

PRIVACY NOTICE
Finance Services
EU's General Data Protection Regulation
(2016/679),
Articles 13 and 14
Date: 9 October 2018
Updated: 26 March 2019

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

Data controller's representative:
Name: HR and Finance Director Minna Sutela
Phone: +358 40 825 5407
E-mail: minna.sutela@lut.fi

Data controller's contact:
Name: Controller Outi Saimalahti
Phone: +358 50 464 0684
Sähköposti: outi.saimalahti@lut.fi

3. Data protection officer

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

4. Purpose of personal data processing

Personal data is processed to produce the university's finance services.
Personal data is processed for recording working hours, reporting on financial and HR matters, handling sales and purchase invoices, handling travel claims and expense claims, producing travel services, financial and operational planning, and budgeting and invoice archiving.

5. Legal basis of personal data processing

The legal basis of the personal data processing is the preparation or implementation of an agreement, the pursuit of legitimate interests by the data controller, or compliance with a legal obligation by the data controller.

6. Content of data filing system and storage period

The specific identifiers collected on the data subject are the person's name, personal identity code, staff number, bank account number, basic education, nationality and native language. The following contact details are collected: address, phone number(s), and e-mail. The processed data also includes information on the data subject's contracts and recruitment terms, organisational unit, roles, regular working hours, customer number, periods of service, leaves of absence, annual leave, positions of trust, recorded working hours, office and facilities, projects, employment relationship details, salary details, cost centre and system username.

The data is stored permanently in accordance with legislation in force and with storage periods defined in the university's filing plan.

7. Information systems employed

Finance Services employs the following information systems to produce services: working time management system, accounting and travel management system, travel agencies online-reservation system, financial planning and reporting system, university repository, invoice circulation and archiving system, university e-commerce system and credit card ordering system.

8. Data sources

Specific identifiers and contact details of data subjects are obtained from the university's personal data system and student data system. Some of the data is received from the data subjects (recorded working hours, leaves of absence, annual leave, travel and expense claims). Other data processed by Finance Services is received from the accounting system, working time management system, facility management system and university data warehouse.

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.

Browser-based systems employ cookies in the processing of personal data.

10. Data transfer and disclosure

Reports on the working hours and salaries of project employees are disclosed to external sponsors, coordinating organisations of collaborative projects, and accountants.

Data on university credit cards is disclosed to the credit card company.

Travel reservation data is disclosed to the university's travel agency.

Travel costs paid for persons are reported to national income register.

Data related to the payment of purchase invoices and travel and expense claims is disclosed to the bank.

Sales invoices are sent electronically to the e-invoicing operator and data related to debt collection are sent to collection agency.

Data from the invoice archive is disclosed to accountants.

Personal data needed to produce finance services is transferred to the university's data repository where the financial planning and reporting system can access it.

The financial planning and reporting system is a cloud service by an external service provider. The system processes personal data in accordance with legislation and a separate security agreement.

Personal data is processed by Certia.

11. Data transfer and disclosure beyond the EU or EEA

Data is not transferred 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. The data may be accessed only by those with a username for the system. 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 non-disclosure 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 in the data processing.

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