APPROVED BY
Order of Kauno kolegija HEI Director
No. 1-594 of 20 December 2024

DESCRIPTION OF THE PROCEDURE FOR THE PROCESSING OF PERSONAL DATA AT KAUNO KOLEGJA HEI

CHAPTER I
GENERAL PROVISIONS

1. Description of the procedure for the processing of personal data at Kauno kolegija HEI (hereinafter referred to as Description) aims to regulate the processing of personal data at Kauno kolegija HEI (hereinafter referred to as Kauno kolegija or KK), ensuring the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation*) (hereinafter referred to as GDPR), *Law on the Legal Protection of Personal Data of the Republic of Lithuania* (hereinafter referred to as LPPD), in compliance with and implementation of the provisions of the *Labour Code of the Republic of Lithuania* and other legal acts regulating the protection of personal data.

2. The Description defines the objectives and principles of data processing, the rights of data subjects and the procedure for their implementation, the rights and obligations of the KK employees when processing personal data, organisational and technical means of data protection and other issues related to the processing of personal data.

3. The provisions of the Description are obligatory for all KK employees whose functions are related to the processing of personal data and other persons who, in the course of their duties and/or providing services to KK, become aware of personal data and are obliged to protect them.

4. Kauno kolegija processes the personal data of all KK community members - current and former employees, students, unclassified students and others who have provided information based on contractual and other legal relations as specified by law.

5. Kauno kolegija is the controller of all data collected during the collegial activities and internal administrative processes of KK, as well as the processor of personal data submitted by data subjects and third parties.

6. In performing their duties and processing personal data, employees of KK are obliged to comply with the basic principles of personal data processing and with the confidentiality and security requirements set out in the GDPR, the LPPD and this Description.

7. Key concepts:

7.1. **Personal data** is any information related to a natural person - a data subject (e.g. student, unclassified student, employee) - whose identity is known or can be identified, directly or indirectly, by reference to data such as name, surname, personal identification number, location data, an online identifier or to one or more factors specific to that person, such as his or her physical, physiological, psychological, economic, cultural or social features.

7.2. **Personal data breach** is a breach of security resulting in the unintentional or unauthorised destruction, loss, alteration, unauthorised disclosure, unauthorised access or unauthorised transmission, storage or other processing of personal data.

7.3. **Data protection officer** (hereinafter referred to as DPO) is an employee appointed by KK to perform the duties imposed on a data protection officer by the GDPR and the LPPD regarding data held and/or processed by the institution.

7.4. **Data recipient** is the legal or natural person to whom the personal data are provided.

7.5. **Data subject** is a natural person whose personal data is processed by the controller or processors.

7.6. **Data subject consent** is any freely given, specific and unambiguous indication of the data subject's will, provided by a duly informed person, through a statement or an unambiguous action, by which the data subject consents to the processing of personal data concerning him or her.

7.7. **Data provision** is the disclosure of personal data by transmission or otherwise making it available (other than publication in the media).

7.8. **Data processor** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

7.9. **Data processing** means any operation or set of operations which is performed upon personal data or sets of personal data, whether by automated or non-automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, access, use, disclosure by transmission, distribution or otherwise making available, alignment or combination with other data, restriction, deletion or destruction.

7.10. **Automated data processing** is the processing of data wholly or partly by automated means.

7.11. **Non-automated data processing** means processing operations carried out by non-automated means (processing of structured collections of personal data such as lists, files, records, catalogues and other documents).

7.12. **Data processing for statistical purposes** means conducting statistical research and providing and storing the results.

7.13. **Data controller** is a natural or legal person, public authority, agency or other body which, alone or together with others, determines the purposes and means of processing.

7.14. **Supervisory authority** means an independent public authority established by a Member State under Article 51 GDPR. In the case of the Republic of Lithuania, such authority is the State Data Protection Inspectorate.

7.15. **Profiling** is any form of automated processing of personal data which uses personal data to evaluate certain personal aspects related to a natural person, particularly, to analyse or predict aspects of that natural person's performance, economic situation, state of health, personal hobbies, interests, trustworthiness, behaviour, location or mobility.

7.16. **Specific categories of (special) personal data** are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data, health data, and data concerning the sexual life and sexual orientation of natural persons.

7.17. **Internal administration** is the activity that ensures the autonomous functioning of the controller (structure management, personnel management, management and use of available material and financial resources, and document management).

7.18. **Video surveillance** is the processing of image data relating to a natural person (hereinafter referred to as image data) using automated means of video surveillance (video and still cameras, etc.), regardless of whether or not the data are stored in a medium.

8. Other terms used in the Description shall be understood as defined in the GDPR and the Law on Electronic Communications of the Republic of Lithuania.

CHAPTER II
GENERAL PRINCIPLES AND TERMS FOR PERSONAL DATA PROCESSING

9. Employees and/or authorised people of Kauno kolegija HEI are obliged to comply with the following **general principles for the protection of personal data** when performing their duties and processing personal data (Article 5 of GDPR):

9.1. personal data shall be collected and processed accurately, fairly and for legitimate purposes as defined in the Description;

9.2. personal data of data subjects shall be stored in personal files, if created, and in relevant databases maintained by KK and service providers. Personal data must be accurate and, where necessary for the processing of personal data, kept up to date: the data's accuracy, currency and

completeness are of particular importance and are assessed according to the purposes for which they are processed. The updating of personal data is under the responsibility of the heads of the departments in which the personal data are processed, or their authorised staff. Data which are inaccurate, or incomplete are to be corrected, supplemented, destroyed or suspended;

9.3. personal data shall be collected at Kauno kolegija only under the procedure established by the legislation. Such data may be collected directly from another data controller, from the data subject, through official inquiries to the entities that process the necessary information and are authorised to provide it, or by accessing databases, registers and information systems that collect individual data based on contracts and legal acts. In some cases, the processing of personal data at KK shall be done with the consent of the data subject.

9.4. personal data must be identical, relevant and limited to the scope necessary for their collection and further processing. The processing of personal data shall be restricted to what is necessary to achieve the purposes of the processing set out in this Description.

9.5. personal data must be kept for no longer than is necessary for the purposes of processing. Personal data must be kept for as long as the documents or media containing the personal data are required to be kept by law or regulation. Personal data must be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes of processing.

10. The above principles must also be respected when drafting documents, i.e. avoiding the use of excessive data on natural persons, and their private or family life, unless the factual circumstances or the legal basis so require.

11. Personal data shall be processed at Kauno kolegija only on a lawful basis, in compliance with the GDPR, the laws of the Republic of Lithuania, and internal normative acts, as well as when the data subject has provided (given) his/her consent, or when the information about the processing of personal data is made available to all under the procedures established by Kauno kolegija.

12. Personal data may be processed at Kauno kolegija, by automatic or non-automatic means, only for the purpose for which they are collected. The processing of personal data shall be carried out to the minimum extent possible to fulfil a specific purpose. Personal data that are not accurate for the purposes for which they are processed shall be erased immediately. Personal data shall be processed and stored for no longer than the time limit laid down for their retention, which shall be no longer than is necessary for the purposes for which the personal data are processed unless otherwise provided for by law.

13. The processing of personal data shall be considered lawful if the **following conditions for the processing of personal data are complied with (Article 6 of GDPR)**:

13.1. the data subject has given consent to the processing of his or her personal data for one or more specified purposes. The use of the data subject's data, such as photographs, the use of his or her image in advertising, leaflets, etc., is only possible with the data subject's expressed consent. Consent is also required when providing information about persons attending or participating in KK events;

13.2. the processing is necessary for the performance of a contract to which the data subject is a party or to take action at the request of the data subject before the conclusion of the contract, i.e. where the processing is related to an existing employment relationship and/or recruitment, application for employment, studies at KK etc.;

13.3. the processing is necessary for compliance with a legal obligation to which KK is subject (e.g. to provide data and information about the data subject to public authorities);

13.4. the processing is necessary to protect the vital interests of the data subject or another natural person;

13.5. the processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority delegated to the data subject;

13.6. the processing is necessary for the legitimate interests of KK or of the third party to whom the personal data are provided, for the protection of KK and its assets, the security of technological processes, the health and safety of employees, internal administration, etc. For this purpose, video surveillance and security systems, IT controls, detection of intoxication and other

measures may be put in place to ensure the achievement of the aforementioned purposes (except where the interests of the data subject or his/her fundamental rights and freedoms predominate over the purposes of the processing, i.e. the right to privacy, hygiene, recreation, etc.).

13.7. If there is a need to process personal data based on consent (Article 13.1) or legitimate interest (Article 13.6), this must be coordinated with the DPO.

14. The processing of specified categories of personal data shall be prohibited unless at least one of the conditions set out in Article 9(2) of the GDPR is met.

15. Kauno kolegija HEI, as data controller:

15.1. ensure the implementation of the obligations of a personal data controller set out in the GDPR and other legal acts regulating the processing of personal data;

15.2. ensure that the DPO is involved in an appropriate and timely manner in all matters relating to the protection of personal data;

15.3. approving legislation on the protection and processing of personal data; determining the purposes and means of processing personal data;

15.4. ensuring staff training and professional development in the legal protection of personal data;

15.5. ensure that personal data are processed at KK only by those employees who need to process them for the performance of their job functions and only to the extent necessary for the performance of their job functions (need to know).

