

(1050/2018) Date created:

27.10.2023

Combined document for informing data subject (EU General Data Protection Regulation 2016/679) Articles 13 and 14.

1. Controller	<p>Seinäjoki University of Applied Sciences Kampusranta 11, Frami F 60320 Seinäjoki +358 20 124 3000 seamk(at)seamk.fi</p>
2. Controller's & this register's representative	<p>Project manager Kampus 2030 project, Katja Kaataja, +358 40 830 4023, katja.kaataja@seamk.fi</p>
2b. Contact persons for matters related to the personal data file	<p>Projektipäällikkö Kampus 2030 -hanke, Katja Kaataja, +358 40 830 4023, katja.kaataja@seamk.fi</p>
2c. Data Protection Officer's contact details	<p>Jarmo Jaskari, Data Protection Officer, Seinäjoki University of Applied Sciences tel. +358 40 8680680 tietosuojavastaava(at)seamk.fi</p>
3. Personal data file name	<p>Kampus 2030 –hankkeen rekisteri</p>
4. Purpose of processing personal data / purpose of file use / duration of data storage	<p>In the project, information, opinions, and data are collected from various target groups. The collected material is used for the following purposes within the Campus 2030 project: - conducting needs and objective analysis - conducting pilots and experiments - planning resource allocation and measures - evaluation and continuity planning - compiling the Campus 2030 development plan. Various events and communications may be organized for different target groups within the project.</p>
5. Purpose of maintaining the file	<p>Personal data is processed based on participation in the project's surveys, events, workshops, etc. Personal data is processed based on the individual's consent.</p>

5a. Data content of the file	Name, email, phone number, city/town of residence, age, occupation, education level
5b. Information systems using the file	Sähköposti, Webropol, Forms, Word, Excel
6. Regular data sources	Individuals and organizations themselves, and for organizations also public sources
7. Regular disclosures of data	Employees of organizations within the project team have the right to use information in anonymized form. The organizations within the project team include SeAMK, as well as the City of Seinäjoki, the South Ostrobothnia University Consortium, and the Seinäjoki University Center.
8. Transfers of data to non-EU or EEA countries	No transfers.
9. Principles of file protection	<p>A. Manual material Paper materials are kept in locked cabinets and locked premises. Access to the materials is restricted to personnel handling the information.</p> <p>B. Data processed in computer systems The data subject has the right to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed. The data subject has the right to access their data. A fee may be charged for this right of access or the request may be refused if the requests are manifestly unfounded or excessive, especially if they are repetitive. (Article 12 and Article 15)</p>

10. Data subject's rights

The EU General Data Protection Regulation (2016/679) provides data subjects with the following rights:

Right to withdraw consent

The data subject shall have the right to withdraw his or her consent at any time. (Article 7)

Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. The data subject has the right of access to his or her data. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either charge a fee for the right of access or refuse to act on the request. (Article 12 and Article 15)

Right to rectification

The data subject shall have the right to obtain from the controller the rectification of inaccurate personal data concerning him or her (Article 16). The request for rectification shall be made in writing.

Right to erasure

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her where one of the following grounds applies: (Article 17):

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- The data subject withdraws consent on which the processing is based and there is no other legal ground for the processing
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing (Article 21)
- the personal data have been unlawfully processed
- 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;

Right to restriction of processing

The data subject has the right to obtain from the controller restriction of processing where one of the following applies (Article 18):

- 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
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
- 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
- The data subject has objected to processing pursuant to Article 21 pending the verification whether the legitimate grounds of the controller override those of the data subject.

	<p>Right to data portability</p> <p>The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format where the processing is based on consent and the processing is carried out by automated means. (Article 20)</p> <p>Requests for exercising these rights are addressed to: Seinäjoki University of Applied Sciences Data Protection Officer P.O. Box 412 (Kampusranta 11 F) 60320 Seinäjoki</p>
<p>11. Rectification</p>	<p>The controller shall, on its own initiative or at the request of the data subject, without undue delay rectify, erase or supplement personal data contained in its personal data file and erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing.</p> <p>Immediately after discovering an error, the person responsible for the file shall rectify it or inform the person with sufficient rights to rectify the error of it. The data subject has the right to demand that the data be rectified, and the rectification should be carried out without undue delay. If the controller refuses the request of a data subject of the rectification of an error, a written certificate to this effect shall be issued. The data subject may bring the matter to the attention of the Data Protection Ombudsman at: Office of the Data Protection Ombudsman, P.O. Box 315, 00181 Helsinki. The Data Protection Ombudsman may order the controller to rectify the data.</p> <p>A request for rectification should be made in writing or orally to the contact person for matters related to the personal data file, and the data subject's identity should be verified if necessary.</p> <p>In other cases, the request for rectification should be addressed to: Seinäjoki University of Applied Sciences Jarmo Jaskari, Data Protection Officer P.O. Box 412 (Kampusranta 11) 60101 Seinäjoki</p>
<p>12. Other rights related to the processing of personal data</p>	<p>Verification of identity</p> <p>Unless the person requesting the information is already known or verifying their identity by other means is not possible, they must always prove their identity before the information is disclosed. As proof of identity is accepted an official photo ID, which are a driving licence, a passport or an identity card issued by the police, and a Kela card.</p> <p>Prohibition of disclosure of address data</p> <p>A data subject has the right to prohibit the disclosure of information concerning them from the Population Information System and related documents.</p>

Act on Population Information System and the certificate services of the Digital and Population Data Services Agency 21.8.2009/661. Chapter 4, sections 28 to 50a
Public access to Population Information System data and disclosure thereof

- for purposes of direct advertising, distance selling, other direct marketing, market research and opinion polls
- as an address service
- for a public register
- for genealogical research

A request to prohibit the disclosure of the personal data for the above-mentioned purposes should be addressed to the Population Register Centre or the Local Register Office. Once the prohibition enters into force, the Population Register Centre will no longer provide the above information to SeAMK as an address service. A data subject who does not wish to provide their address data will be personally responsible for any harm and damages incurred if they cannot be reached.

Non-disclosure order

If you have a justified reason to suspect that your or your family's health or safety is threatened, the Local Register Office can on request stipulate that data on your municipality of residence or address may only be disclosed from the Population Information System to authorities. To obtain a non-disclosure order, you need to submit a well-founded written request to your Local Register Office, or at least visit the Office. The first non-disclosure order is granted for a maximum of five years. It can be extended by two years at a time. It can be extended for two years at a time. When you have been granted a non-disclosure order, your address is in many cases not disclosed even to the authorities. The authorities that can access a person's contact details through their systems will also be informed of the non-disclosure order.

If necessary, a person who has been granted a non-disclosure order should inform the officer responsible for the personal data file of it.

Restraining order

By a restraining order, the life, health, liberty or inviolability of a person may be protected by prohibiting another person from contacting him or her. An application for a restraining order may be filed by anyone who has justified grounds for feeling threatened or seriously harassed by someone else. An application for a restraining order is filed with the police or directly with a district court.

If necessary, a person who has been granted a restraining order must inform the officer responsible for the personal data file.