

**APPROVED**

Tallinn Health Care College
Rector's Order No 1-4/34 of
November 8, 2022

TALLINN HEALTH CARE COLLEGE'S PRIVACY POLICY

Current privacy policy was established in accordance with [General Data Protection Regulation](#) of the European Parliament and of the Council (hereinafter: *GDPR*) and [Personal Data Protection Act](#).

Tallinn Health Care College (hereinafter: College) is a state institution governed by the Ministry of Education and Research, which means that they are a holder of public sector information in respect of all their activities.

1. What are personal data, who is a data subject and what is processing of personal data?

- 1.1.** Personal data consist of any information about the data subject. E.g., person's name, national identification number, contact information, IP address of their computer etc.
- 1.2.** Data subject is a natural person identified or identifiable who personal data are being processed by the College, incl. learners of degree studies or continuing education, participant of a training or a conference, employee, service provider, homepage guest, applicants;
- 1.3.** Personal data processing means activities performed using these, incl. collecting, storing, using, changing, deleting it at Tallinn Health Care College.

2. General principles of personal data processing at the College

- 2.1.** The College values person's privacy and protection of personal data, and trust of the data subject.
- 2.2.** The College processes personal data to complete the tasks derived from legal acts.
- 2.3.** The College follows the principles set in Personal Data Protection Act and GDPR to complete the tasks derived from legal acts.
- 2.4.** All documents created or received in the course of the action of the College, are registered in document management system incl. documents containing personal data.
- 2.5.** The College prevents personal data they have access to, from unauthorised and inadequate use. Organisational, technical, and other measures are implemented by the College to secure personal data and ensure their legal processing. These are:
 - 2.5.1.** Information consisting of personal data is classified as information intended for internal use; access to it is restricted. Internal organisation is aimed to ensure the minimum infringement of your private life. Therefore, only these personal data are being processed, which are necessary to achieve the goals, and we allow access to the data only to authorised employees to complete their work-related tasks to the extent they need to;
 - 2.5.2.** Personal data are processed by the College in written form or in information system. The information system used for personal data processing and locations set to the

documents, their restrictions on access, and retention periods have been provided in the list of College's documents;

2.5.3. Access to the personal data is allowed by the College to the employees of the College with special training only, and they have the right to process personal data to the extent necessary to achieve the goals of personal data processing;

2.5.4. Regardless of the access restriction, the College will issue documents to those institutions or persons who have the legal right to claim the respective documents (courts, bailiffs, police officers and others with respective competences).

2.5.5. Personal data not needed by the College will be deleted, incl. due to expiry of the retention period.

3. Request for explanation, letter of formal notice, request for information and other exchange of letters

3.1. Activities of the College are public, therefore its actions result in personal data received, incl. sensitive and private information. These data may reach the College via exchange of letters. It is also possible if the person is a party of certain proceedings.

3.2. Personal data are used to reply to requests. If it requires requests from third person, the personal data are published to the minimum extent considering most necessary ones.

3.3. In case the College receives a request for explanation, letter of formal notice or a request for information, which should be replied in the field of the competency of another institution, the document will be transferred to this other recipient, and we will notify you about it.

3.4. Pursuant to [Public Information Act](#), the College's register of documents is public and published on College's website. It is essential to differentiate if the documents have access restrictions or not when using the register. The document having no access restriction can be accessed if to submit a request for information in case it is not published to the public view.

3.5. Exchange of letter with private persons has access restrictions and EKIS register of documents' public view demonstrates the initials of letter's sender or a recipient instead of their name only. If a request of information will be submitted to view exchange of letters with a private person, the contents of the letter will be reviewed by the College and it will be decided whether the document can be partially or fully issued. The issued document will be cleared of personal contact information, e.g., e-mail or snail mail address and a phone number (except if the exchange of letters is regarding the representative of a legal person or an institution). Access restrictions are depending on the contents of the document in all other cases. Basis for possible access restrictions is described in the Public Information Act.

