident.

If the surveillance data relates or is suspected of relating to a committed crime or act of vandalism, the data will be retained as long as necessary for investigation of the incident.

8. The right of data subjects to access their own data, to rectify or erase it, or to transfer it from one system to another

The right to inspect data usually does not apply to video recordings. Data subjects may, however, have a limited right to access data on themselves if the access does not jeopardise the confidentiality of the security arrangements or the privacy of other persons. The right also depends on the data subject providing additional information so that he or she may be unambiguously identified from the recordings.

Requests concerning these rights must be sent by email to the individual responsible for the personal data file.

The data subject does not have the right to transfer data from one system to another, as such processing is not based on consent or on a contract.

9. Right of data subject to oppose or request a restriction of the data processing

The data subject may in certain circumstances have the right to request a restriction of the data processing.

The data subject does not have the right to oppose the processing, as the personal data processing is not based on fulfilling a legitimate interest of the controller or of a third party, nor is it based in the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller.

10. The right of the data subject to lodge a complaint with a supervisory authority

The data subject has the right to bring matters concerning the lawfulness of the university's data protection operations to the Office of the Data Protection Ombudsman for evaluation (tietosuoja(at)om.fi).