Haaga-Helia University of Applied Sciences Privacy Notice for Quality Management System

In compliance with the requirements of the EU General Data Protection Regulation (GDPR, Articles 13, 14 and 30)

Created on: 14/5/2018

Updated: 22/6/2023

1. Controller of data file

The controller of the data file is Haaga-Helia University of Applied Sciences Ltd (Business ID 2029188-8).

Ratapihantie 13

00520 Helsinki, Finland

2. Controller's contact person

Tia Hoikkala, Quality Manager

tia.hoikkala@haaga-helia.fi

+358 40 488 7590

3. Controller's Data Privacy Officer

dpo@haaga-helia.fi

+358 29 447 1222

Requests concerning the exercising of the data subject's rights should be addressed to the controller's data privacy officer.

4. Name of data file

Data file concerning quality management system.

5. Purpose of processing of personal data

Personal data are processed for the purpose of managing, administering, maintaining and developing the controller's quality management system. The quality management system comprises the organisation's way of operating and developing, and it covers the controller's entire organisation (e.g. education services, RDI, and their support services).

The controller processes the data in house, as well as subcontracting parties to process the data on the controller's behalf.

6. Lawfulness of processing of personal data

6.1. The lawfulness of processing personal data is based on the following principles of the EU General Data Protection Regulation:

a) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (GDPR Art. 6 (1)b); or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (GDPR Art. 6 (1)f).

b) Processing is necessary for compliance with a legal obligation to which the controller is subject (GDPR Art. 6 (1)c);

c) The personal data belongs to a special category, and processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (GDPR Art. 9 (2)g).

The aforementioned legitimate interests of the controller are based on a meaningful and appropriate relationship between the data subject and the controller, which arises when the data subject is related to the controller in connection with the purpose of use of the data file, as long as the processing is done for purposes which the data subject can reasonably be assumed to have expected at the time of, and in conjunction with, the data being collected.

7. Content of data file and personal data categories processed

7.1. Personal data categories

a) Basic details of data subject
b) Other data on data subject

7.2. For each data category, the data file contains the <u>following personal data, considered legitimate (the list is not exhaustive, and not all of the data listed is necessarily present for every data subject)</u>:

a) Basic details of data subject
   - Name
   - Email address
   - Username
   - Age
   - Gender

b) Other data on data subject
   - Educational background
   - Employment status
   - State of health (when recorded by data subject)
   - Course/degree programme/training session/event attended by data subject
   - Academic year and semester when the data subject started at Haaga-Helia
   - Mentions of personnel member or student in open feedback
   - Responses to surveys

8. Regular data sources and personal data generated as part of controller's operations

Personal data are collected from the data subjects themselves. Additionally, the controller collects personal data generated in the operation of the quality management system.

Data for the data file is collected from official data systems (e.g. the Arvo system of the Ministry of Education and Culture, and the AVOP survey that collects feedback from graduands), as well as from other sources in the public domain.

Within the bounds of applicable legislation, personal data are collected from sources in the public domain, as well as from other third parties, such as companies in the same group and other contractual partners.

9. Period of storage of personal data

The personal data in the data file are only stored for as long as and to the extent that each category of data is needed, proportionate to the purpose of processing of the personal data. Additionally, the duration of storage of personal data complies with possible statutory requirements.

The controller of the data file regularly evaluates the need for storing data in accordance with its internal practices.

10. Regular disclosures of personal data

When necessary, the personal data in the data file are disclosed to:

a) within the bounds and demands of applicable legislation, to, for example the Ministry of Education and Culture, the Finnish Education Evaluation Centre, or other similar parties who have a legal basis for receiving data from the data file;
b) other companies in the same group;
c) partners (e.g. accreditation organisation) who need them to execute the quality management system.

11. Transfers and disclosures of data to outside of the EU or EEA

Data from the data file are not habitually transferred to outside the EU or EEA, nor processed outside the EU or EEA, unless this is necessary for the technical implementation of the processing (for example if the technical maintenance of systems is located outside the EU or EEA), or in order to manage international functions related to the purpose of use of the data file.

In transferring personal data, the controller complies with the standard contractual clauses approved by the European Commission in relation to the transfer of personal data to third-party countries, or alternatively implements other appropriate safeguards, or alternatively ensures that the third-party country can guarantee a sufficient level of data protection.

12. Data security principles

Access to databases and systems and use of the data file are only available to such employees of the controller or of subcontractors working on the controller's behalf, whose work duties entitle them to handle the data contained in the data file. Every user of the data file has an individual username and password for the systems.

Materials containing personal data are stored in locked facilities that may only be accessed by specifically appointed persons whose work duties entitle them to do so.

The database containing personal data is stored on a server which is placed in a locked facility that may only be accessed by specifically appointed persons whose work duties entitle them to do so. The server is protected by an appropriate firewall and technical security systems.

13. Rights of the data subject

The data subject has the following rights in accordance with the EU General Data Protection Regulation:

1) The right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
    i) the purposes of the processing;
    ii) the categories of personal data concerned;
    iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
    iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
    v) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    vi) the right to lodge a complaint with a supervisory authority;
    vii) where the personal data are not collected from the data subject, any available information as to their source; and
    viii) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (GDPR Art. 15)

Additionally, the data subject has the following rights:

1) The right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. (GDPR Art. 7)

2) The right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her, as well as the right to have incomplete personal data completed, including by means of providing a supplementary statement. (GDPR Art. 16)

3) The right to obtain from the controller the erasure of personal data concerning him or her without undue delay, where one of the following grounds applies:
    i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    ii) the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
    iii) the data subject objects to the processing on grounds relating to his or her particular situation, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes;
    iv) the personal data have been unlawfully processed;
    v) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject. (GDPR Art. 17)

4) The right to obtain from the controller restriction of processing, where one of the following applies:
    i) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
    ii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
    iii) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
    iv) the data subject has objected to processing on grounds relating to his or her particular situation, pending the verification whether the legitimate grounds of the controller override those of the data subject. (GDPR Art 18)

5) The right to receive the personal data concerning him or her, which he or she has provided to the controller, in a structured, commonly used and machine-readable format, and the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to the GDPR, and the processing is carried out by automated means. (GDPR Art. 20)

6) The right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. (GDPR Art. 77)

Requests concerning the exercising of the data subject's rights should be addressed to the controller's data privacy officer.