

Privacy notice (11.1.2024) for scientific research

EU General Data Protection Regulation (EU 2016/679), art. 12, 13, 14

1. Title, nature and duration of research

Title of research: Effectiveness of cybersecurity teaching in Cryptography engineering II course

- ☐ Case study
- ☒ Follow-up study

Duration of research: 2022–2026

Duration of data processing: Until planned publications have been published and one year after the last publication.

2. Data Controller

- ☒ Research will be conducted in an employment contract with the Tampere University, indicating the University to be the data controller.

Tampere University Foundation sr
33014 Tampere University
Kalevantie 4, 33100 Tampere
Business ID: 2844561-8

Data Protection Officer of Tampere University dpo@tuni.fi

- ☐ Research is conducted by a student not employed by the Tampere University which makes the student the data controller. Name and contact information of the student:

- ☐ Registry is jointly controlled with several data controllers (joint controllership). Name all the data controllers and contact details of their Data Protection Officers:

3. Principal investigator or research group

The Principal Investigator is a person assigned by the Data Controller to oversee the implementation of the research project. A research group may also be assigned to serve as the Principal Investigator.

Name: Tiina Schafeitel-Tähtinen

Contact detail: tiina.schafeitel-tahtinen@tuni.fi

4. Researchers

Please indicate the persons who will carry out the research activities. If the project is collaboratively conducted, please list the researchers from each partner organisation.

Tiina Schafeitel-Tähtinen

5. Content of research records

Add a description of the personal data to be processed by categories, e.g. names, contact information etc.:

Surveys:

- Gender
- Phase of studies (bachelor, master, doctoral)
- Additional information about studies (e.g., exchange, work-life)
- Study field
- Previously completed education

Course performance data:

- Students' exercise and quiz points in Moodle

Students' written self-evaluations in Moodle (a "learning diary") concerning their learning in

1. peer-evaluated,
2. automatically evaluated,
3. teacher-evaluated, and
4. reading group

exercises.

The types #1, #2 and #3 of evaluations are voluntary, but the reading group scoring (for the course grade) is partly based on a self-evaluation report. The student can divide that report in such a way that a major part is excluded from the research records, and writing the remaining part is voluntary. That remaining part is supposed to complete the student's learning diary, and it is crucial from the research point of view. It will provide these data to the research records:

- perceived success in type #4 exercise: numerical scale in these dimensions:
 - usefulness of the topics
 - interest in the topics
 - learning achievement compared to one's own goal
 - learning achievement compared to what one thinks or knows the others achieved
 - comparison of perceived success in type #4 exercises in relation to each of the other types of exercises: numerical scale telling how much more or less
 - interesting
 - memorable
 - usable
- did approach #4 make the topics for which it was used in comparison to approach #1, #2 and #3.
- any explanations the student wants to add to make these scores understandable.

6. Sources of personal data

From which sources are data being gained or collected:

Participants (survey, scores, written reports), Tampere University Moodle platform for course Cryptography Engineering II

7. Purpose of processing personal data

The purpose of processing personal data is scientific research. Please, describe the project in more detail:

Participants fill out pre- and post-course surveys. Pre- and post-responses are compared and combined with the course performance data and self-evaluations (partial, as stipulated in section 5). Effectiveness of the teaching methods are compared, and the effectiveness of the course is measured. Personal information is used as variables in statistical analysis.

8. Lawful basis for processing personal data

The lawful basis for processing is the EU General Data Protection Regulation Article 6 Paragraph 1 and the Data Protection Act (1050/2018) 4 §:

- ☒ Public interest or the exercise of official authority
 - ☒ Scientific or historical research purposes or statistical purposes
 - ☐ Archiving of materials relating to research or cultural
- ☐ Consent
- ☐ Legal obligation of the data controlled
- ☐ Legitimate interests of the Data Controller or a third party
Please specify the legitimate interests:
- ☐ Other, please specify:

9. Sensitive personal data (special categories of data and criminal records)

- ☒ No sensitive personal data will be processed during the research project
- ☐ The following types of sensitive personal data will be processed during the research project:
 - ☐ Racial or ethnic origin
 - ☐ Political opinions
 - ☐ Religious or political beliefs
 - ☐ Trade union membership
 - ☐ Genetic data
 - ☐ Biometric data to uniquely identify a person
 - ☐ Health data
 - ☐ Data concerning a natural person's sex life or sexual orientation

Will personal data concerning criminal convictions and offences be processed during the research project?