CHAPTER III
DUTIES AND RESPONSIBILITIES OF STAFF WHEN PROCESSING PERSONAL DATA

16. When processing personal data in their professional activities, the employees of Kauno kolegija shall:

16.1. process personal data lawfully, fairly and transparently;

16.2. collect personal data for the specified, clearly defined and legitimate purposes of KK and further process them only in a consistent manner with those purposes;

16.3. when collecting and processing personal data, respect the principles of purpose limitation, proportionality and data minimisation, i.e. not to require individuals to provide data that is not necessary for the performance of their functions, and not to collect and process excessive data and data that are not necessary for the achievement of the relevant purposes;

16.4. ensure the accuracy of personal data and, where necessary as a result of the processing of personal data, update, correct, supplement, delete or suspend the processing of inaccurate or incomplete data;

16.5. store personal data in compliance with the procedures set out in the legislation and in this Description;

16.6. process personal data adequately to ensure, by appropriate physical, technical or organisational measures, the security of personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage (integrity and confidentiality principle);

16.7. before each personal data processing operation (action), assess whether such personal data processing complies with the requirements of the principles set out in Article 5(1) of the GDPR, and evaluate whether such personal data processing has at least one of the conditions for the lawfulness of the processing of personal data set out in Article 6(1) of the GDPR, and ensure that personal data is not processed in the absence of at least one of the aforementioned legal grounds, and ensure that the processing of the personal data is carried out under one of the purposes established by Kauno kolegija HEI.

17. In processing personal data, the heads of Kauno kolegija’s departments and divisions shall:

17.1. ensure that personal data is processed in KK units and departments under the GDPR, the GDPR and other normative and legal acts of Kauno kolegija regulating data protection;

17.2. ensure that personal data is processed under organisational and technical data security measures designed to protect personal data processed against accidental or unlawful destruction, alteration, disclosure or any other unlawful processing;

17.3. systematically familiarise the staff of his/her division or department with the Description;

17.4. take responsibility for the preparation, registration and submission to the DPO of the documents necessary for the processing of personal data (orders, agreements, protocols, contracts, notices, etc.) under the procedures laid down by KK and the law (to implement the rights of data subjects);

17.5. ensure the destruction of electronic and/or paper documents containing personal data after the expiry of the storage periods set for personal data;

17.6. prepare and submit records of the data processing activities of KK DPO departments or divisions.

18. IT Development and Maintenance Unit of Kauno kolegija:

18.1. ensure the lawful processing of personal data and the implementation of the necessary technical data protection measures by implementing the information systems managed and/or maintained by KK;

18.2. establish and implement technical data protection measures for the information systems maintained by KK;

18.3. ensure that technical measures are in place to enable personal data to be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed;

18.4. ensure that personal data that are deleted from the information systems owned and/or maintained by Kauno kolegija are also deleted from the storage locations of backup copies (if any) of the KK information systems;

18.5. at least once a year, carry out impact assessments of the processing of personal data in the KK information systems and consult with the DPO on these issues;

18.6. supervise the compliance of data processors with the requirements specified in their contracts.

19. In the internal documents of Kauno kolegija HEI, the personal identification number of the data subject may be processed only under the requirements established by the legislation or in agreement with the DPO.

CHAPTER IV
DATA PROTECTION OFFICER

20. The DPO is responsible for the data processing activities conducted at Kauno kolegija HEI within his/her competence. Kauno kolegija, as the data controller, shall ensure that the DPO does not receive any instructions regarding the performance of personal data processing tasks entrusted to him/her, and shall not assign tasks and duties that may give rise to a conflict of interest.

21. Data protection officer:

21.1. informs and advises the controller or processor and the data processing staff of their obligations under the GDPR and other data protection provisions of the European Union or a Member State on the following matters.

21.2. monitors compliance with the GDPR, other European Union or national data protection provisions and the controller’s or processor’s policy on personal data protection, including the delegation of responsibilities, awareness-raising and training of staff involved in data processing operations and related audits.

21.3. on request, provides consultation on and monitors the data protection impact assessment in respect of Article 35 of the GDPR;

21.4. cooperates with the supervisory authority, the State Data Protection Inspectorate;

21.5. acts as a contact person for the supervisory authority about questions concerning data processing, including prior consultation as referred to in Article 36 of the GDPR, and provides consultation on all other matters as necessary;

21.6. assists in the development of documents and procedures in line with the requirements of the GDPR;

21.7. monitors, as necessary, the compliance by employees and other processors of personal data under the control of Kauno kolegija with the personal data processing obligations set out in this Description and the processing of personal data;

21.8. submits proposals and conclusions to the KK management on the establishment of data protection and data processing measures;

21.9. gives direct instructions to staff, if necessary, to rectify breaches of the processing of personal data;

21.10. ensures that records of data processing activities are kept and updated;

21.11. decides on the need for data protection impact assessments. The Data Protection Officer shall, if necessary, seek preliminary consultations with the State Data Protection Inspectorate;

21.12. informs the data subject and the State Data Protection Inspectorate of a personal data incident in the prescribed cases;

21.13. ensures the secrecy or confidentiality of his/her tasks in compliance with the requirements specified in the legal acts of the European Union and the Republic of Lithuania;

21.14. conducts a risk assessment of the processing of personal data and draws up a report;

21.15. performs other tasks and duties assigned to the DPO by the legislation.

CHAPTER V
PURPOSES OF PROCESSING PERSONAL DATA

22. Personal data shall be processed at Kauno kolegija HEI for the following purposes:

22.1. *Alumni career monitoring and Alumni Club activities* - the following data is processed for alumni and Alumni Club members: name, surname, higher education institution, study programme, start and end date of studies, telephone number, email address, work experience (workplace, position) and other personal data voluntarily provided by the alumnus.

22.2. *Academic staff individual work activity planning and planned activity implementation records* - academic staff name, title, planned annual activity, travel, internship and other planned work activity data of the academic staff member, and activity implementation report data are kept.

22.3. *Administration of dormitory accommodation services, establishment, execution and management of accommodation contracts* - name(s), surname, personal identification number, date of birth, gender, place of residence and contact details - street, house number, apartment number, settlement (post office), city/municipality, country, telephone number, email address, signature, nationality, social status, study programme (for students), the form of study (for students), year of study (for students), student status (for students), start and end date of reservation, country of origin, employer, family status, financial obligations and settlement periods, fact and circumstances of violation of the established procedure, periods of arrival and departure.

22.4. *Conducting surveys* - the name of the person taking part in the survey, survey responses, email address, and telephone number.

22.5. *Handling of complaints, requests, appeals and petitions from persons* - name(s), surname, telephone number, e-mail address, signature, date and number of the complaint, request or petition (date and number of registration in KK document management system), information (including specific personal data) contained in the complaint, request or petition, result of the handling of the complaint, request or petition, information received during the handling of the complaint, request or petition, date and number of the response to the complaints, requests or petitions.

22.6. *Auction conducting* - name, surname, email address, telephone number, position, legal entity represented, number of individual activity certificate or business license, business location,

date of validity, bank and current account details, lists of goods to be purchased under the contract, commitments, signature.

22.7. *Library readers and visitors' services* - the name, surname, address (data of residence and/or declared place of residence - street, house number, apartment number, settlement, city, municipality, country), telephone number, e-mail address, personal identification number, date of birth, signature, photograph, student ID number, employee's position, library visitor's ID.

22.8. *Collection, storage, monitoring and accounting of library resources* - name(s), surname, personal identification number, e-mail address, telephone number; student ID number, faculty, course, study programme of staff, students and other persons who visit the KK library.

22.9. *Employment contract, administration of employment relations* - name(s), surname, nationality, address, personal identification number, date of birth, gender, photograph, signature, marital status, signature, number of dependents and dates of birth, the fact of single parenthood, details of disability, details of the right to drive, details of education and qualifications, duties, functions, changes of duties and dates, amounts of salary and social security contributions, dates of public insurance, details of participation in pension schemes, current account number, telephone number, e-mail address, curriculum vitae and activities, job title, details of recruitment (transfer), dismissal, length of service, post to which the person wishes to be appointed or transferred, staff identification number in table, details of education and qualifications, pedagogical titles, identification code in the register of academics, date of entry/change of data, details of holidays, their timing and location, details of secondments, internships, their timing and location, details of individual work schedules, details of teleworking and the place of work, working conditions, compensation, working time arrangements, details of remuneration, allowances, compensations, benefits and the reasons for their payment, information on working time worked, information on incentives and penalties, breaches of service or professional duties and/or ethics, data on performance appraisal of employees, data on declaration of public and private interests, special categories (specific) of data relating to the health of the person, passport and/or identity card number, date of expiry, previous employment and position, former surname, systematised lists of tools and instruments issued for the work, dates of expiry of the driving licence, dates of expiry of the insurance against civil liability in respect of personal motor vehicles, other personal data supplied by the person himself.

22.10. *Salary and grant award and payment* - employee/student name, surname, personal identification number, bank and current account details, amount and date of payment, and number of deductions.

22.11. *Occupational health and safety, accident investigation* - name, date of birth, personal identification number, job title, signature, place of work and functions performed, results of briefings and training, facts of the accident and results of the investigation.

