

## **PRIVACY NOTICE**

**Information Services and Technology**

**EU's General Data Protection Regulation (2016/679), Articles 13 and 14**

**Date: 17 May 2018**

**Updated: 29 February 2028**

### **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: Antti Sirviö, CIO  
Address: LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland  
Phone: +358 40 5820878  
E-mail: antti.sirvio@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**

Information Services and Technology (IS&T) as a service provider processes personal data in all systems produced and maintained by IS&T. Personal data is processed to produce services, to resolve faults and anomalies, and to compile user statistics.

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

The personal data processing is based on the pursuit of legitimate interests by the data controller. The data controller has the right to process data to produce services necessary for the activity of the university.

### **6. Content of data filing system and storage period**

Data provided to University that identifies person, such as name, social identification number, contact details and user account. Data is used to produce services, identify customers and transfer necessary personal data to other target systems. Access to all personal data saved in systems.

Data is stored for the duration of an employment relationship or studies. As an exception, user account data is stored for two years after the termination of an employment relationship or after graduation. Separate privacy notice exists to the processing of log data.

## **7. Information systems employed**

Identity management and recognition systems, customer support system, network management and surveillance systems, log systems, security system, system management and control systems.

## **8. Data sources**

Personal data related to identity management and user recognition is received from basic data files on the university's students and students. User activity creates log data.

## **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 properly.

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

## **10. Data transfer and disclosure**

Data is transferred within the organisation to produce services and the cloud services currently employed. Cloud service provider stands as a personal data processor and processes log data in accordance with EU General Data Protection legislation and with agreement commitments.

## **11. Data transfer and disclosure beyond the EU or EEA**

As a rule, 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 administrators with specific authorisation have access to 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 liaison in matters related to the data subject's rights is the data protection officer; contact details in section 3.*