Created by Karelia data protection and data security committee

Version: 26 January 2018 (Translated on 15 November 2018)

Discussed in Karelia cooperation and safety committee on 20 February 2018

Karelia Data Protection Policy

The General Data Protection Regulation, GDPR (EU 2016/679)[1] became applicable on 25 May 2018 and it is observed in this Karelia Data Protection Policy.

Data privacy and security management guarantees the responsible and proper conduct from the perspectives of legality and ethical procedures. Furthermore, data protection is an important element of risk management in Karelia UAS. The Karelia Data Protection Policy outlines the basic principles how Karelia UAS ensures the lawful processing of personal data and high-level of data protection in all UAS activities. The Karelia Data Protection Policy is complemented by practical instructions.

The scope, aims and principles of the Karelia Data Protection Policy

Data protection covers the protection of the private life and other rights of an individual securing the privacy when personal data is being processed. Data privacy encompasses the protection of personal data and other confidential or sensitive data of natural persons, i.e. data subjects. Data protection laws require that the processing of personal data must be protected, and that personal data is safeguarded against inappropriate use. The use of data and data systems is monitored, and malpractice addressed according to the Karelia IT regulations.

The GDPR includes the principles of privacy by design and default.

The data privacy principles are:

− lawfulness, fairness and transparency of data processing
− purpose limitations
− data minimisation
− accuracy
− storage limitation
− integrity and confidentiality
− accountability and compliance

> *"The principle of privacy by design and default requires that the above-mentioned data protection principles are implemented effectively in all activities and at all stages of data management.*
>
> *The principle of privacy by default means that the controller processes only such data that are needed for each specific purpose. This obligation concerns the amount of data, scope of processing, storage time and availability. The controller has to take such measures that especially ensure that personal data is by default not accessible to an unlimited number of people without the contribution of the natural person*." [2] (The quote is an unofficial English translation.)

[1] Regulation: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Karelia collects and processes e.g. personal data registers that relate to studies and students, employees, and research, development and innovation. Regarding those registers, Karelia University of Applied Sciences Ltd. is the “controller” and those processing data are “processors”. Part of data is privileged, sensitive and confidential and, if disclosed, can breach privacy and weaken trust in Karelia UAS and its operations.

The accuracy and integrity of personal data need to be verified, and data need to be processed correctly and be accessible when needed. The processing of incorrect, outdated or erroneous data is prohibited, and such data need to be rectified if necessary.

Personal data can be used only by the persons who need them in their studies or work and only to the extent that is necessary for performing their duties or conducting their studies. Data can be transferred only with the consent of the individual or by virtue of applicable law.

Data privacy and data protection are closely connected with data security. Karelia UAS data security policy (available in Finnish) defines what data security means and how it is maintained.

Karelia Data Protection Policy considers also the policy and principles of open science. When balancing between privacy and open science special emphasis is put on practical instructions and solutions regarding research data.

Data retention time and usage

The processing of personal data is based on the consent of the individual or on other purpose defined by applicable law. Personal data is used only for the specific purpose and only to the extent and for the time that it is needed for the purpose. The accuracy of personal data is verified, and the data are updated by consulting the individual or reliable sources, e.g. public authorities. When data are no longer needed for the specific purpose, they must be properly erased.

Data is collected for the specified, explicit purpose in compliance with applicable laws. Data is transferred only on the basis of the consent of the data subject or on the grounds of applicable law and only to the receiving parties specified in the consent or by law. Data may be transferred to another country than that of the controller and in exceptional cases to outside the EU. In such cases, measures regarding data transfer in the GDPR are observed. When transferring personal data outside the EU, special diligence is demonstrated, and applicable regulations strictly followed.

Informing data subjects

The controller is Karelia University of Applied Sciences Ltd. Privacy notices are made for all person registers in compliance with the law. Data subjects are given legally assigned or otherwise important information when collecting personal data.

Responsibilities and organisation

The responsibility for implementation and legitimation of personal data processing belongs to the management of Karelia UAS. Every employee and student who processes personal data needs to know and manage the data protection regulations and risks of his/her area of responsibility. Karelia UAS has appointed a data protection officer (DPO), who directs and develops data protection in Karelia UAS. The position and duties of the DPO are in compliance with the Articles 38 and 39 of the GDPR (see Appendix 1). The contact information of the DPO is publicly available.

The Data Protection Officer is supported by the Karelia UAS data protection and data security committee. The committee consists of the DPO, Director of Administration and Finance, Human Resource Manager, Student Services Manager and the Safety Delegate. The duties of the committee are described in Appendix 1.

Karelia UAS units and educational programmes have nominated their contact persons regarding data protection and privacy. They enhance data privacy at the level of their units and collaborate with the DPO and the data protection and data security committee in Karelia UAS.

When data processing is outsourced, it is secured that the chosen partner follows this Karelia Data Protection Policy. The outsourcing of personal data processing is always defined in a contract, which specifies the responsibilities and obligations of parties.