22.12. *Surveillance and monitoring of electronic communications flows* – based on a legal obligation, users' actions in information systems are automatically recorded in action logs.

22.13. *Financial settlements and debt collection* - name(s), surname(s), personal identification number, telephone number, current account number (for natural persons - beneficiaries), residential address, e-mail address, fact and amount of debt, fact of debt collection.

22.14. *Information about studies and/or scientific, art and project activities implemented at Kauno kolegija HEI and other activities of members of KK and its community* - photo(s) and/or video(s), name, surname, group (for students), workplace (for third parties), position (for employees of KK/ third parties).

22.15. *For authentication of information systems for user account management and identification* - name, surname, student ID number (for students), position (for staff), e-mail address, institution (work or study), personal identification number, e-mail address, telephone number, student's faculty, group of studies, year of study, dates of entry into force and expiry of work and study contracts, data on password recovery, IP and MAC address of the computer, the date and time of accessing the system or website, cookies, session and other information from the activity records.

22.16. *Organisation and administration of the public competition and selection procedures for posts* - name(s), surname(s), curriculum vitae and the data contained therein - photograph, personal telephone number(s), e-mail address, current and former places of employment, date of birth, institution of study (current or former), position, degree and other personal data provided voluntarily by the candidate.

22.17. *Election and registration of members of the governing bodies of Kauno kolegija HEI* - candidates' and members' names, surnames, personal identification numbers, date of birth, residential address, telephone number, e-mail address, educational qualifications, employment details, data relating to social activities, signature, facts concerning impeccable reputation, criminal convictions, dismissal for serious breaches of professional discipline, conduct incompatible with ethical principles and academic values. Date of appointment/election, position, telephone number, e-mail address, expression of the will to take decisions, signature.

22.18. *Administration of the KK arts groups and/or athletes/sports teams* - staff and students' names, surnames, email addresses, telephone numbers, date of birth, programme of study, year of study, faculty, photographs, audio-visual recordings, facts about the sport, achievements.

22.19. *Organisation and execution of conferences and other events* - name, surname, signature, personal telephone number(s), current account number (for natural persons - payers), personal email address, workplace, date of birth, institution (work or study) of employees, students and third party participants, Institution (work or study), position, degree, e-mail address, the language of writing, abstract of the thesis or dissertation in English and Lithuanian, status of online access to the thesis or dissertation, date of restriction, date of publication, data used for identification of the person who carried out the matching check, attendance figures, results;

22.20. *Organising and carrying out secondments (including internships)* - staff name, email address, phone number, job title, location, dates and report.

22.21. *Communication with employees and/or students/unclassified students, alumni, contractors' representatives, community and/or public* - name, surname, telephone number, email address, position, legal entity represented, of the employee and/or student/unclassified student, alumnus, and the contact person named in the event of a disaster.

22.22. *In-service training and competency development* - staff and student name, title, competency level and fact of need, date and time of training, location, topic, and results.

22.23. *Administration of the research (and art) process* (to establish authorship of scientific output, to record and evaluate the results of the scientific (and art) activities of staff and students, to carry out graduation procedures at Kauno kolegija HEI, to complete and submit documentation) – name, surname, personal identification number, personal telephone number(s), personal e-mail address, place of work, date of birth, signature, institution (work or study), department of the institution (work or study), type of study (for students), academic group (for students), the start date of the study (for students) of the investigators and authors date of completion of studies (for students), position, degree (for staff), date of commencement of the thesis or research project, date of completion and/or defence of the thesis or research project, the language of the thesis or research project, the topic of the thesis or research project, the topic of the thesis or research project in English, the abstract of the thesis or research project in both Lithuanian and English, the responsibilities of the participants in the defence process and the data used for identification, the online access status of the thesis or research paper, the restriction period, the date of publication, the attribute of the thesis or research paper that has been subject to the match check, the impact of the match check, the data used for identification of the person who has carried out the match check, and the thesis or research paper documents.

22.24. *Contracting and execution of applied research, experimental development, and art activities (hereinafter referred to as R&D), recording and publishing the results of staff members' scientific (and art) activities, and publishing scientific (and art) and other works* - data from academics, students and stakeholders: name, surname, degree (for staff), e-mail address, signature, position (for staff), institution (work or study), personal identification number, date of birth, topic, title, date of production, date of writing, language of writing, topic, abstract, access status of the

scientific work on the Internet, date of publication, text match checking and results, type of study (for students); academic group (for students), institution (work or study), field of research (work or study), research papers, contribution.

22.25. *Non-formal education service provision* – participants' name, surname, date of birth, education/training institution/workplace, the content of the educational service, educational outcomes, and details of the certificate issued.

22.26. *Organising of the tender for the lease of the property* - name, surname, e-mail address, telephone number, position, legal entity represented, number of individual activity certificate or business certificate, place of business, date of validity, details of bank and current account, lists of premises to be leased under the contract, commitments, signature.

22.27. *Project development and implementation* - name, surname, address, e-mail address, telephone number, workplace, job title, faculty, study group, personal identification number, home address of staff, students, project participants, partners and/or their representatives and other interested parties.

22.28. *For marketing purposes* - name, surname, and e-mail address of employees, students, and third parties.

22.29. *Distribution and organisation of various events* - photo(s) and/or video(s) of staff, students, third parties, name, group (for students), workplace (for third parties), position (for KK staff/third parties), date of the event, fact of attendance, signature, details of the certificate issued.

22.30. *Establishing, execution and administration of contracts (other than employment, study, professional internship, accommodation, R&D contracts)* - name, surname, email address, position, date of birth, details of the representation document, bank account number, details of residence or declared residence, contractual obligations and rights, details and expiry date of the documents authorising the relevant business activity, other data generated during the execution of the contract, signature.

22.31. *Student papers and final thesis publications* – students' name, surname, e-mail address, workplace, position, faculty, study group, final thesis, language of writing, topic, abstract, online status, date of publication, text matching check and check results.

22.32. *Conclusion, administration and execution of admissions and study agreements* - name, surname, personal code, date of birth, gender, nationality, type of personal document, indication of whether they have a permanent residence permit, telephone number, email address, declared/residential address, priority of preference, faculty, national code of the study programme, name of the study programme, study programme title, study form, source of funding, competition score calculated under either the Competition Queue Procedure or the School's rules, name of the school where secondary education was obtained, country, year and language of secondary education, code and name of the school where the vocational qualification was obtained, code and name of the school where the higher education studies were completed, name and year of the qualification obtained in higher education, and the higher education institution, name of the higher education institution in which he/she is currently studying, the indication of whether he/she is paying for the studies in which he/she is presently studying, choice of foreign language for future studies, series, number, bank code and date of issue of the matriculation certificate, series, number of the supplement to the matriculation certificate, fact of the length of service in the occupational qualification, the fact of having performed military service, the information about having limited work capacity, having been placed under guardianship, the death of the parent.

22.33. *Individualisation of studies and adaptation of the environment to individual needs* – students' name, surname, date of birth, academic department, study programme, course, group, the fact of disability, level of incapacity for work, long-term physical and/or mental and/or intellectual and/or sensory impairment, the fact of behavioural and emotional, speech and language impairment and learning difficulties which may hinder their ability to study at the same level as other persons, their individual needs, the date of commencement and end of the personalisation of the study process.

22.34. *Organisation of studies and recording of study results* - name, surname, ID number, type of ID, residence and contact details - street, house number, apartment number, settlement (post

office), city/municipality, country, telephone number, email address, signature; additional data for students coming on exchange programmes (nationality, dates of expiry of entry visa, English language proficiency data (certificates), arrival/departure data); length of employment, social status (membership of a disadvantaged group), military service, education data (school code, name, type, year of graduation, country), details of studies (a form of study, faculty, programme, year of study, semester, group, student status (student, unclassified student), type of funding, amount and year of the voucher, student certificate number, subjects taken, duration of studies, study withdrawals, the form of payment, date, grades of study achievements, place, time and feedback on the placement, time and place of Erasmus+ trips abroad and arrival/departure data (copies of tickets), other diploma data, thesis documentation, the significance of the thesis matching check, identification numbers given to the student, bank account number, contributions and/or payments made, their amounts and dates, type, series, number, expiry/issue date of documents issued to the student, health data - the fact of illness.

22.35. *Social network administrating* - messages sent by employees, students and third parties (in favourite posts, posts shared by the person, posts commented on by the person), marked to attend events, messages sent to KK by the person's account, comments under the KK posts, reactions to the KK posts, photographs of the KK posts, certificates on the KK posts, certificates to attend KK posts and the KK posts shared by persons.