3.6. Pursuant to subsection 6 in [Response to Memoranda and Requests for Explanations and Submission of Collective Proposals Act](#) a response to a memorandum or request for explanation shall be provided without undue delay but not later than within 30 calendar days after the date of registration thereof. Under special circumstances, the term may be extended to up to two months depending on the complexity of the response. The person shall be informed of extension of the term for response, and of the reasons for extension.

- 3.7. Data included in exchange of letters will be retained for five years since the request was submitted.
- 3.8. Documents with access restrictions are issued to these institutions and persons only that have a legal right to claim these (e.g., persons conducting pre-trial proceedings or the courts).

4. Applying for work at Tallinn Health Care College, processing of personal data in human resources

- 4.1. The vacancies at College will be recruited on the basis of an open application procedure and everyone has equal opportunities to apply.
- 4.2. The College's evaluation of applicants is based on information submitted by the applicant and their documents, if necessary, they can collect additional information about the applicant from public sources. The applicant has the right to view the collected information and submit their explanations and objections.
- 4.3. Only employers involved in recruit process may view the application documents (HR, future immediate superior, members of the Council in case of lecturers), and documents and data are not transmitted to third persons, except in cases pursuant to the law. It is expected by the College that a person referred to as someone to recommend them can be contacted without asking any further permission from the applicant.
- 4.4. Documents of unsuccessful applicant are retained for 1 (one) year with the aim to solve possible arguments and claims. After elimination of legal basis or achievement of data collection and use these will be destroyed.
- 4.5. HR processes personal data to complete financial and staff activities based on legal acts (Employment Contracts Act, Law of Obligations Act, Accounting Act and other state and College's regulations regulating accounting), and of obligations formed in contracts.

5. Processing of personal data of the employees and collaboration partners

- 5.1. Following personal data of College's employees and collaboration partners are processed by the College as a responsible collector on the basis of employment contracts and contracts following the Law of Obligation Act and other legal acts (e.g., tax-related laws, legal acts regulating employment, Accounting Act) and to fulfil obligations derived from these:
 - 5.1.1. Data to identify a person: first and last name, national identification code – if it does not exist the date of birth and citizenship;
 - 5.1.2. Contact information to sign and fulfil the contract (employment contract and contracts pursuant to the law of Obligation Act): e-mail, phone number and postal address;
 - 5.1.3. Family and social data, e.g., employee's vacation period depending on their children's data; death certificate of the employee or their close ones to pay funeral benefits; certificate about obligation to participate in service in defence forces or training gathering etc.;
 - 5.1.4. Data regarding qualification and further training;

- 5.1.5. Financial data, e.g., bank account number, application to account income tax free minimum and retirement information, data from bailiffs regarding seizure of salary;
- 5.1.6. Data regarding employment, such as documents of development evaluation; data of paid traineeship, mentorship and data sabbaticals of academic members of staff (Higher Education Act § 36);
- 5.1.7. Data of employee's health status, e.g., medical certificate, decisions of health check-up, data of occupational accidents and occupational diseases.
- 5.2. Personal data are processed by the College on a legitimate interest also to complete their administrative tasks and ensure safety (incl. registering employees' data in databases).
- 5.3. Personal data of staff member of the College are retained for ten years after termination of duties.
- 5.4. Data will be deleted, and documents destroyed after the end of retention period.

6. Personal data processing in management and administrative activities

- 6.1. The aim of collecting and processing personal data in management and administrative activities is to complete management and administrative duties based on legislation.
- 6.2. Only authorised employees of the College (based on work assignments) collect and process personal data. Retention period is based on legislation from the beginning of creation/receiving data until destruction/or storing for ever.

