PRIVACY NOTICE
CAMERA SURVEILLANCE AND ACCESS CONTROL
EU's General Data Protection Regulation (2016/679), articles 13 and 14
Date: 11 April 2019
Updated: 22 January2021

1. Data controller

LAB University of Applied Sciences
Business ID: 2630644-6

Lahti campus
Mukkulankatu 19, FI-15210 Lahti
Niemenkatu 73, FI-15140 Lahti
Phone: +358 3 828 18 (exchange)

Lappeenranta campus
Yliopistonkatu 36, FI-53850 Lappeenranta
Phone: +358 29 446 5000 (exchange)

2. Data controller's representative and contacts

Data controller's representative:
Name: President Turo Kilpeläinen
Address: LAB University of Applied Sciences, Mukkulankatu 19, FI-15210 Lahti
Phone: +358 44 708 5085
E-mail: turo.kilpelainen@lab.fi

Data controller's contacts:
Name: Facility and Security Manager Janita Markwort
Address: LAB University of Applied Sciences, Mukkulankatu 19, FI-15210 Lahti
Phone: +358 50 502 0670
E-mail: janita.markwort@lut.fi

Name: Service Manager Mirva Törmälä
Address: LAB University of Applied Sciences, Mukkulankatu 19, FI-15210 Lahti
Phone: +358 44 708 1778
E-mail: mirva.tormala@lut.fi

3. Data protection officer

Name: Legal Counsel Anne Himanka
Address: LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland
Phone: +358 50 564 4623
E-mail: tietosuoja@lab.fi

4. Purpose of personal data processing

The LAB University of Applied Sciences employs access control systems and camera surveillance to improve security and protect property. Personal data is processed only by specifically assigned people. Prevent 360 Turvallisuuspalvelut Oy sees to access control and camera surveillance in the data controller's facilities at Mukkulankatu 19 as of September 2018, and Paavolakiinteistöt Oy is responsible for equivalent activities at Niemenkatu 73 and Kirkkokatu 27.

Measuring effectiveness of facilities by camera surveillance is used to calculate utilization levels of facilities and recourses, as learning rooms, research devices and parking areas. Measurement is used for organizing those facilities.

In addition, LAB has an EXAM eletronic examination facility at Niemenkatu 73, where the administrator, information services and technology expert and security expert have the right to conduct online camera surveillance (footage and audio) and the right to view recordings. In the EXAM facility, surveillance cameras enable students to take examinations at a time they choose without the need for invigilators present.

5. Legal basis of personal data processing

Data processing in the camera surveillance and access control systems is based on the data controller's legal obligation (Universities of Applied Sciences Act 14.11.2014/932, section 31) and the pursuit of legitimate interests of the data controller (security and protection of property).

In the EXAM examination space, the basis for data processing consists of a task carried out in the public interest or the exercise of public authority, and the controller's legal obligation (Universities of Applied Sciences Act 14.11.2014/932, section 8).

6. Content of data file and storage period

The access control system stores data on people who have accessed the facilities by opening the electronic lock (first name and last name). As a rule, the data is stored for one year.

The camera surveillance system stores footage of people who access the facilities. Depending on the available capacity, the data is stored for at least seven days unless there is a specific need to store the data for a longer period.

Facility effectiveness measuring system collects outdoor and indoor footage taken by the surveillance cameras. The surveillance cameras record footage from parking areas and learning rooms. Footage data is analyzed with machine vision to fade out identification of persons or vehicles. Footage collected is used only to organize rooms and other space.

Facility effectiveness measuring footage data is stored for 7 days after collection.

EXAM: Camera surveillance prevents misconduct during an examination. The cameras survey every workstation and the front of the room where students leave their belongings. The recordings are stored for 30 days.

7. Information systems employed

The LAB University of Applied Sciences employs secure camera surveillance and access control systems in its facilities and facility effectiveness measuring system.

8. Data sources

The data for the access control system is collected through terminals on doors. With an access control key or tag linked to their ID badge, people can open doors to which they have rights. Data on the person is stored in the access control system (first name, last name). Surveillance cameras record footage in real time and save images of indoor spaces and people in them at specifically defined locations. Outdoor camera surveillance is the responsibility of the property owner.

9. Use of cookies

No cookies are employed in the processing of personal data.

10. Data transfer and disclosure

Camera surveillance and access control at Niemenkatu 73 and Kirkkokatu 27 are seen to by Paavolakiinteistöt Oy and camera surveillance and access control at Mukkulankatu 19 by Prevent 360 Turvallisuuspalvelut on behalf of the data controller.

Facility effectiveness measuring data is processed by external service provider. The footage is stored on service providers servers. Service provider stands as a personal data processor and processes log data in accordance with EU General Dataprotection legislation and with agreement commitments.

11. Data transfer and disclosure beyond the EU or EEA

Data is not transferred or disclosed beyond the EU or EEA.

12. Safeguards for data processing

The data protection guidelines and regulations of the university of applied sciences apply to data processing systems used. Technical safeguards for the systems and their user interfaces include e.g. firewalls, encryptions and backups. The data has been protected from unauthorised use. Only the system administrator and specifically authorised people have access to personal data. Usernames are personal, and only those who need the data for their work have access rights for the duration of their employment relationship. Camera surveillance screens and servers that store access control data are in a locked space. Printed documents are stored and protected from outside use.

Employees of the university of applied sciences are bound by secrecy obligations under the Act on the Openness of Government Activities, section 23. In addition, university employees may not, during their employment relationship, use trade or business secrets to their profit (Employment Contracts Act, chapter 3, section 4). Secrecy obligations are provided for in the employment contract. Secret information and its storage periods, filing and disposal are defined in the university’s filing plan.

13. Automated decision-making

Doors to facilities open automatically to those with pre-defined access rights when the access control key is swiped over the terminal.

14. Rights of the data subject

Data subjects have the right to withdraw their consent if the data processing is based on consent.

Data subjects have the right to lodge a complaint with the Data Protection Ombudsman if the subjects consider that the data processing regarding them is in breach of data processing legislation in force.

Data subjects have the following rights under the EU’s General Data Protection Regulation:

a) Right of access to data concerning the data subject (article 15)
b) Right to rectification of data (article 16)
c) Right to erasure of data (article 17); the right to erasure shall not apply if the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if the right to erasure prevents or significantly hinders the data processing
d) Right to restriction of processing (article 18)
e) Right to data portability to another data controller (article 20).

The data subject's rights involving the processing of personal data may be restricted in accordance with the EU’s General Data Protection Regulation.

The liaison in matters related to the data subject's rights is the data protection officer; contact details in section 3.