22.36. *Organising international staff and student mobility* - name, surname, former surname, email address, telephone number, personal identification number, date of birth, photograph, nationality, work plan, bank account number, signature, start and end of participation in the mobility programme, amount of funding and grant awarded and payment arrangements, duration of the visit, fact of compliance/non-compliance with the funding agreement, results and period of mobility, field of study, academic group, level of English or other foreign language, start and end of participation in the mobility programme, income of family members, fact of belonging to a disadvantaged group, orphan status, having young children and age of children, being a member of a large family, starting date of employment as a working student, refugee status, having a residence permit for humanitarian reasons in Lithuania, the fact of a disability which results in additional costs in the mobility activity, the fact of participation in and results of the mobility selection, the academic performance, the student's motivation, the student's ability to integrate the opportunities offered by the study abroad into his/her studies at KK and his/her further academic plans; the student's communication skills and his/her readiness for intercultural experiences; special needs for studies, the doctor's report on special needs and the date of its submission; the amount and timing of the funding and/or scholarship granted; the fact of complying/not complying with the funding agreement; the results of the study and/or internship in the foreign higher education institution or company and the period of time.

22.37. *Management of available material and financial resources* - name(s), surname, nationality, address, personal identification number, date of birth, gender, photograph, signature, marital status, signature, number of dependants and dates of birth, amounts of wages and social security contributions, dates of public insurance, pension contributions, current account number, phone number, e-mail address, curriculum vitae and activity description, job title, details of recruitment (transfer), dismissal, length of service, post to which the person wishes to be appointed or transferred, staff identification number in the table, details of education and qualifications, pedagogical titles, identification code in the register of academics, date of entry/amendment of data, data on leave, secondments, internships, individual working hours, teleworking, working time arrangements, salaries, allowances, benefits, compensation, payments, information on working time, information on incentives and penalties, offences of misconduct in public office or in the course of employment, data on performance appraisals, declarations of public and private interests, special categories (specific) of data relating to personal health, passport and/or identity card number, date of expiry, previous employment and position, former surname, systematised lists of tools and instruments issued for work, dates of expiry of driving licence, dates of expiry of personal motor vehicle liability insurance, other personal data provided by the person himself.

22.38. *Admission of foreign students* – applicants' and students' names, surnames, e-mail addresses, telephone numbers, date of birth, date of place of residence and/or declared place of residence, citizenship, social status, bank account number, education, data of place of residence, planned and actual period of stay in Lithuania, conditions and period of issuing a visa, fact and period of issuing a residence permit in Lithuania, signature.

22.39. *Executing of public procurement* - name, surname, e-mail address, telephone number, position, number of the certificate of individual activity or business licence, place of business, date of validity, bank and current account details, income from the contract, liabilities, details of documents proving education and qualifications, or copies thereof, and signature of the tenderers and their representatives, contractors, and their representatives.

22.40. *Controlling public order, property protection, transport and access* (ensuring the safety of staff, students and other persons visiting Kauno kolegija and the security of the KK property) - name(s), surname, signature, security camera videos and photos. Security cameras shall be used to record courtyards, entrances to KK buildings, common areas, and areas of concentration of network or engineering system equipment (server rooms, communication nodes, building management system control panels, laboratories, etc.).

23. If there is a need to process personal data for a purpose other than that for which the personal data were collected, or if such a purpose is not provided for in this Chapter, approval of the DPO shall be obtained.

CHAPTER VI
RECORDS OF DATA PROCESSING ACTIVITIES

24. Kauno kolegija HEI maintains records of its data processing activities in the form approved in this Description (Annex 2 to the Description). Records of data processing activities shall be correct, up-to-date and complete and must reflect KK's actual data processing activities.

25. Records of data processing activities shall be kept in electronic form.

26. The DPO is responsible for keeping a record of processing activities.

27. Employees shall inform the DPO without delay if the prepared records of data processing activities do not correspond to KK's actual need to process personal data, by submitting a form (Annex 2 to the Description) for data processing activities.

CHAPTER VII
PROCESSING OF PERSONAL DATA

28. Personal data shall be processed at Kauno kolegija either automatically or in structured collections.

29. Data from social profiles or similar sources shall not be collected or processed.

30. Kauno kolegija, in compliance with the requirements set out in the Description and GDPR, inform data subjects about the processing of personal data (Annex 1).

31. In some cases, personal data shall be processed at KK with the consent of the data subject (e.g., when providing necessary information in the event of a disaster or an accident or the like, as well as when processing special categories of (specific) data, when the data subject's image is used in advertisements, information leaflets, etc.).

32. The direct collection of personal data from the data subject must be preceded by the notification referred to in Article 30.

33. Persons who have provided information about themselves to apply for employment at Kauno kolegija (e.g. submission of a CV) shall be informed that the personal data they have provided may be processed for the administration of candidates, and if the person agrees to the storage and processing of his/her data for that purpose, the data provided by him/her shall be processed under the procedures set out in this Description.

34. The Human Resources Unit keeps the data of applicants for a post for 3 months from the date of receipt. If at the end of the selection process for a given position Kauno kolegija does not

select a candidate and does not conclude a contract of employment with the candidate, all personal data collected for the selection process shall be securely destroyed, unless consent for data processing for administration of the candidates is obtained.

35. Personal data relating to the qualifications, professional abilities and professional qualities of an applicant for a post or job may be collected from the former employer/state and municipal bodies where the applicant performs his/her civil service or employment contract, with the previous information of the applicant, and from the current employer/state and municipal body where the applicant performs his/her civil service or employment contract, only with the applicant's consent.

36. Kauno kolegija shall not process or record additional personal data provided by candidates about themselves, which is irrelevant to the recruitment.

37. Kauno kolegija shall not process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data for specific identification of a natural person, health data or data concerning a natural person's sexual life and sexual orientation. This restriction shall not apply where one of the following conditions exists:

37.1. the data subject has expressly consented to the processing of such personal data for one or more of the specified purposes, except where the processing of such data is mandatory by law or regulation;

37.2. when an alternative option for providing personal data is available;

37.3. when processing is necessary for the fulfilment by Kauno kolegija or by the data subject of legal obligations and the exercise of special rights in the areas of employment and social security, insofar as this is permitted by regulatory provisions or by a concluded collective agreement, which provides for measures to protect the fundamental rights and interests of the data subject;

37.4. processing of personal data which the data subject has made public;

37.5. when processing is necessary for preventive or occupational medicine, for the assessment of the employee's fitness for work, or the provision of health care services, based on a contract with a health care institution;

37.6. when data processing is necessary for archiving, research or statistical purposes, as well as in other cases provided in the GDPR or the laws of the Republic of Lithuania.

38. Kauno kolegija HEI may process only those personal data of employees which are necessary for the conclusion and performance of an employment contract or other contract concluded with an employee, for the fulfilment of KK legal obligations under the law, and the protection of KK's specific legitimate interests. The purposes of employees' data processing are set out in the records of processing activities.

39. Kauno kolegija is forbidden to process the personal data of employees that are not related to their work and the exercise of their rights (excessive), as well as to disclose the employee's data to third parties, except in the cases stipulated by the laws and this Description.

40. A staff member may use a computer, e-mail and other KK equipment, devices, appliances, information and communication technologies, and software provided for the performance of his/her job functions only for work-related purposes and only for the performance of his/her job functions. Employees are prohibited from using computers, telephones and other equipment, devices, devices, information and communication technologies, and software provided by KK for personal purposes, to store information of a personal nature and personal data on them. If an employee uses computers, telephones and other equipment, devices, appliances, information and communication technologies, and software provided by KK for personal purposes, and stores personal information and personal data on them, the employee assumes the risk that such information and personal data may become known to KK during the inspection. Kauno kolegija does not ensure the confidentiality of employees' personal information when using email, internet, social networks and software for personal purposes.

41. Internet services may also be used for personal purposes (use of social networking sites, personal tax and bank transfers, e-mail service, instant messaging for personal purposes, etc.), insofar as this does not interfere with the optimal and efficient performance of job duties.

42. Constant monitoring or checking of the computer, e-mail and other devices, appliances, equipment, information and communication technologies, and software provided to an employee of

Kauno kolegija is prohibited. Work tools, equipment, including e-mails, computers, mobile phones, personal data, other data and information provided to the employees of KK may be inspected only under the following conditions:

42.1. the staff member is informed of the possibility of the inspection;

42.2. there are grounds for assuming that the staff member has committed a breach of his/her employment duties or has engaged in activities incompatible with the interests of Kauno kolegija or has engaged in activities contrary to the law, or KK seeks to verify that the staff member has complied with his/her obligations to Kauno kolegija, or has duly complied with the requirements of the law, including KK internal documents, or there are any other valid reasons justifying such a verification;

42.3. it is not feasible to achieve the inspection objectives by other means that are less intrusive on the employee's privacy.

43. The verification set out in this Description is limited in scope, i.e. a specific period for which the verification is to be carried out, the verification of the execution of a specific project, the verification of the execution of specific functions, and the verification is to be carried out only in so far as it is necessary to clarify the circumstances set out in this Description and to protect KK's interests. The Data Protection Officer shall provide counselling to ensure that the inspection does not infringe on the provisions of the GDPR, the Description provisions and the right to privacy of data subjects.

44. Video surveillance may be carried out at the workplaces of employees only where the nature of the work makes it necessary to ensure the safety of persons, property or the public, and in other cases where other ways or means are inadequate and/or inappropriate for the purposes set out above, except for the direct purpose of controlling the quality and scope of work. Video surveillance at a specific location shall be indicated by a visual marking in a visible place.

45. When processing video data in the workplace and in the premises or areas of Kauno kolegija where its employees work, when processing personal data relating to monitoring the behaviour, location or movement of employees, such employees must be informed of such processing of their data in a manner which demonstrates the fact of being informed.

