PRIVACY NOTICE
LOG DATA PROCESSING
EU's General Data Protection Regulation (2016/679),
Articles 13 and 14
Date: 17 May 2018
Updated: 19 May 2021

1. Data controller

LAB University of Applied Sciences
Business ID: 0245904-2

Lahti Campus
Mukkulankatu 19, FI-15210 Lahti
Niemenkatu 19, FI-15140 Lahti
Tel. +358 3 828 18

Lappeenranta Campus
Yliopistonkatu 36, FI-53850 Lappeenranta
Tel. +358 29 446 5000

2. Data controller's representative and contacts

Data controller's representative:
Name: Rector Turo Kilpeläinen
Address: LAB University of Applied Sciences, Mukkulankatu 19, 15210 Lahti
Phone: +355 44 708 5085
Email: turo.kilpelainen@lab.fi

Data controller's contacts:
Name: Antti Sirviö, CIO
Address: LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland
Phone: +358 40 5820878
E-mail: antti.sirvio@lut.fi

Name: Jari Taipale, CISO
Address: LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland
Phone: +358 40 5575893
E-mail: jari.taipale@lut.fi

3. Data protection officer

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

4. **Purpose of personal data processing**
   Log data is processed in following tasks: IT services problem solving and anomaly investigation, legislation demand of collecting log from information systems and monitoring of information security for producing overall real-time view of information security state. Event logging is also used for controlling the use of information systems.

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**
   Personal data of staff, students and persons belonging to other stakeholders using University IT-services is processed in log systems.
   Log data processed is divided to following classes: error- and alarm log, communication log, information security log, system log, access control log, usage- and change log, transaction log and maintenance log. Following services collect and store personal data during usage: communication services, access control of application- and network services, network and connection access control, operating system and application logging.

   Retention time of log data is normally two (2) years. Access control logs retention time is 2 to 5 years depending on nature of data.

7. **Information systems employed**
   Log data is stored locally to information systems log files. Log data of some information systems is collected to centralized log system. Log data is processed both in local log data files and in centralized logging system. Log data is also processed in Cloud providers logging systems.

8. **Data sources**
   Sources of log data are different information systems: communication devices, servers, workstations, information systems, databases and applications.

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.

   No cookies are used in the processing of personal data.

10. **Data transfer and disclosure**
    Log data is not disclosed outside organization. However, during data breach investigation or preliminary investigation of crime, University may have the right to disclose information to police or other authority.

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.

External service provider stands as a personal data processor and processes log data in accordance with EU General Dataprotection legislation and with agreement commitments.

13. Automated decision-making

Thread detection and response systems may prevent harmful operation automatically.

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)

Data subject's rights under the EU's General Data Protection Regulation do not automatically apply to all data processing

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