KAMK • University of Applied Sciences

Kajaani University of Applied Sciences' (KAMK Oy) Data Protection Policy

The translation has been produced using AI.

Compiled:	14.5.2018
Approved: Board of KAMK Oy	21.5.2026, 274/07.01.00/2026

Content

Scope of the data protection policy

Data protection means protecting the privacy of natural persons in the processing of personal data. Personal data means any information relating to an identified or identifiable natural person.

KAMK's data protection policy is the highest-level document that guides data protection at KAMK. It describes the basic principles, liabilities and significance of personal data processing at KAMK.

The data protection policy covers all activities involving personal data processing at KAMK. All personal data processing activities must comply with the provisions of the General Data Processing Regulation, the law and data protection policy. The policy is based on the principle of transparency and openness towards the data subject.

Key Concepts of Data Protection

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data include, but are not limited to, name, address, personal identity code, location information, IP address, other online identifiers, photographs, information regarding dietary habits, health data, or any other information which, alone or in combination with other data, can be used to identify the data subject."

‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Examples of processing include the collection, recording, organization, storage, adaptation or alteration, retrieval, dissemination or otherwise making available, including by email or other means.

The ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

The ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The ‘data subject’ means an identified or identifiable natural person whose personal data is processed.

‘Special categories of personal data’ (sensitive personal data) refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation.

‘Pseudonymised data’ means personal data that has been processed in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information.

‘Anonymised data’ means data that has been processed in such a manner that it is no longer possible to associate it with an identified or identifiable natural person.

Data protection by design and default

Ensuring that data protection measures are implemented is part of KAMK's everyday work and risk management. Data protection is already considered when services, processes and systems are in the planning stage.

When processing personal data, KAMK complies with the following data protection principles during every stage of the data life cycle:

- lawfulness, reasonableness and transparency
- processing for intended purpose of use
- data minimization
- data accuracy
- data storage restriction
- data integrity and confidentiality
- controller's burden of proof

KAMK has taken the appropriate technical and organizational measures to ensure that the data protection principles are integrated into personal data processing by design and that by default only those personal data that are needed to accomplish the purpose shall be processed.

In its employer capacity, KAMK must ensure that every employee understands the significance of the principles above and complies with them.

Roles and responsibilities in the implementation of data protection

Every member of the higher education community (management, employees, students, visiting experts and users of the university of applied sciences' systems and services) has the legal obligation of complying with the data protection regulation, the law, data protection policy and any other procedures, rules and instructions concerning data protection at KAMK, as well as to develop and maintain their data protection competence. Every member is liable to report suspected or observed data protection/data security threats or breaches.

KAMK's management (Board of KAMK Oy, CEO/Rector) has the overall responsibility for maintaining the data file as well as organizing, developing and providing resources for data protection.

The directors and Heads of School are responsible for ensuring that the schools/units comply with the data protection regulation, the law, data protection policy and any other procedures, rules and instructions concerning data protection at KAMK.

Managers are responsible for ensuring that the General Data Protection Regulation, applicable legislation, the data protection policy, and other KAMK data protection and information security practices, rules, and guidelines are followed within their area of responsibility or unit. Managers are also responsible for allocating resources for the development of their personnel's data protection competence.

Supervisors are responsible for ensuring that their subordinates have sufficient competence, access to adequate training, proper instructions, and appropriate tools for the lawful processing of personal data. Supervisors are tasked with monitoring the implementation of data protection in their personnel's work, ensuring the onboarding of each new employee in data protection matters, and tracking the completion of data protection training among their staff.

The owner of the personal data file is the manager/director of the respective function. He/she is responsible for ensuring that the personal data processing under his/her charge has been planned and documented in accordance with the data protection regulation taking into account the principles of data protection. He/she is responsible for, monitors and checks that the necessary technical and organizational measures are in place to guarantee compliance with data protection obligations.

The contact person for the personal data file is/are the person(s) responsible for processing or for the practical management of the personal data file. The contact person is responsible for ensuring the personal data file is up to date, among other duties.

The data protection officer's role is to provide data protection expertise to those responsible for maintaining the personal data file. He/she participates in personal data processing planning, preparing and maintaining data protection and security guidelines, follows and monitors personal data processing, advises the staff and data subjects on data protection issues and contacts the supervisory authority if necessary. The data protection officer reports directly to the management of KAMK on the current state of data protection and its development needs.

The data protection group deals with serious and critical breaches in data protection and security and helps the owner of the personal data file to resolve the breach. The data protection group decides whether to request an investigation or to notify the supervisory authority in compliance with the data protection regulation as well as whether to implement internal communication measures together with the CEO/President.

Each member of the higher education community is responsible for implementing data protection in his/her own work. Employees must know and master the data protection regulations and risks relevant to their own responsibilities and develop and maintain his/her data protection competence. All employees at KAMK are bound by KAMK Oy's regulations and non-disclosure and confidentiality duty, which is set out in the employment contract.

Lawfulness of processing

Personal data are only processed for a specific and legitimate purpose that is determined in advance and are only processed to the extent and for as long as is necessary to accomplish the purpose. This concerns the amounts, scope of processing, storage periods and availability of the personal data. After processing, the data are destroyed, anonymized or archived appropriately.

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

At KAMK, particular attention is accorded to the processing of special personal data categories. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, is prohibited. Processing such data is only permitted when a specific condition precedent mentioned in the data protection regulation is fulfilled.

Data Protection Impact Assessment (DPIA)

A data protection impact assessment (DPIA) must be carried out in the following cases:

- when the processing falls under the specific situations defined in the General Data Protection Regulation
- when the processing activity is included in the list issued by the data protection authority
- when required by national legislation

The purpose of the impact assessment is to help identify, assess and manage the risks associated with the processing of personal data. The assessment must be conducted before the processing of personal data begins.