46. Where personal data concerning a data subject have been obtained indirectly from the data subject, the data subject must be informed in compliance with the procedure set out in Article 30 within 30 days of the first day of processing of his or her data. Where the intention is to transmit the personal data to third parties, the data subject must be informed at the latest before the data are first communicated, unless the data subject is already in possession of such information, or the transfer of the data is provided for by other legal acts. The information must be provided to the data subject in writing, either directly, by registered post or by electronic means which allows the data subject to be identified and to obtain acknowledgement of receipt of the information, ensuring that access can be evidenced.

47. The data subject has the right, in the cases provided for in the GDPR, to object to the processing of his or her data by a third party by informing the DPO about his or her decision.

48. In the cases and according to the procedure established by the legislation, Kauno kolegija HEI shall provide the personal data of the data subject to the Ministry of Education, Science and Sports of the Republic of Lithuania, the Ombudsman for Academic Ethics and Procedures of the Republic of Lithuania, the State Tax Inspectorate of the Republic of Lithuania, the Special Investigation Service of the Republic of Lithuania, the State Security Department of the Republic of Lithuania, among others, but not limited to, the State Social Insurance Fund Board of the Republic of Lithuania, the National Cyber Security Centre of the Republic of Lithuania, the Communications Regulatory Authority of the Republic of Lithuania, and other third parties upon request (in the case of a single collection of personal data) or according to a contract for the provision of personal data (in the case of multiple collections of personal data), or according to a contract for the processing of data.

49. Personal data shall be provided to data recipients located in the Member States of the European Union and other countries of the European Economic Area under the same conditions and procedures as to data recipients located in the Republic of Lithuania.

50. Personal data processed or intended to be processed following a transfer to a third country or an international organisation shall only be transferred if the controller and the processor comply with the GDPR.

51. When a written data agreement is concluded between Kauno kolegija and a data processor, the data processor is bound to ensure the implementation of appropriate organisational and technical measures to protect personal data against accidental or unlawful destruction, alteration, disclosure or any other illegal processing.

52. The protection measures the data processor applies to protect personal data must comply with the requirements set out in KK's security documents.

53. Kauno kolegija may, following the provisions of the GDPR, process the personal data collected for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

54. The time limits for the storage of personal data and the actions to be carried out after the expiry of this time limit shall be determined by the legal acts regulating the processing of personal data. Personal data shall not be kept for longer than required by the purposes of the processing and/or the General Index of the Republic of Lithuania for the storage of documents. The specific time limits for the storage of personal data (documents containing personal data) are laid down in Kauno kolegija’s documentation plan. Personal data processed by automated means shall be stored for the periods laid down in the internal legal acts of KK. When personal data are no longer required for their processing, they shall be permanently destroyed, except for those personal data which must be transferred to the New Archives of the State of Lithuania in cases specified by law. The timely destruction of the data shall be the responsibility of the staff who process the personal data.

55. Departments must, in compliance with the requirements of Kauno kolegija’s legislation, destroy unnecessary data (documents containing personal data or copies thereof) which have not been collected automatically in such a way that the information contained therein is not identifiable, and must destroy data collected automatically by deleting the unnecessary files of personal data from the storage medium in such a way that they are not capable of reproduction.

CHAPTER VIII
DATA SUBJECTS' RIGHTS AND THEIR ENFORCEMENT

5.6. Data subjects have the right to:

56.1. to receive information about the processing of their data;

56.2. have access to their data and how they are processed;

56.3. to request the correction or, taking into consideration the purposes of the processing of the personal data, the supplementing of personal data which are incomplete (right of rectification);

56.4. to have their data destroyed or to stop the processing of their data, except for storage (right to destruction and right to be forgotten);

5.7. to require the controller to restrict the processing of personal data (right of restriction);

5.8. to request the transfer of his or her data, where such transfer is reasonable and technically feasible, where the request is for the transfer of personal data processed by Kauno kolegija by automated means (right to transfer);

56.7. to object to processing certain optional personal data where the data subject's objection is legally justified.

57. The controller may exclude data subjects from the exercise of these rights when, in cases provided by law, it is necessary to ensure the prevention, investigation and detection of criminal offences, breaches of official or professional ethics, as well as the protection of the rights and freedoms of the data subject or other persons.

58. Data subjects have the right to directly contact the heads of the structural divisions of Kauno kolegija HEI and/or the DPO in all matters related to the processing of data subjects’ data and the rights of data subjects provided for in the GDPR, the LPPD and other related legislation.

59. The data subject has the right to know from what sources and personal data have been collected, for what purpose they are processed, and to which recipients they are provided and have been provided in 1 year.

60. The data subject has the right to have personal data concerning him or her deleted by KK without delay, provided that one of the following grounds applies:

60.1. the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

60.2. the data subject withdraws the consent on which the processing is based according to Article 6(1a) or 9(2a) of the GDPR and there is no other legal basis for the processing;

60.3. the data subject objects to the processing under Article 21(1) of the GDPR and there are no overriding legitimate reasons for the processing, or the data subject objects to the processing under Article 21(2);

60.4. the processing of personal data was unlawful;

60.5. the personal data must be deleted in compliance with a legal obligation imposed by the law of the European Union or a Member State to which the controller is subject;

60.6. the personal data were collected in the context of the offering of information society services referred to in Article 8(1) of the GDPR.

61. Kauno kolegija provides the data requested by the data subject to the data subject free of charge once per calendar year. In other cases, the data is provided in compliance with the service fees approved by the order of the Director.

62. If the data subject, having familiarised himself/herself with his/her data processed by KK as provided in the response, finds that his/her data are incorrect, incomplete or inaccurate, and applies to KK for their correction, the DPO suspends the processing of such personal data, except for the storage of such personal data, and, after checking the personal data, takes measures within 5 working days at the latest to rectify the incorrect, incomplete, inaccurate data, and provides a response to the data subject informing him/her about the steps taken.

63. If the data subject, having familiarised himself/herself with his/her data processed by Kauno kolegija as provided in the reply, finds that his/her data are being processed unlawfully or improperly and contacts Kauno kolegija, the data the DPO verifies the accuracy, lawfulness and integrity of the processing of the personal data at the latest within 5 working days, and takes measures to promptly destroy the unlawfully and improperly collected personal data or to suspend the processing of the personal data, except for the storage of the personal data, and informs the data subject of the actions taken.

64. If the data subject, after familiarising himself or herself with the processing of his or her data by Kauno kolegija as set out in the response, finds that further processing of his or her data is inappropriate and withdraws his or her previous consent to the processing of the data and asks KK to forget it, the DPO takes measures to delete the personal data processed by the data subject based on the consent, except for the storage, and informs him or her of the steps taken or of the reasons for the impossibility of the deletion.

65. When Kauno kolegija has made publicly available the personal data of a data subject but is obliged to delete the personal data at the request of the data subject, the DPO takes reasonable steps, taking into account the technology used by KK and the cost of implementation, including technical measures, to ensure that such personal data and/or copies or duplicates of such personal data are destroyed without delay.

66. The requirements to forget and delete personal data are not applicable in cases where the reasons listed in Article 52 of the Description cannot be substantiated and, in the cases, provided for in Article 17(3) of the GDPR, including when:

66.1. Kauno kolegija is subject to legal obligations which require it to process data or for the performance of a task carried out in the public interest;

66.2. for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in complying with the GDPR and other legal requirements;

66.3. in other cases, provided for in the GDPR and other legislation.

67. Kauno kolegija, having suspended the processing of personal data at the request of the data subject, shall keep the personal data for which processing has been suspended until they have been rectified or destroyed (either at the request of the data subject or after the expiry of the data storage period).

68. The data subject has the right to submit a complaint to the State Data Protection Inspectorate against Kauno kolegija's actions (inaction).

69. The data subject has the right to claim compensation for material and non-material damage caused to him/her by Kauno kolegija because of unlawful processing of personal data (inaction).

70. The data subject shall submit a written request to the DPO of Kauno kolegija (Annex 3) on all matters related to processing his/her data and exercising his/her rights.

71. Requests or complaints by current and former employees of Kauno kolegija, and other data subjects shall be submitted to the Legal and Document Management Unit of KK directly, as well as by registered mail or by electronic means of communication that allows for proper identification of the person (e.g., by qualified electronic signature).

72. Current and former students and/or unclassified students of Kauno kolegija shall submit requests or complaints to the academic division of KK that handles the data subject's data, as well as by registered mail or by electronic means of communication that allows for the proper identification of a person.

7.3. The request must be legible, signed, containing the data subject's name, surname, address and other contact details for the form of communication requested, and indicate which of the data subject's rights, and to what extent, are sought to be implemented.

74. The data subject may exercise his or her rights only after Kauno kolegija has had the opportunity to verify his or her identity. The identity of the data subject shall be verified in one of the following ways:

74.1. by coming to KK and presenting proof of identity with the request to exercise rights;

74.2. in compliance with the procedures established by law or employing electronic means of communication that allow proper identification of the person (e.g. by a qualified electronic signature). When submitting a request or a complaint to KK's offices, the data subject shall be obliged to show a personal identification document to the staff member receiving the documents.

