**PRIVACY NOTICE**
**Camera surveillance – electronic exam room**
**EU's General Data Protection Regulation (2016/679),**
**Articles 13 and 14**
**Date: 19 July 2018**
**Updated: 5 March 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

Data controller's representative:
Name: Director of Study Affairs Anne Himanka
Phone: +358 50 564 4623
Email: anne.himanka@lut.fi

Data controller's contact:
Name: Educational Technology Manager Marjaana Kareinen
Phone: +358 40 7171805
E-mail: exam@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

Data obtained with the camera surveillance system in the electronic exam room facilities of LUT University is used to resolve suspected cases of misconduct in examinations.

## 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 perform the tasks referred to in section 4.

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

The system collects surveillance camera footage from the university's electronic exam room facilities. The surveillance cameras record footage and audio material from the electronic exam

room facilities and on people in them. The images are time-stamped.

The data is stored for 60 days from its collection. If the data is connected or suspected to be connected to misconduct, it will be stored for as long as needed to resolve the case.

## 7. Information systems employed

Camera surveillance system.

## 8. Data sources

The data sources are surveillance cameras, and their footage and audio material compose the personal data file. The surveillance cameras are located in the university's electronic exam room facilities.

## 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.

No cookies are used in the processing of personal data in this case.

## 10. Data transfer and disclosure

Data may be disclosed to the university staff to the extent necessary if the data is connected or suspected to be connected to misconduct.

## 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 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. The footage and audio material is stored on a server located in the university's facilities. Only specially authorised persons may access the server facilities. 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.*