The impact assessment describes the processing of personal data, evaluates the necessity and proportionality of the processing, as well as the risks arising from it and the measures required to address those risks. The assessment helps the data controller comply with data protection legislation, document compliance, and demonstrate it.

Rights of the data subject

KAMK guarantees that data subjects' rights shall be fulfilled in compliance with the data protection regulation and the law. The data subjects' rights are

- right to access data ("right to check data")
- right rectification of data
- right to transfer data from one system to another (portability)

- right to erasure (“right to be forgotten”)
- right to object to processing and automated individual decision-making, including profiling
- right to withdraw consent
- right to lodge a complaint with the supervisory authority

Information on how data subjects can exercise their rights is described in the privacy notices. Privacy notices for job applicants, students, as well as customers and stakeholders are available on KAMK’s website. The privacy notice for employees is available on KAMK’s intranet.

Providing information relating to personal data processing

As the controller, Kajaani University of Applied Sciences, KAMK OY shall provide information concerning personal data processing activities openly and transparently. This information shall be published in the KAMK website, Intranet pages or by other means to ensure that the information reaches the data subjects.

How to proceed when a data protection breach occurs

A data protection or data security breach is a deliberate or indeliberate event or state of events in which the integrity, confidentiality or usability of data and services for which KAMK is responsible are threatened or may come under threat.

It is the responsibility of each one of us to report a suspected or observed threat or breach in data protection/data security without delay. The first observation of a data protection/data security breach can be made by anyone, for example an employee, a student, a partner, a system administrator, an authority, an automated reporting system or an external user of an online service. A report can be submitted using the observation form published on KAMK’s website, by sending an email to secure@kamk.fi, or by contacting a representative of KAMK (the data controller)."

If a data protection/data security breach is suspected or observed, the reason for the breach and its consequences and impacts on data protection shall be investigated immediately. Appropriate measures will be taken to prevent the breach from spreading. The breach shall be documented and analysed. After the situation has been resolved necessary changes and development action shall be identified.

If a personal data breach can cause a risk to the rights and freedoms of natural persons, the supervisory authority must be notified. Personal data breaches must be reported to the Office of the Data Protection Ombudsman without undue delay and, where feasible, not later than 72 hours after the controller has become aware of the personal data breach.

Where a personal data breach is likely to result in *a high risk* to the rights and freedoms of the data subject, the controller shall communicate the breach to the data subject without undue delay.

Communication concerning data protection/data security breaches is a part of KAMK’s crisis and disruption communication strategy.

Development and Maintenance of Data Protection Competence

KAMK actively seeks to develop and maintain the data protection awareness of its staff and students. Guidance related to data protection and template documents for data protection are available on the intranet, where training opportunities related to data protection and information security are also published. Information on data protection-related events and webinars is made available to staff via intranet news and the calendar.

All persons working at KAMK are required to complete KAMK's data protection training, which is also part of the induction process for new staff members. The training is valid for two years, after which it must be repeated. Completion of the training is recorded in the human resources system under the employee's training records. Supervisors are responsible for monitoring completions. Once a year, supervisors and employees are informed by the Data Protection Officer of training completions that are due to expire.

Disclosure / Transfer of Personal Data Outside the EU/EEA

KAMK discloses personal data only on legal grounds or with the data subject's consent, in accordance with the principles of the General Data Protection Regulation (GDPR), such as purpose limitation and data minimization. KAMK may also use external personal data processors, such as companies providing system services, which process personal data on behalf of KAMK under a data processing agreement.

KAMK exercises particular care when transferring personal data outside the European Economic Area (EEA). In such cases, data protection and information security aspects are always assessed on a case-by-case basis. Transfers are carried out in compliance with the provisions of Chapter V of the GDPR concerning the transfer of personal data.

Where the disclosure of personal data is not based on law, it is governed by a personal data disclosure agreement, and the processing of personal data is governed by a personal data processing agreement.

Classification, retention and deletion of personal data

The classification, retention and deletion of personal data are described in KAMK's information management plan. The information management plan includes details of the documents and information assets generated within the organization, as well as the methods related to their registration and processing, and the public accessibility of documents.

Data processing monitoring and supervision

KAMK shall guarantee that the procedures, rules and instructions of good data processing practice and good data management practice will be complied with and supervised. Good data management practices will be implemented to ensure the legal protection of different parties.

Data processing monitoring and supervision is a part of KAMK's internal supervision and risk management strategy.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) of Kajaani University of Applied Sciences (KAMK):

- Acts as an expert resource for persons responsible for records in matters relating to data protection.
- Participates in the planning activities concerning the processing of personal data.
- Contributes to the drafting and maintenance of data protection and information security guidelines.
- Monitors and supervises the processing of personal data and the methods used to protect it.
- Supports staff and data subjects in data protection matters.
- Serves as the contact point for supervisory authorities.
- Reports directly to the organization's management on the state of data protection and development needs.

KAMK may also obtain Data Protection Officer services from an external service provider.

Contact: tietosuojavastaava@kamk.fi

Validity and maintenance of the data protection policy

The Board of Kajaani University of Applied Sciences, KAMK Oy has approved this data protection policy as a binding rule and has authorized the operational management to be responsible for its implementation and maintenance.

The data protection policy is in force until further notice. The Data Protection Policy is reviewed annually, in accordance with the data protection annual schedule, by the Data Protection and Information Security Working Group.

The data protection policy will be published in the www.kamk.fi website and the staff and students' Intranet pages.