7. Personal data processing in application process for studies

- 7.1. According to the College's regulations for admission, highly motivated applicants are expected to study in College's specialties – ready to contribute to promote and develop the field of health care.
- 7.2. To apply to study the applicant will submit an application and other documents electronically via admission information system www.sais.ee (hereinafter SAIS) or on-the-spot in the College or on the basis on the agreement via international application system DreamApply. The applicant agrees to have their personal data processed via an application submitted in SAIS or at the College. You can read the scope and principles of personal data processed via application in SAIS on a website of admission information <https://sais.ee/ContentPages/Term>. You can find same principles about DreamApply on their website <https://dreamapply.com/terms/>.
- 7.3. Personal data of the applicant will reach SAIS based on national registries (population register, Estonian Education Information System (EHIS) and examination information system (EIS)) or these are entered into the system based on documents on paper submitted by the applicant or their information. The applicant agrees to have their personal data processed in SAIS in both cases, if they enter the data themselves or when these are entered by the College based on application online or on paper.
- 7.4. The College has a right to check the data by submitting requests of information to national registers. Also, the College may repeat the requests to check if the studies conducted at the time of submitting the application were completed or to update the name of the applicant based on their application in case it has changed. The College is allowed to check the validity and authenticity of the documents (e.g., international language certificates) from relevant registers and to submit personal data of a foreign applicant to check the qualification to Estonian ENIC/NARIC Centre, which is a

structural unit of Educational and Youth Board, incl. educational data based on applicant's agreement.

- 7.5. Aim of collecting personal data (name, date of birth, national personification code, gender, citizenship, contact information, education etc.) in studies and processing (data regarding study activities) is to conduct study activities.
- 7.6. Data are received from documents/data submitted by the person; documents related to the person (diplomas, certificates, supplements, certified statements); information systems (TAHVVEL), national databases (EHIS) and registers (eesti.ee).
- 7.7. Only authorised employees of the College (based on work assignments) collect and process personal data. Retention period is based on legislation from the beginning of creation/receiving data until destruction/or for ever.

8. Personal data processing in study activities

- 8.1. Aim of collecting and processing personal data in study activities is to organise studies and conducting it; and organising and completing study-related and study-supporting activities.
- 8.2. College's legal basis for personal data processing of the learners is its statutory obligation and/or a task carried out in the public interest (obligation to organise studies). Legal basis derives from national legal acts (e.g., Higher Education Act, Statutes of the College, Study Allowances and Study Loans Act, Vocational Act, Aliens Act), which completion is regulated by regulations (e.g., state scholarship regulation, diploma's and academic supplement regulation, statutes of EHIS) and College's legal acts (admission requirements and its appendixes, academic regulations, conditions for application, approval and payment of various scholarships and benefits, e.g., achievement stipend);
- 8.3. Learner's personal data are processed in several information systems: TAHVEL, document information system and other e-environments (e.g., Moodle, Office365, Mobility Tool, Vocational Registry).
- 8.4. As a responsible collector, the College processes via information system TAHVEL, incl. population register and other study-supporting information systems following personal data of degree study student/learner and external students:
 - 8.4.1. First name and last name, national identification code, date of birth, origin, citizenship and contact information. The main goal of processing these personal data derives from Higher Education Act (<https://www.riigiteataja.ee/akt/116062020009?leiaKehtiv>) and the processing is necessary to individualise the student/learner/external student, organise their studies, to create user account for the student/learner/external student in College's computer network and to issue academic documents. Also, to receive and send invitations to participate in College's research, collecting statistics and to forward vital information about College's organisations (student and learner council) and what is happening at the College (e.g., events);
 - 8.4.2. Earlier education info to organise studies, e.g., data of previous education, of higher education/vocational education to be completed (specialty and choices within it, form of studies and volume, begin and end date of studies), and of work experience;