75. The staff member who receives the request or complaint must verify the identity of the person.

76. When sending the request by registered mail, the data subject shall submit a copy of a personal identity document certified by the notary, equivalent or simplified procedure as provided for in the Civil Code of the Republic of Lithuania and other legal acts. The envelope shall bear a note that the correspondence is addressed to the DPO of Kauno kolegija.

77. The data subject may exercise his/her rights himself/herself or through a representative authorised by a certified public notary or the Register of Authorisations.

78. If a representative of a person applies on behalf of the represented data subject, he/she shall indicate in his/her application his/her name, surname, place of residence, contact details, as well as the name, surname, place of residence of the represented person, the information on which of the data subject's rights referred to in the Description and to what extent the data subject wishes to exercise them and shall attach a document confirming the representation, or a copy of his/her document, certified following the procedure provided for by law. The request submitted by the representative shall comply with the same requirements as those of the person represented.

79. In case of doubt as to the identity of the data subject, the controller shall request additional information necessary to verify it.

80. All requests and complaints from data subjects regarding the processing of personal data, as well as the responses to them, must be recorded in Kauno kolegija Document Management System.

81. A request or complaint from a data subject that is not submitted following the requirements established in this Description shall not be examined unless the DPO decides otherwise. The DPO shall inform in writing the person submitting the request or complaint of the grounds for refusal to examine the request or complaint.

82. Requests and complaints from people shall be answered in the state language and in the way in which the request or complaint was submitted unless the person wishes to receive an answer in another way.

83. If necessary, a request or complaint may be answered in a language other than the state language when the request is made by a foreign authority, other foreign entity or international organisation in compliance with international law.

84. The DPO or another person authorised by the KK Director shall coordinate the preparation of the response to the request or complaint, advise the divisions, and provide the response to the data subject.

85. The reply to the data subject shall be signed by the DPO or another person authorised by the KK Director.

86. Replies to a request shall be based on the content of the request:

86.1. request for a document or a copy, transcript or extract thereof, shall be responded to by providing the service requested or by stating the reasons for the refusal;

86.2. the complaint shall be answered by informing the person of the circumstances investigated or by stating the reasons for refusal to do so;

86.3. a request for information held by Kauno kolegija shall be answered by providing the requested information in line with the procedure established by the Law of the Republic of Lithuania on the Right to Obtain Information from State or Municipal Institutions and Bodies or the reasons for refusal shall be indicated;

86.4. a request from a person stating his/her views on a particular matter, informing him/her of deficiencies in KK's or its divisions' performance and suggesting how to improve them, drawing attention to a specific situation, telling him/her of staff abuse or unlawful acts not involving a violation of the legitimate interests and rights of a particular person, or any other request from a person, shall be responded to in a free form letter.

87. The reply to the request or complaint shall be clear and well-reasoned, indicating all the circumstances relevant to the handling of the request or complaint and the specific provisions of the legislation relied on in considering the content of the request or complaint.

88. The reply stating the reasons for refusing to provide the service or information requested shall inform the person or his representative of the procedure for appealing against such a reply, indicating the name(s) and address(es) of the body(ies) to which the appeal may be submitted, and the time limit(s) within which an appeal may be made. In the case of a transfer of the application or complaint to another competent authority and informing the person or his/her representative thereof, the notification to the person need not specify the abovementioned appeal procedure.

89. Information on personal data processing issues not contained in the information systems maintained by Kauno kolegija shall be collected by the KK divisions processing the data subject’s data and shall be submitted to the DPO not later than within 14 (fourteen) calendar days from the date of the data subject’s request.

90. The response to a request or complaint from a data subject concerning the processing of his or her data shall be provided free of charge within 30 calendar days from the date of the request, except in the cases and under the terms and conditions provided for in the GDPR and other legislation, including Article 12(3) of the GDPR, where, depending on the complexity of the request and the number of other requests, that period may be extended by an additional 2 months.

91. The employee dealing with the request or complaint shall remove himself/herself from the examination of the request or may be removed by the decision of the Director or his/her authorised representative if the data subject submits a request or complaint related to the activities of Kauno kolegija’s employee processing the personal data, or if specified circumstances occur:

91.1. the employee is a close relation (as defined in the Civil Code of the Republic of Lithuania), a brother-in-law or a cohabitee of the person who is the subject of the investigation;

91.2. there is a subordinate relationship between the staff member and the person making the request or complaint;

91.3. the impartiality of the staff member is reasonably doubtful on any other grounds which may give rise to a public-private conflict of interest.

92. Copies of the personal documents received in connection with a data subject's request or complaint shall be destroyed within six (6) months from the end of the investigation of the complaint. Complaints, requests and documents relating to their processing shall be kept for 1 (one) year and shall be destroyed after the expiry of the retention period, in compliance with the procedure established by law.

93. Documents containing personal data or copies of those documents on external data storage media or in electronic mail shall be deleted as soon as they have been used and/or transferred to storage facilities, but at the latest within five (5) working days after the request or complaint has been met.

94. Documents containing personal data or copies of those documents must be destroyed in such a way that they cannot be reproduced and the contents identified.

95. In handling requests and complaints, KK staff must be guided by the principles of respect for human rights, justice, fairness and common sense.

96. Kauno kolegija may provide processed personal data to third parties only in the cases and according to the procedure established by laws and other legal acts. A written request from third parties shall specify the purpose of using personal data, the legal basis for the provision and receiving of personal data and the scope of the personal data requested.

97. Requests made by telephone, electronic or other means by third parties not authorised by law to provide them with information about Kauno kolegija’s students/unclassified students (e.g., requests made by parents of students regarding the results of their children’s studies) shall be answered with a statement that no information is provided.

CHAPTER IX
SECURITY MEASURES

98. To ensure the protection of personal data, Kauno kolegija shall implement appropriate organisational, technical and software security measures to protect personal data against accidental or unlawful destruction, alteration, disclosure or any other unlawful processing.

99. KK employees shall have the right to collect, process, transmit, store, destroy or otherwise use personal data only in the performance of their direct functions as defined in their job description or on the instructions of their immediate manager, and only following the procedures specified by law. Staff members shall not intentionally collect, process, transmit, store, destroy or otherwise use personal data.

100. Access rights to personal data and the mandate to process personal data shall be granted, terminated and amended in compliance with the procedures established by the order of the KK Director or the Staff Regulations.

101. The KK staff shall sign an obligation to respect the principle of confidentiality and to keep secret any information relating to personal data of which they become aware in performing their duties, except where such information is public according to the provisions of applicable laws or regulations. The principle of confidentiality also implies that persons processing personal data are prohibited from disclosing them, except with the consent of the data subject, where the data subject has made the data public, where necessary to prevent or investigate a criminal or unlawful act, where necessary to prevent or investigate a criminal or unlawful act, or where the personal data are necessary for a judicial procedure.

102. The Head of Human Resources of Kauno kolegija shall ensure that staff members sign an obligation to protect the confidentiality of personal data (hereinafter referred to as the Commitment) (Annex 4). This Commitment shall be valid upon termination of the employment or contractual relationship or transfer to another post. The Commitment, signed by each staff member, shall be kept together with his/her employment contract.

103. Personal data (documents containing personal data or copies of them) shall be stored in special premises, locked cabinets or safes, local network areas and on computer hard drives. Personal data (documents containing personal data or copies of them) shall not be kept in a visible place accessible to all, where unauthorised persons may have unhindered access to them.

104. Staff members shall have access only to those documents and files they have been authorised to handle, make them available only to authorised persons, and use them to perform their direct duties and only when necessary to achieve the objectives specified in the Description.

105. Employees must prevent the accidental or unlawful destruction, alteration, disclosure or any other unauthorised processing of personal data by storing documents properly and securely, keeping them out of public view, and avoiding unnecessary copying.

106. If a staff member or other person has doubts about the reliability of the security measures in place, he/she shall write to the Head of Division or the Data Protection Officer, who shall instruct the responsible staff of the Information Technology Development and Maintenance Unit to assess the security measures in place and, if necessary, initiate the acquisition and implementation of additional measures.

107. Kauno kolegija shall ensure the proper placement and maintenance of technical equipment, compliance with fire safety rules, proper network management, maintenance of information systems and the implementation of other technical measures necessary to ensure the protection of personal data.

108. Personal data are processed automatically in Kauno kolegija at the second level of security - organisational and technical measures for the security of personal data are ensured by KK and by data processors who process personal data in an automated mode and who have access to them via external data networks.

