Rīgas Stradiņa Universitāte

Personal data protection in the learning process

RSU Data Security and Management Unit

Important to remember!

Data processing is not just about preparing documents - data processing is any activity with personal data:

- interviewing/addressing a research participant / a patient,
- undergoing tests,
- measuring indicators, researching,
- providing procedures to a patient,
- patient monitoring,
- audio or video recording during the learning process or for carrying out the research work, etc.

What is the processing of personal data?

Any operation or set of operations carried out with personal data or with sets of personal data, whether or not by automated means (including collection, recording, input, storage, organisation, modification, use, transfer, transmission and disclosure, blocking or erasure). Processing may be done orally, in writing or electronically.

Does not apply to the processing of personal data::

- Operations carried out by natural persons for personal or family purposes, without the personal data being disclosed to third parties. Provided that it is not related to a professional or commercial activity.
- Operations carried out by competent authorities to prevent, investigate, detect or prosecute criminal offences or to impose criminal penalties, including to protect against and prevent threats to public security.

Personal data

When processing personal data, it should be noted that personal data is any information relating to an identified or identifiable natural person. Personal data also consists of various pieces of information which, when collected, may identify a specific person.

Personal data may include:	Personal data does not include:
• name and surname (e.g. Datis Datne); • place of work (e.g. Datis Datne works for “X” Ltd); • position held (e.g. Director of “X” Ltd); • home address (e.g. Datis Datne's declared address of residence is 15 Trotuāra iela, Riga); • e-mail address (e.g. datis.datne@siax.lv); • personal identity number, number of personal identity documents; • location data (e.g. location data function on a mobile phone); • Internet Protocol (IP) address; • cookie identification number; • patient data stored by a medical institution, etc.	• Signe Bērziņa has debts of €10 000 (no identifier in this case); • the deceased Datis was a good employee (no personal data as the person is deceased); • “X” Ltd is an insolvent company (the company is not a natural person but a legal person); • company registration number; • Trotuāra iela 15, Riga; • datis958@inbox.lv or info@siax.lv (as long as there is no identifiable link to any person); • anonymised data (to be truly anonymised, anonymisation must be irreversible. Meanwhile, personal data that has been identified, encrypted or pseudonymised, but can be used to repeatedly identify a person, still qualifies as personal data).

It should be noted that a name and surname alone, which is common, will not be personal data in the absence of additional information. On the other hand, if this particular name and surname is linked to an additional identifier, such as a personal identity number, study course, place of work, etc., it is personal data because the person is already identifiable. Personal data that has been de-identified, encrypted or pseudonymised but can be used to repeatedly identify a specific person is still be considered personal data and is subject to the requirements of the General Data Protection Regulation.

Special categories (sensitive) data

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), health data or data concerning a natural person's sex life or sexual orientation. The processing of such special categories of personal data is prohibited by the General Data Protection Regulation, except in specified cases, such as:

- the person has given explicit consent to the processing of their personal data - in this case informed consent must be given;
- the person has intentionally made his/her data publicly available on a website, on social networks, etc.;
- legislation provides for the processing of such data for a specific purpose in order to exercise the rights of the controller or data subject in the field of employment, social protection, healthcare;
- legislation provides for the processing of certain data in public interest, such as archiving purposes, scientific or historical research, statistics, etc.;
- defending own legal rights by making a court claim;
- protecting the vital interests of a person, where the data subject is physically or legally incapable of giving his or her consent, etc.

When drawing up Bachelor's, Master's, Doctoral theses, research-related documentation or as part of the study process, it is important to remember that special categories of data may also be available in various documents and information units (e.g. video recordings, photographs). However, it is necessary to critically assess whether this information is intended to be used as special categories of data.

Health data and biometric data

Health data includes the following information:

- the health status of a person and the medical procedures (treatment) applied to him/her;
- the results of the data subject's medical tests, information about the blood group, certain diagnoses, treatment and about family history of diseases;
- the data contained in medical records relate directly to a person's health and therefore to his private life.

Biometric data includes the information about:

- personal data, after specific technical processing, relating to the physical, physiological or behavioural characteristics of a natural person which allows or confirms the unique identification of that natural person.

Health and biometric data may be used with the free and explicit consent of the data subject or, where the processing of biometric data is necessary for reasons of substantial public interest.

ALL DATA PROCESSING PRINCIPLES MUST BE ADHERED TO

- Data is processed fairly and lawfully, in a manner that is transparent to the data subject
- Data processing is done for a specific purpose
- Data is adequate and not excessive - the principle of data minimisation must be respected
- Data is accurate - data must be updated, corrected and deleted
- Data is not stored longer than is necessary for the purpose for which they are processed - i.e. they are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed - the data retention limit must be respected
- Data is secure - integrity and confidentiality
- Accountability - data storage can be ensured and proven (most often by documentation)

Data storage

- Data must be stored in a secure place: RSU primarily MSTeams, OneDrive (files uploaded to MS Teams are automatically saved to OneDrive
- Both OneDrive and MS Teams files can be controlled and access restricted (benefit - files are available 24/7 even remotely)
- Data storage needs to be assessed
- If there is uncertainty, the Director of the study programme, colleagues at the Academic Affairs Department or Data Security specialist may be consulted

Processing of personal data prior to conducting the research:

Plan - idea

- Student research is usually primarily carried out for obtaining higher education qualifications, but it is also possible that research will be planned as part of the research projects carried out at RSU under the supervision of a responsible researcher.
- In order to ensure that the research is carried out in accordance with good practice recommendations, it is necessary to answer questions before the research is conducted that will help to organise personal data protection issues and to identify the documents required for the research - decisions, permits, agreements, etc.
- It is the student's responsibility to use the information obtained in the research only for the purpose of the research work.
- It is the student's responsibility to store the results and data obtained from the research.