- 8.4.3. To apply benefits, stipends, exemption of reimbursement of study fees and academic leave and data necessary to check the requirements, incl. financial data, e.g., bank account number, data of their family members and data of attending defence forces;
- 8.4.4. Personal data of special categories, included in certificates from medical institutions to apply for exemption of reimbursement of study fees, adjustments derived from special needs, reasons to have been absent on an exam; and application to approve academic leave and stipend applications.
- 8.5. User of information systems and e-environments can complement their user profile with voluntary data, which help to improve use friendliness of e-learning environments. Legal basis for processing these data is agreement by the user. The user has a right to change or delete these data at any time.
- 8.6. If a student/learner applies for benefits from persons outside the College (e.g., collaboration partners, benefit givers), or participates in projects financed and controlled by persons out of the College, the College will transmit data of the student/learner to these persons. In that case basis for personal data processing is student's/learner's agreement given at submitting the application and/or letter.
- 8.7. In case the student/learner completes their internship in a traineeship institution offered by the College, the College has the right to forward personal data of the student/learner necessary to complete the internship to the traineeship institution.
- 8.8. In case the College has legitimate interest, they can use contact data of the alumni to conduct surveys among alumni, to introduce options for further studies and to introduce alumni activities.
- 8.9. Retention period of personal data of students/learners is fifty years after graduation or exmatriculation. After the end of retention period the data will be deleted, and documents destroyed.

9. Processing personal data in continuing education

- 9.1. Participants of continuing education trainings are asked to provide their personal data by the College, incl. their name and national identification code derived from „[Adult Education Act](#)“ and „[Standard of Continuing Education](#)“. To send information about continuing education trainings, contact information (phone, e-mail) is asked for the registered person. In case the training requires paying fees, and the participant pays for it, data necessary to issue an invoice is asked (whose name, where to send etc).
- 9.2. Since several trainings are completed in the frameworks of projects, the participant is asked about their workplace in case required for paperwork.
- 9.3. Feedback collected of the trainings is anonymous and it is used for statistics. Personal data are not issued for unauthorised persons.
- 9.4. Depending on the category of the training, processing of personal data of the learner is based on either an obligation set in the law and/or a task completed in public interest.
- 9.5. Legal basis is derived from state legislation (e.g., Adult Education Act, Aliens Act), which completion is regulated by regulations (e.g., statutes of EHIS) and College's legal acts (e.g., Tallinn Health Care College forms of continuing education and conduction rules, academic regulations). In case of a fee-based training, the legal basis for personal data processing may be the separate contract signed by the learner.
- 9.6. If separate agreement is given by the learner, the College will use their e-mail to send information about any trainings organised by the College by adding the learner to the

relevant information list. The learner is allowed to delete themselves from the list using the link provided at any time;

- 9.7. If necessary, several information systems are used to process learner's personal data by the College: continuing education system Juhan, document administration information system and in e-learning environment Moodle.
- 9.8. Training materials consisting of personal data (e.g., attendance sheets) are retained according to the conditions set in projects and these are destroyed after achievement of goals of collected data.

10. Use of the Tallinn Health Care College Student Hostel

- 10.1. Personal data are processed by the College in case you would like to use College's Student hostel and you would like to sign an accommodation contract.
- 10.2. In case mentioned above your personal data will be processed by the College for following aims:
 - 10.2.1. To proceed the Student Hostel application and sign the accommodation contract;
 - 10.2.2. To follow the accommodation contract, if necessary, to change the contract;
 - 10.2.3. To check the accommodation contract and/or other and reasoned and necessary inquiries derived from the accommodation contract and for completion of it;
 - 10.2.4. To provide accommodation service, to transmit messages regarding accommodation services;
 - 10.2.5. To send invoices and for accounting;
 - 10.2.6. Communication with clients, incl. contacting to forward operative information;
 - 10.2.7. To complete obligations derived from legislation;
 - 10.2.8. To improve service;
 - 10.2.9. To protect their rights.
- 10.3. College's retention period for personal data derives from legislation or is reasoned to achieve the goals set in current document about the Student Hostel.

