v1.0 (21.5.2018)

Privacy policy

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Principles

"Personal data" means any information relating to an identified or identifiable natural person. Personal data is processed ethically with due care and in accordance with applicable legislation and internal guidelines. The starting point is openness towards data subjects. Personal data is processed only using procedures and information systems that are mutually agreed upon. Furthermore, with the documentation of personal data processing, we are able to demonstrate that we have operated in the right way.

Data protection is taken into account already in the planning phase of services, processes and systems. Data protection is also included in the tendering process of information systems. We use reliable services and systems. HAMK is actively involved in cooperation activities concerning data protection between higher education institutions. Well-executed personal data processing supports the efficient functioning of an organisation when the personnel is aware how personal data should be handled.

Data protection principles

Data protection principles are:

- lawfulness, fairness and transparency of processing
- purpose limitation
- data minimisation
- data accuracy
- storage limitation
- data integrity and confidentiality
- accountability of the data controller.

Special categories of data (sensitive data) are only processed under specific conditions set out by law. Special care is taken when processing sensitive personal data. "Special categories of personal data" refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sexual orientation or activity and genetic and biometric data for identifying the person.

As far as possible, identifiable personal data will be removed from the material containing personal data, or it will be converted into unidentifiable form (using anonymisation or pseudonymisation). Data subjects shall have the right to request access to, restriction and rectification or erasure (with certain limitations) of personal data and to object processing. Furthermore, they shall have the right to lodge a complaint with a supervisory authority.

Responsibilities and organisation

The top management is responsible for ensuring the implementation of data protection. The designated data protection officer (DPO) reports directly to the top management. The DPO's duties include, for instance, monitoring, advising and developing matters related to data protection. The DPO also acts as the contact point for the supervisory authority. The DPO shall act independently.

The DPO has a data protection core team and a network of data protection contact persons to help him/her in his/her duties. The data protection core team consists of the DPO, administration manager and risk management manager. Data protection contact persons observe the processing of personal data within their respective fields and, when necessary, guide and report on their observations to the DPO. Some of the data protection contact persons serve as a link between national networks in the field.

Each employee must familiarise themselves with and command data protection legislation and risks related to their duties.

Communications, information and training

Data protection is integrated into instructions. In addition to this, particular instructions concerning personal data processing are available.

Public websites, Yammer and intranet pages serve as data protection communication channels.

Independently performed and acquired open badges are used for recognising and verifying successful completion of data protection training. Matters and trainings related to data protection are introduced to new employees during orientation. Data protection matters are also included in development discussions.

Privacy notices of each personal data file will be elaborated as required by law.

Personal data lifecycle and usage

A legal basis is determined for personal data processing before the processing is initiated. Furthermore, a risk analysis is conducted for the processing of personal data. If there is a potential high risk to the processing of personal data, a data protection impact assessment will be carried out. This is particularly important when new technology are to be implemented or special category data or breaches are being handled.

Personal data shall be disclosed outside the EU/EEA only in exceptional cases. In these cases, the grounds for disclosures will be reviewed in advance with the DPO.

The processing of personal data and the use of information systems are being monitored, and detected issues are taken care of.

Data retention periods will be described in the information management plan. Unnecessary personal data will be destroyed in a secure manner.

When necessary, HAMK personnel and students must update their personal data in HAMK systems.

Each personal data file has a designated organisation in charge and a contact person that take care of responding register-specific contacts and requests.

Reporting and follow-up

Reporting of data protection matters will take place in accordance with annual operating plan (vuosikello). Incidents related to data protection will be gathered in a separate event log. A data balance sheet will be prepared annually.