Ensuring data protection and privacy

Ensuring data protection closely relates to a risk-based approach.

> "*To be able to follow the principle of privacy by default of the regulation and other regulatory obligations, the controller has to make a profound analysis of risks posed by processing personal data. In the GDPR, risks mean the potential physical, material and immaterial damage cause to the data subject when his/her personal data is being processed, e.g. when the data processing might lead to discrimination, identity theft or fraud, financial loss, social damage or reverse of pseudonymization.*
>
> *Risks may be higher when the personal data of specific groups of people are being processed. When the processing of personal data is especially prone to risks, the controller must make a data privacy impact assessment. When assessing the risk level, the nature, context and purpose of data processing must be considered as described above.*" [2] (The quote is an unofficial translation from Finnish.)

When assessing the impact, the controller must seek advice from the Data Protection Officer.

Data protection and privacy is an integral part of new employee orientation and regular training sessions are being organised for all employees. For students, data protection is included in the Career Planning and Development course. All people processing personal data are under legal and separately agreed and documented obligations of secrecy.

The use of the data systems that include personal data are controlled by Karelia UAS user and access management solutions and through other documented procedures.

Karelia UAS assesses and oversees the realisation of data protection and carries out investigations on data privacy as part of its normal control procedures. The application of data protection is verified by providing annual and other reports to Karelia UAS management.

Problems in data protection

The GDPR imposes an obligation on the controller to notify the supervisory authority and the data subject about the personal data breach. Personal data breach includes violation that causes accidental or illegal erasure, loss, alteration, unauthorized transfer of or access to personal data.

As part of the planning of data processing, Karelia UAS has made a procedure regarding personal data breach in order to be able to fulfil the obligations of notification. Every member of Karelia UAS community is

responsible for informing of all shortcomings, threats and procedural faults by sending a message to tietosuoja@karelia.fi. If the data privacy is suspected or discovered to have been endangered, the matter will be immediately investigated. Additionally, the data subject whose data has been breached is informed without delay provided that the notification is justified for rectification or for limiting the damage.

Notifying the personnel, data subjects and stakeholders

Karelia UAS notifies the personnel and student of this Karelia Data Protection Policy and possible amendments in the intranet. The Karelia Data Protection Policy is updated when necessary. Moreover, internal instructions regarding data privacy are being provided.

Karelia Data Protection Policy is valid until further notice. It is a public document and available on the web to internal and external users.

Approval of the Data Protection Policy

The Data Protection Policy has been confirmed by the Karelia UAS data protection and security committee on 13 March 2018.

References:

1. Lapin yliopiston tietosuojapolitiikan luonnos 7.9.2017 (iso osa tekstistä perustuu tähän), linkki 6.1.2018 (edellyttää pääsyn ja kirjautumisen eduuniin korkeakoulujen GDPR-yhteistyön materiaaliin): https://tt.eduuni.fi/sites/kity/EUGDPR/Dokumentteja/_Tiimi_MP_Muut_Palvelut/Ryhm%C3%A4%201%20dokumentit/Lapin%20yliopiston%20tietosuojapolitiikka%20LUONNOS.docx?Web=1

[Draft of the data protection policy of the University of Lapland 7 September 2017. The Finnish site was accessed on 6 January 2018. The access is available only for registered users of eduuni of higher education institutions in Finland.]

2. Tietosuojavaltuutetun ohje ”Miten valmistautua EU:n tietosuoja-asetukseen?” oikeusministeriön ohje 4/2017, linkki 6.1.2018 tietosuojavaltuutetun www-sivuille: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html#mitenvalmistautuatietosuoja-asetukseen

[Instructions by the Finnish Data Protection Ombudsman “How to prepare for the EU General Data Protection Regulation” Guide by the Finnish Ministry of Justice 4/2017. Link to the web site of the Data Protection Ombudsman accessed on 6 January 2018.]

Links: Tietoturvapolitiikka (in Finnish), IT Service User Rules

Appendices: Appendix 1 Data Protection and Data Security Committee, Data Protection Officer

Appendix 1.

President's Decision on 13 October 2017 § 30, appointing the Data Protection and Data Security Committee of Karelia University of Applied Sciences

A committee in charge of data protection and data security at Karelia UAS is formed and appointed as of now to

- prepare the application of the GDPR in Karelia UAS (transition period ends on 25 May 2018),
- process, comment, make statements and approve instructions and alignments that relate to data protection and data security,
- handle major deviations and breaches that relate to data protection and data security and
- develop and promote the implementation of data protection and data security at Karelia UAS.

The Data Management and Data Security Committee consists of:

- Director of Administration and Finance
- Data Protection Officer
- Human Resource Manager
- Manager of Student Services
- Safety Delegate.

Position and duties of Data Protection Officer according to the GDPR are the following:

Article 38

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues that relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

d) to cooperate with the supervisory authority;

e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.