11. Visiting Tallinn Health Care College's website

- 11.1. Collected and stored data on visiting the website of the visitor are as follows:
 - 11.1.1. IP-address of the computer used or the computer network;
 - 11.1.2. Software version of computer's browser or operational system;
 - 11.1.3. Time of the visit (time, date, year).
- 11.2. IP-addresses are not linked to information identifying the person. The data are collected about, which parts of the website are being visited and how much time spent there. Collected data are used for visitors' statistics, which is the basis for development of the website and its improvement for more convenient use.
- 11.3. College's website is using permanent and session cookies to offer better user experience and to develop the website or we offer additional contents, e.g., videos, blogs, and instant messages. Cookies are little files downloaded to user's device by the websites, which the user is visiting. The goal of use of cookies is to distinguish the user from other people visiting the website and improve the user friendliness using the collected information.
- 11.4. Cookies may also be created by other outer service providers, which are used to improve our website (e.g., Facebook or Google).

- 11.5. Users are considered as agreed with cookies if their settings for websites have allowed to use cookies.
- 11.6. If you do not want the cookies to be recorded into your computer, you may block these in settings of your browser.
- 11.7. We point out that it is possible to visit College's website without accepting cookies, however, then certain services or parts of the website are not functioning as expected.
- 11.8. You should also notice that College's website may include links to other websites and the College is not responsible for data sharing in other websites and neither of privacy policy of these websites.

12. Video surveillance

- 12.1. When being in College's buildings, we ask to consider that there is a video surveillance working 24/7 at College's territory and buildings, incl. in Student Hostel. The data retention period is 3 (three) months, and one may view these in case of legitimate interest by submitting motivated application to the e-mail address info@ttk.ee.
- 12.2. Video surveillance is used as security measures by the College to prevent unauthorised persons from entering the workplace rooms without any reason; and to prevent situations threatening safety of College's staff members, learners and third parties; to ensure safety; to react in case of hazardous situations and to protect College's property.
- 12.3. Video surveillance is used to observe College's outside areas, entrance areas, halls and lobbies.
- 12.4. Corresponding signs inform about the use of video surveillance at College's premises or rooms.
- 12.5. To ensure security of data of video surveillance processed by the College, unauthorised access to observation equipment and video surveillance is prevented to eliminate the option for unauthorised monitoring, copying, changing, transmission and deletion of the recordings.
- 12.6. Observation equipment and video surveillance are accessed by staff members with special training only, who have the right to process personal data to the extent necessary to achieve the goals of personal data processing.
- 12.7. The College has the right to transfer collected data to law enforcement institutions and other state or local government institutions.
- 12.8. The College shall transfer the video surveillance recordings in case of proceedings for the infringement of the law only following legislation rules if the institution proceeding submits a request and in case the recordings exist.

13. Access system

- 13.1. The College and the Student Hostel are equipped with access system and necessary access cards (chips) to use the access system are issued after concluding contracts with the College (employment contract, under the law of obligation, housing contract or other relevant contract); or in case of learner after their matriculation.
- 13.2. Access system allows it user the access to the areas determined to them individually by their contract derived from their work tasks. Learners may access the lockers and the outer door can be opened by the card.

- 13.3. Only the employee authorised and trained by the College has the permission to access system and its logs, and to the extent necessary to achieve the goals of processing personal data only.
- 13.4. The College has the right to transfer data collected by access system to law enforcement institutions only in case of proceedings for the infringement of the law following legislation rules if the institution proceeding submits a request and in case the logs exist. Retention period for access system logs is for 30 calendar days.

14. Commemoration of events by taking photos and videos

- 14.1. College records their events if they organise these; or participates at events where it is ordered by the College to record the event by photos or videos. Photos and videos taken at public events by the College are property of the College and these are retained mostly for historical reasons and for an indefinite period.
- 14.2. Recorded photos and videos may be used by the College and if necessary to edit using every way, e.g., to use for advertisement or marketing campaigns and to publish in internal network of the College, on their website, social media or in public media without asking for a permission.
- 14.3. In case you participate in events organised by the College, you should consider that your personal data (e.g., image, voice) may be recorded. In case you do not want to be included in the recordings, you should inform the people performing the action beforehand.