109. The following hardware and software security measures shall be implemented at Kauno kolegija, including but not limited to:

109.1. Kauno kolegija’s fixed and portable computers on which personal data and/or confidential information may be stored shall be protected by a password of at least 8 characters consisting of upper and lower case letters, numbers and special characters (!, @, #, $, %, ^, &, etc.). For example: L^ba$1du.3 (do not use this password);

109.2. the password must be changed at least every 60 calendar days;

109.3. computer screensavers must automatically switch on when the user is inactive for more than 5 minutes and require a password to return to the computer;

109.4. laptop hard drives (HDD, SSD) and external storage media (USB sticks, external HDDs and SSDs) that may store personal data and/or confidential information must be encrypted using the BitLocker software, which is supported by Microsoft operating systems;

109.5. mobile phones and tablets (smart - with Android or MAC operating systems) must have the ESET Endpoint security for business antivirus software installed on them, and the employee must contact the Information Technology Development and Maintenance Department for installation and activation. In addition, unlocking the screen of service mobile devices must be PIN protected (a graphical template is not appropriate) and, if the technical capabilities of the device allow, fingerprint scanning must be enabled for unlocking the device; facial recognition for unlocking is not appropriate;

109.6. employees who work with personal data and use the kaunokolegija.lt account provided by KK on mobile phones or tablets are also subject to the requirement specified in Article 109(5);

109.7. files containing personal data and/or confidential information must be shared with staff authorised to process personal data using Google Drive tools or by sending an encrypted email with the code key in a separate email;

109.8. data stored on the computer (potential personal data, desktop, documents and other relevant directories) must be synchronised with Google Drive or an alternative cloud technology to prevent data loss;

109.9. Kauno kolegija’s website www.kaunokolegija.lt shall limit as far as possible the possibility for publicly available internet search engines and search engine robots to copy the

information contained on the website and shall limit as far as possible the possibility for these search engines and robots to find copies of information that has been previously published on KK's website, but which has been removed from KK's website. Computer equipment shall be protected against malicious software (installation of anti-virus programs, updates, etc.);

109.10. controlling access to personal data through organisational and technical personal data security measures that record and control registration and authorisation efforts;

109.11. the number of failed connections allowed to the information system is determined;

109.12. the following logins to personal data are recorded: the author of the logon, date, time, duration, and the result of the logon (successful, unsuccessful). These records shall be kept for at least 1 year;

109.13. the purpose(s) for which the personal data is used shall be indicated in the search request;

109.14. the use of secure passwords when personal data is transmitted over external data networks is ensured;

109.15. it is ensured that personal data contained in external data storage media and emails are controlled and deleted after use;

109.16. for remote working or study sessions, the wireless network (Wi-Fi) used at the employee's and/or student's workplace must be password protected (not open to everyone).

110. For assistance in implementing these measures, staff members should contact the IT engineer in their division or the Information Technology Development and Maintenance Unit staff, or email itpagalba@go.kauko.lt.

111. To install ESET Endpoint security for business anti-virus for mobile devices Article 109(5), department staff should contact the Information Technology Development and Maintenance Unit.

112. At least once a month, a designated staff member or other responsible person shall make a copy of the data file on the computers. In the event of loss or damage to these files, the staff member shall contact the ITD and the Maintenance Unit. They shall be restored within two working days by the staff responsible for the ITD and the Maintenance Unit.

CHAPTER X
PERSONAL DATA BREACH MANAGEMENT PROCEDURES

113. Staff members with access rights to data must inform their immediate manager and the DPO if they become aware of any breach of data security (omissions or actions by individuals that could lead to or cause a risk to the security of data).

114. Having assessed the risk factors of a data breach, the degree of impact of the breach, the damage and the consequences of the breach, and in line with the Procedure for Responding to Personal Data Breaches (Annex 6), the responsible staff shall decide on the measures necessary to remedy the breach and its consequences.

CHAPTER XI
DATA PROTECTION IMPACT ASSESSMENT

115. In cases when, considering the category of personal data and data subjects, the nature, scope, context, purposes of the processing, the rights and freedoms of the data subjects may be at significant risk, Kauno kolegija shall perform a data protection impact assessment of the planned processing operations before the data processing operations (actions) and processing of the data are undertaken.

116. The data protection impact assessment is performed when:

116.1. the data processing operation is included in the list of data processing operations subject to the requirement to conduct a data protection impact assessment, approved by the Order of the Director of the State Data Protection Inspectorate of 14 March 2019 No 1T-35 (1.12.E) *On*

Approval of the List of Data Processing Operations Subject to the Requirement to Conduct a Data Protection Impact Assessment (hereinafter referred to as List of Data Processing Operations), which are subject to the requirement of conducting a data protection impact assessment;

116.2. the processing operation is not included in the List of Processing Operations for which the requirement of a data protection impact assessment is mandatory, however, KK assesses that the processing operation is likely to result in a significant risk to the rights and freedoms of data subjects in the light of the criteria specified in Article 117 of the Description;

116.3. when the conditions for the implementation of the processing operations/activities have changed and this may result in a serious risk to the rights and freedoms of data subjects;

116.4. in other cases provided for in this Description.

117. Every time, the following criteria are considered to determine whether processing operations/actions are likely to result in a serious risk to the rights and freedoms of data subjects:

117.1. systematic monitoring of personal data or data subjects;

117.2. sensitive data or highly personal data, such as specific categories of personal data, are processed on a large scale;

117.3. large-scale processing (number of data subjects involved, amount of data processed, variety of data processed, duration and regularity of processing activities, geographical scope of processing);

117.4. linking and combining datasets;

117.5. data relating to vulnerable data subjects (e.g. data relating to children, employees, sensitive subjects in need of special protection, and other segments where an unequal relationship between the data subject and the controller can be established);

117.6. applying new technologies or organisational solutions;

117.7. the processing prevents data subjects from exercising their rights, accessing services or entering into contracts;

117.8. other circumstances indicating a possible serious risk to the rights and freedoms of the subjects.

118. The more criteria specified in Article 117 of the Description are met by a specific processing operation (operations), the more likely it is that the processing operation (operations) may pose a serious risk to the rights and freedoms of data subjects. The DPO shall be consulted in all cases on the necessity of a data protection impact assessment.

119. If a data processing operation/activity meets two or more of the criteria outlined in Article 117 of the Description, but it is concluded that such data processing operation/activity is unlikely to result in a serious risk to the rights and freedoms of data subjects, such decision and the reasoning shall be expressed in writing and shall be communicated to the Director of Kauno kolegija, or the person designated by him/her, together with the opinion of the DPO;

120. A data protection impact assessment must be conducted before the implementation of processing operations/actions.

121. The DPO shall be responsible for initiating and organising the data protection impact assessment upon receiving information about a new processing operation from the Head of the KK division(s) which will process the personal data. External consultants, specialists, and experts (lawyers, IT specialists, security experts, ethics experts, etc.) may be used to perform the data protection impact assessment if Kauno kolegija’s human and time resources are insufficient to perform a proper data protection impact assessment.

122. After completing the data protection impact assessment, the person or persons who conducted the data protection impact assessment shall complete the data protection impact assessment report form. A single data protection impact assessment may be carried out to examine a sequence of similar high-risk processing operations.

123. If it is feasible in the light of the nature of the envisaged processing operation, Kauno kolegija shall seek the opinion of the data subjects or their representatives on the envisaged processing, without prejudice to the protection of commercial or public interests or the requirements of the security of the processing operation.

124. The data protection impact assessment report shall be submitted to the Director of Kauno kolegija HEI.

125. Kauno kolegija carries out a regular review to assess whether the processing is conducted in compliance with the data protection impact assessment, in cases where there are changes in the risks to the rights and freedoms of data subjects caused by processing operations.

126. Kauno kolegija HEI, before initiating data processing operations (actions) that may pose a serious risk to the rights and freedoms of data subjects, must consult with the Inspectorate in the cases set out in Article 2 of the Rules for Provision of Prior Consultations, approved by the Order of the Director of the State Data Protection Inspectorate of 29 August 2018 No 1T-84(1.12.E) *On Approval of the Rules for Provision of Prior Consultations* (amended by the Order of the State Data Protection Inspectorate of 3 September 2020 No 1T-88(1.12.E)).

127. Processing operations which are likely to result in a serious risk to the rights and freedoms of data subjects may be implemented only if Kauno kolegija fully and properly implements the recommendations, instructions and measures of the Inspectorate received during the consultation procedure.

128. Where the scope, nature, context and purpose of the processing are very similar to the processing for which a data protection impact assessment has been conducted, it is possible not to reassess the data protection impact, but to make use of the data protection impact assessment conducted for similar processing.

CHAPTER XII
FINAL PROVISIONS

129. This Description establishes, including but not limited to, the personal data security measures that should be taken when processing personal data. To ensure a higher level of data protection, Kauno kolegija HEI may take additional protective measures.

130. The basic technical and organisational measures for processing personal data and for the implementation of the data subject's rights using the information systems and databases operating at KK shall be specified in the regulations of these systems, data security regulations and other legal acts.

131. Heads of Divisions and Units are responsible for the protection of personal data and the lawful processing of personal data within their structural units.

132. Recruits shall be given a signed briefing on the Description by the Human Resources Officer. Heads of Units shall ensure that all staff under their authority are constantly aware of and familiar with the amendments and additions to this Description.

133. Employees who do not comply with the provisions of the Description, if the State Data Protection Inspectorate detects violations of the GDPR, the LPPD and/or other legal acts regulating the protection of personal data, shall be held liable following the procedure established by the laws of the Republic of Lithuania.

134. Non-compliance with the provisions of this Description may, depending on the seriousness of the violation, be considered a breach of labour obligations, for which the employees may be liable to the penalties provided for in the Labour Code of the Republic of Lithuania.

135. The Description shall be reviewed and updated at least once every 2 years or in the case of changes in the legislation governing the processing of personal data.

