PRIVACY NOTICE
Facility Services
EU's General Data Protection Regulation (2016/679), Articles 13 and 14
Date: 3 September 2018
Updated: 29 February 2024

1. **Data controller**
   LUT University
   Business ID: 0245904-2
   Address: Yliopistonkatu 34, 53850 Lappeenranta, Finland
   Phone: +358 294 462 111
   E-mail: info@lut.fi

2. **Data controller's representative and contacts**
   Name: Director Mika Sipi
   Phone: +358 40 5060 910
   E-mail: mika.sipi@lut.fi

3. **Data protection officer**
   Name: Ilona Saarenpää, Legal Counsel
   Phone: +358 50 430 1072
   E-mail: dataprotection@lut.fi

4. **Purpose of personal data processing**
   Facility Services processes personal data related to all of the services it produces. Personal data is processed to manage and monitor facilities, for facility bookings, to manage facility expenses, to monitor access, to mail letters, for car rentals, for reserved parking and its monitoring, and to provide services related to facility and equipment maintenance.

   In addition to the above processing purposes, personal data may be processed under the conditions specified by the university in order to establish the identity of persons visiting in the university campus area. For example in a pandemic situation, it is necessary to establish the identity of persons visiting the university campus area in order to establish the identity of those infected or exposed to infection.

5. **Legal basis of personal data processing**

   The basis for processing personal data is the legitimate interest pursued by the controller and the protection of the vital interests of the data subject or another natural person in exceptional circumstances.

6. **Content of data filing system and storage period**
   Personal data collected on different systems include the person's name, email address, phone number, ID-number, address, office number and vehicle registration number.

In addition, the access control system collects information about a person's residence times in the campus area. A dedicated privacy notice has been prepared for the camera monitoring system operating in the university campus area.

Data is stored for the duration of an employment relationship or studies or for as long as the offered service is valid.

7. Information systems employed

Property management system, facility booking system, data file on key holders, access control system, parking control system, camera surveillance. Camera surveillance has its own privacy notice.

8. Data sources

The property management system and parking control system receive personal data from the university's identity management system. Additional data for the parking control system and all personal data for the other systems is received from the data subjects.

9. Use of cookies

Browser-based filing information systems employ cookies to process personal data. A cookie is a small text file that the browser saves on the user's device. Cookies are used to implement services, facilitate login, and enable the compilation of statistics on services. Users may prevent the use of cookies in their browser programmes, but this may prevent the system from operating appropriately.

The Facility Services' browser-based systems employ cookies in personal data processing to recognise users. Cookies are not used to compile statistics on users.

10. Data transfer and disclosure

Data is disclosed from the parking control system to a parking control company.

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 university's information security rules and guidelines apply to the management of information systems that process personal data. The information systems and their user interfaces are technically protected e.g. with a firewall, encryptions and data backups. Personal data is protected from unauthorised use. Only service administrators or others with specific prior authorisation may access the personal data. Usernames are personal, and user rights to information systems are limited through user group definitions: users may only access data that they need for their professional duties for the duration of their employment relationship. Printed documents are stored and safeguarded from external access.

University employees are bound by secrecy obligations under the Act on the Openness of Government Activities, section 23. In addition, university employees may not use the employer's professional and business secrets to their own advantage or disclose them to others (Employment Contracts Act, chapter 2, section 4). The employment contract has a nondisclosure clause. Secret information and its storage periods, archiving and disposal are defined in the university's filing plan.

13. Automated decision-making

No automated decision-making takes place.

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.