- ☒ No
- ☐ Yes

10. Transfer of data to external parties (Transfer means that some other party will process personal data and return the results to data controller)

☐ Personal data will be regularly transferred to parties other than the members of the research group.

Please describe the type of data that will be transferred, the recipient and the legal grounds for transferring personal data:

Processing activities will be outsourced (for example to a subcontractor). Please, specify:

☐ Data will be disclosed. To whom it will be disclosed, please specify:
What is the legal basis to disclose data, please specify:

11. Transfer or disclosure of data outside the EU/EEA

Will data stored in the research records be transferred to a country or an international organisation that is located outside the EU/EEA?

☒ No

☐ Yes, please specify (contact always Data Protection Officer):

Description of the measures taken to protect data:

12. Data protection principles

Protection of digital materials (e.g. information systems and equipment):

☒ usernames

☒ password

☒ multi-factor authentication (MFA)

☒ access management (IP address)

☐ collection of log data

☐ physical access control

☐ other, please specify

Processing of data that directly identifies an individual:

☐ Directly identifiable data will be removed during the analysis stage

☒ The materials will be pseudonymized, pseudonymization codes are separate from research material, researcher does not have access to information linking codes and research participants

☐ The materials will be analysed without removing directly identifiable data, because (please provide the reasons for retaining personally identifiable data):

Protecting data in transit:

☐ secure transmission, please specify:

☒ file encryption, please specify: The teacher using the course Moodle will send the pseudonymised data to the researcher in an encrypted file, and agree on the key by using a phone. The researcher is not participant on the course Moodle.

☐ other, please specify:

13. Processing of personal data after the research project has been concluded

- ☐ The research records will be destroyed
- ☒ The research records will be anonymised and archived without personally identifiable data
- ☐ The research records will be archived without anonymisation

Where will the research materials be stored and for how long: The research material is processed according to Fair Data principles. After the research, survey data is opened and stored in the IDA - Research Data Storage Service. All collected survey data from several courses during 2022-2026 is combined without information which course and year the data is from. Background information with less than 5 students is aggregated under "other" category to mitigate the risk of identifying students with rare combination of background variables. Opening data gives other researchers access to data, and they can, for example, repeat the analysis of data. In addition, opening the research data enables the reuse of the collected material as part of another research.

14. Data subjects' rights and possible restriction thereof

Data subjects have the following rights under the EU's General Data Protection Regulation (GDPR):

- Right of access
 - o Data subjects are entitled to find out what information the University holds about them or to receive confirmation that their personal data is not processed by the University.
- Right to rectification
 - o Data subjects have the right to have any incorrect, inaccurate or incomplete personal details held by the University revised or supplemented without undue delay. In addition, data subjects are entitled to have any unnecessary personal data deleted from the University's systems.
- Right to erasure
 - o In exceptional circumstances, data subjects have the right to have their personal data erased from the Data Controller's records ('right to be forgotten').
- Right to restrict processing:
 - o In certain circumstances, data subjects have the right to request the University to restrict processing their personal data until the accuracy of their data, or the basis for processing their data, has been appropriately reviewed and potentially revised or supplemented.
- Right to object
 - o In certain circumstances, data subjects may at any time object to the processing of their personal data for compelling personal reasons.
- Right to data portability
 - o Data subjects have the right to obtain a copy of the personal data that they have submitted to the University in a commonly used, machine-readable format and transfer the data to another Data Controller.
- Right to lodge a complaint with a supervisory authority
 - o Data subjects have the right to lodge a complaint with a supervisory authority in their permanent place of residence or place of work, if they consider the processing of their personal data to violate the provisions of the GDPR (EU 2016/679). In addition, data

subjects may follow other administrative procedures to appeal against a decision made by a supervisory authority or seek a judicial remedy.

Contact information:

Office of the Data Protection Ombudsman

Street address: Lintulahdenkuja 4, 00530 Helsinki, Finland

Postal address: PO Box 800, FI-00531 Helsinki, Finland

Switchboard: tel. +358 29 56 66700

Fax: +358 29 56 66735

Email address: tietosuoja@om.fi

The Data Controller follows a GDPR-compliant procedure for responding to subject access requests.