Students themselves or together with their supervisor, shall draw up a research protocol, an application, Informed Consent (IC) forms, if necessary, and, in accordance with the general principles, apply for their research permit by submitting documents to RSU Research Ethics Committee. Information about RSU Research Ethics Committee is available on the website Research Ethics Committee | RSU.

Control questions before conducting research

- What is the purpose of the research?
- Who will conduct the research? Which institutions will be cooperated with?
- What are the physical and/or psychological risks to the research participants and research staff?
- What measures will be taken to minimise risks and protect research participants?
- What are the expected benefits of the research?
- Who will obtain the patient's or participant's informed consent (if required for the research)?
- Does the research pose risks, what risks and to whom?
- Will genetically modified organisms be used or created in the research?
- Will personal data (e.g. name, surname, personal ID number, IP address, address of residence, questionnaires, audio, video recordings, photographs) be collected and processed as part of the research?
- Will special categories of personal data be obtained and processed as part of the research?
- Will the research involve pseudonymisation or anonymisation of personal data?
- Will the research involve surveys (anonymised or the data subject can be identified)?
- How long, where and how will personal data be stored?
- Who will have access to the personal data within the research?
- What will happen to the personal data if the person stops participating in the research?

Control questions before conducting research

- Is it planned to observe or track research participants within the research?
- Will the research involve secondary processing of personal data previously obtained for other purposes (e.g. from patients' medical records, registers, databases, archives)?
- Will biological samples of human origin be collected and/or used in the research?
- Will human cell lines be used in the research?
- How long and how will the human biological samples, used in the research, be stored and what will happen if the person stops participating in the research?
- Are there plans to transfer personal data and human biological samples or cell lines from/to EU countries or countries outside EU as part of the research? What are the cooperation partners?
- To whom will the data, results of the research be transferred? Where will the results be published?

Further actions

Carried out according to each research individually:

- Conclusion of cooperation agreements with partners (if necessary)
- Conducting public procurement for services and use of infrastructure (if necessary)
- Conclusion of other contracts, as appropriate to the research, e.g. company contracts, employment contracts, other types of cooperation agreements
- Attracting patients or participants
- Surveys (if necessary)
- Obtaining or receiving material and data
- Collection, analysis and evaluation of data received
- Conclusions and publications

How to ensure data protection for the purposes of the learning process?

Anonymisation

- Anonymised information is information that does not allow the identification of the person to whom the information originally processed and/or actually attributed was concerned.
- Anonymisation of personal data is irreversible in nature: anonymisation is equivalent to the complete erasure of information.
- In order to determine whether a natural person is identifiable, consideration should be given to all means that the controller or any other person could reasonably use, for example, separate distribution in order to identify a natural person directly or indirectly.
- In order to ascertain whether the means could reasonably be used to identify a natural person, all objective factors, such as the cost and time required for identification, should be considered, taking into account the technological developments available at the time of processing.

Pseudonymisation

- Pseudonymisation is a process of disguising identity. The purpose of such a process is to be able to collect additional data relating to the same person without knowing his or her identity.
- It reduces the possibility of linking information to a person's identity, but it should be considered as a security measure rather than an anonymisation method.
- The use of a pseudonym means that it is possible to trace back to the person and the identity of the person can be revealed, but only in predefined circumstances.

Notifications of personal data breaches

Any RSU employee or student shall immediately notify the Data Protection specialist of a breach or suspected breach by telephone 67409144 or by sending a report about the breach electronically to personu.dati@rsu.lv.

After identifying and assessing the breach, and no later than 72 (seventy-two) hours after becoming aware of the breach and in cases where it may pose a significant or major risk to the rights and freedoms of the Data Subject, the Data Protection specialist or other authorised person shall prepare and send a notification to the Supervisory Authority.

If, after identification and assessment of the breach, it is concluded that the breach may pose a significant or major risk to the rights and freedoms of the Data Subject, the Data Protection specialist shall inform the Data Subject of the breach using the available contact details of the Data Subject.

Rights of the Data Subject (natural person, including student)

The Data Subject (natural person, including student) has the following rights:

- to know (to receive information in a clear and comprehensible form) about the processing of their personal data;
- to obtain access to their personal data, i.e. access to the following information: the purpose of the data processing, the legal basis, the categories of personal data, the recipients or categories of recipients, the intended period for which the personal data will be stored (if possible), if the personal data is not collected from the data subject, any available information about the source;
- if the personal data is inaccurate and/or incomplete, to request rectification of the processed data;
- request the erasure of their personal data if the personal data is unlawfully processed, an excessive amount of personal data is processed or the data subject withdraws consent;
- request the restriction of personal data;
- object to the processing of personal data if the personal data is processed in accordance with the lawful basis for processing referred to in Article 6(1)(a) and (f) of the GDPR (consent or legitimate interest);
- in cases where personal data is processed in accordance with the lawful basis for processing referred to in Article 6(1)(a) and (b) of the GDPR (consent or the conclusion and execution of the contract), obtain their personal data which the data subject has provided to the controller and transfer it to another controller or request RSU to transfer such personal data directly to another controller where this is technically feasible (right to data portability).

Rights of the Data Subject (natural person, including student)

The data subject completes the request in accordance with the Privacy Policy (available on the website Rīga Stradiņš University Privacy Policy | RSU and the requirements of laws and regulations in paper or electronic form, as well as using the application form (form LK - 20 “Data Subject’s Rights Request”), and submits it in paper form in person to the Records Management and Archives Department or to the official e-mail address of RSU rsu@rsu.lv, or via the portal Latvija.lv.

THANK YOU FOR YOUR ATTENTION