15. Using the Library of Tallinn Health Care College

- 15.1. Your personal data will be processed by the College in case you would like to use its library, its means or register yourself as a reader.
- 15.2. Your personal data will be processed by the College's Library for following aims:
 - 15.2.1. To identify the reader;
 - 15.2.2. To provide public services, incl. to allow using databases and equipment and means of the library and to administer accounts of the clients, to answer enquiries and administer the reservations, for reminders after the deadline of the collection items has passed;
 - 15.2.3. Statistical analysis of the data;
 - 15.2.4. To ensure internal arrangements at library's territory, to prevent misuse of library's property and its protection; to ensure safety of the employees and other service users.
- 15.3. When registering as a reader the person will provide following data (in case the person is underage, younger than 18, then their parent or legal custody to have the right for borrowing the items):
 - 15.3.1. First and last name;
 - 15.3.2. National identification code;
 - 15.3.3. Place of residence (postal address);
 - 15.3.4. Phone number;
 - 15.3.5. e-mail.
- 15.4. One is registered as a reader based on valid identification document (ID-card) or any other identity document.

16. Transmission of personal data to third countries

- 16.1.** In case the College needs to complete their tasks by transmitting personal data to countries outside the European Union or territories equal to these, then pursuant to Data Protection Regulation No 45 for personal data they need to guarantee protection of personal data outside the borders of the EU at least on the same level as it is inside the borders of the EU.
- 16.2.** Personal data will be transferred to third persons and/or third countries by the College only derived from legislation, contract, agreement, or legitimate interest-based goals and to the extent by following all legal acts regulating data protection.
- 16.3.** In case the territory of the target country might have lower level of personal data protection than in force at the territory of the EU known to us, we will notify you of this given fact in a written form by e-mail; and you have the option to confirm either agreement to transfer your data or to forbid this action.

17. Rights of data subject

- 17.1.** Everyone has a right to inspect personal data collected of them by the College. The request to inspect personal data is denied if it may have following consequences:
 - 17.1.1.** Adversely affect the rights and freedoms of others,
 - 17.1.2.** Interfere crime prevention or catching a criminal,
 - 17.1.3.** Complicate the ascertainment of the truth in a criminal proceeding.
- 17.2.** Everyone has a right to demand correction or complementing of their incorrect personal data. One should submit an application signed digitally or by pen for that.
- 17.3.** If College has no legal basis to use personal data, the person has a right to demand the end of data use or data deletion. One should submit an application signed digitally or by pen for that.
- 17.4.** In case of questions regarding personal data processing and the use of person's rights, this person has a right and possibility to turn to College's data protection specialist via e-mail: andmekaitsespetsialist@ttk.ee.
- 17.5.** In case of receiving the request, the College has a right to ask the person to add the details, which information or which actions of personal data processing is the request more specifically linked to. The request will be answered in 30 days the latest since the date of receiving it. If there are complications, which require more time to answer the request, the deadline will be extended by the College for a reasonable delay and the person will be informed.
- 17.6.** In case you find that your rights on personal data processing have been violated by the College, or the way these are processed by the College are incompatible with legal acts regulating personal data processing, you have the right to turn to Data Protection Inspectorate (e-mail info@aki.ee, phone 627 4135) or to another competent institution, most of all to the domiciliary or employment competent monitoring agency.
- 17.7.** In case your permanent place of residence is located in another country of the EU, you will find contact information of the corresponding institution of the website of the European Data Protection Board (EDPB) (https://edpb.europa.eu/about-edpb/about-edpb/members_en - member-ee.)
- 17.8.** GDPR implementation within the administration of the Ministry of Education and Research can be read on the website of the [Ministry of Education and Research](#).

- 17.9.** The College has the right to change current privacy policy unilaterally at any given time.
- 17.10.** Current document is administered by College's data protection specialist.