136. The Description may be supplemented, amended or abolished by an order of the KK Director.

137. The Labour Council of Kauno kolegija has been informed about this Description and consulted on adopting this document.

138. The Description shall enter into force when approved by an order of the Director and shall be published on the Intranet within two working days at the latest.

139. The following Annexes (document templates) are attached as an integral part of the Description:

139.1. Personal Data Processing Information (Annex 1).

139.2. Records the Data Controller's Processing Activities (Annex 2).
139.3. Request to Enforce Data Subject's Right(s) (Annex 3).
139.4. Commitment to Personal Data Protection (Annex 4).
139.5. Consent to the Image Use and Processing of Personal Data (model) (Annex 5).
139.6. Procedure for Responding to Personal Data Breaches (Annex 6).
139.7. Register of Personal Data Protection Breach (Annex 7).

_____

Annex 1
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

PERSONAL DATA PROCESSING INFORMATION

This document explains how the Public Enterprise of Kauno kolegija (hereinafter referred to as **Kauno kolegija** or **KK**) processes the personal data of ..... (hereinafter collectively referred to as the **data subjects**), which Kauno kolegija receives from ..... .

The personal data of the data subjects are processed in compliance with the *General Data Protection Regulation* (EU) 2016/679 (hereinafter referred to as the **GDPR**), the *Law of the Republic of Lithuania on the Legal Protection of Personal Data*, other legal acts, and the *Description of Procedures for the Processing of Personal Data at Kauno kolegija HEI* (hereinafter referred to as the Description) (www.kaunokolegija.lt).

From the moment of signing the contract, this document becomes an integral part of the contract _____ *(when required).*

Data Controller	*Kauno kolegija Higher Education Institution, code 111965284, address Pramonės pr. 20, Kaunas, tel. (+370 37) 352325, email info@go.kauko.lt (hereinafter referred to as Kauno kolegija or KK)*
KK Data Protection Officer	..... (name, surname, tel. no.) email: dap@go.kauko.lt.
The purpose of personal data processing	*One or more of the purposes specified in the Description shall be indicated*
The scope of personal data processed by Kauno kolegija	*For example.* *For the performance of the contract, Kauno kolegija processes the contact and personal data of the other party that are required to be provided for the performance of the contract, such as name, surname, personal identification number, residential address, telephone number, and e-mail address.*
Kauno kolegija processes the data for the following purposes	*For example.* *(a) to enter a contract with a contractor and to perform its obligations under that contract; (b) to comply with applicable law; (c) to maintain a relationship with a contractor, including the marketing of services; (d) to defend against legal or other claims, or to enforce the rights of Kauno kolegija.*
Legal basis for processing personal data	*One or more of the grounds referred to in Article 6 of the GDPR are indicated*
Data source	*For example.* *Kauno kolegija receives the above personal data from the other party to the contract at the time of conclusion and performance of the contract.*
Recipients of personal data and their categories	*For example.* • *Data centre and cloud computing service providers;* • *software providers and maintainers of software;* • *professional advisors, auditors;* • *notaries, if the contract with you requires a notarial*

	form; • *the Public Registry Centre, if the contract, legal facts or other information related to the contract are required to be registered in public registers;* • *bailiffs, entities providing legal and/or debt recovery services, entities that take over the right to claim the debt; managers of joint debtors' data files* • *competent public authorities;* • *the Ministry of Education, Science and Sport of the Republic of Lithuania.*
Period of storage of personal data	*For example.* *Personal data is retained for no longer than is necessary for the purposes for which it was collected or for the period required by law (one of which is the General Index on the Retention of Documents).*
Enforcement of data subjects' rights	*The data subject shall have the right to request Kauno kolegija:* • *to have access to personal data processed by KK (Article 15 of the GDPR);* • *rectification or deletion (Articles 16, 17 GDPR);* • *restrict the processing of personal data (Article 18 of the GDPR);* • *submit a complaint to the State Data Protection Inspectorate (for more information, see www.vdai.lrv.lt).*
Procedure for appealing against the actions (inactivity) of Kauno kolegija	*The processing of the data subject's data by Kauno kolegija as a data controller may be subject to a complaint by the Data Subject to the State Data Protection Inspectorate*

***** *Law on the Legal Protection of Personal Data of the Republic of Lithuania*

** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC (*General Data Protection Regulation*)

_____

Annex 2
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

RECORDS OF THE DATA CONTROLLER'S PROCESSING ACTIVITIES

<table>
<tr><td colspan="4">Data Controller: Kauno kolegija</td></tr>
<tr><td>Postal address:
20 Pramonės Ave.,
LT-50468 Kaunas</td><td>Telephone number:
+370 37 352324</td><td>E-mail address:
info@kaunokolegija.lt</td><td>Other means of communication:
https://www.kaunokolegija.lt/</td></tr>
<tr><td colspan="4">Data Protection Officer:</td></tr>
<tr><td>Postal address: 20 Pramonės Ave., 1-010, LT-50468 Kaunas</td><td>Telephone number:</td><td>E-mail address:
dap@go.kauko.lt</td><td>Other means of communication:
–</td></tr>
<tr><td colspan="4">Purpose of data processing (e.g., recruitment, direct marketing, personnel administration, and ensuring property security (in the case of video surveillance).</td></tr>
<tr><td colspan="4">Description of the categories of data subjects (e.g., employees, persons entering the video surveillance field, students, etc.). In the case of several groups of data subjects, the personal data processed for each group of data subjects (including specific categories of personal data) shall be indicated separately if the data processed are different.</td></tr>
<tr><td colspan="4">Description of the categories of personal data (e.g., name, surname, date of birth, address, image data, salary records, health data, phone records, IP address, etc.).</td></tr>
<tr><td colspan="4">Categories of recipients (recipients to whom personal data have been or will be disclosed or otherwise transferred, including recipients in third countries or international organisations).
(e.g., insurance companies, courier services, banks, etc.)</td></tr>
<tr><td colspan="4">Transfers of personal data to a third country or international organisation (when applicable):</td></tr>
<tr><td colspan="2">Name of the third country or international organisation to which the personal data are transferred:</td><td colspan="2">Documentation of appropriate protective measures in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR:</td></tr>
<tr><td colspan="4">Other information regarding the transfer of personal data:</td></tr>
<tr><td colspan="4">Time limits for storage, and deletion of personal data (when possible) (e.g., 10 years after the performance of the contract, 30 calendar days, 1 year after the last access to the system, etc.)</td></tr>
<tr><td colspan="4">General description of the data security measures (referred to in Article 32(1) of the GDPR) (where possible):</td></tr>
</table>

Technical safety measures: *(e.g., the software is kept up to date, equipped with firewalls and anti-virus, data backups, data encryption, etc.).*	Organisational safety measures: *(e.g., limiting and controlling the rights of users of information systems and databases, imposing statutory duties of confidentiality on those working with personal data, etc.).*
Other information *(e.g., data sources, the legal basis for processing, staff/departments responsible for processing, specifics on the exercise of the data subject's rights, references to other documents related to data protection (e.g., data protection impact assessment, internal rules of procedure, etc.).* **Legal basis -** **Data source(s) -** **Documents regulating the right/obligation to process PD -** **Use of profiling -**	
List of structural divisions processing the data	
List of data processing staff	
Date(s) of data entry, and modification:	

Annex 3
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

(Name and surname of the data subject[1])

(Address and/or other contact details (telephone number or e-mail address (to be provided at the applicant's request)

(Representative and the basis for the representation, if a representative requests the data subject)[2]

_____ (Name of the Data Controller)

REQUEST TO ENFORCE THE DATA SUBJECT'S RIGHT(S)

_____
(Date)

_____
(Place)

1. I request the enforcement of the following right(s) of the data subject: (Please tick the appropriate box with a cross):

- ☐ The right to receive information about processing
- ☐ The right of access to data
- ☐ The right to have the data rectified
- ☐ The right to have the data deleted (right to be forgotten)
- ☐ The right to restrict the processing of data
- ☐ The right to data portability
- ☐ The right to object to the processing of data
- ☐ The right to request that a decision based solely on automated processing, including profiling, is not applied

2. Please specify what you are specifically requesting and provide as much information as possible to enable the proper exercise of your right(s) (*e.g., if you are requesting a copy of the personal data, please identify if you wish to have your data rectified, please indicate which of your data is inaccurate; if you object to the processing of your data, please state the grounds on which you base your objection and the specific processing to which you object; if you are requesting the exercise of the right to data portability, please specify in respect of which data you wish to exercise this right, whether you*

[1] More data may be requested to determine whether the data subject's data are being processed, such as the controller's data subject code, etc.

[2] If the request is made by a representative of the data subject, it must be accompanied by a document certifying the representative's authority.

wish to transfer it to your device or another controller, if the latter, then please indicate to which controller):

_____

SUPPLEMENTED BY[3]:

1. _____

[3] If the request is sent by post, it shall be accompanied by a copy of the identity document certified by a notary or other legal procedure. If the application is for rectification of inaccurate data, copies of the documents proving the accuracy of the data shall be provided; if sent by post, they shall be certified by a notary or other procedure established by law. If the data subject's personal data, such as name, surname and forename, have changed, they shall be accompanied by a copy of the documents confirming the change; if sent by post, they shall be certified by a notary or other procedure established by law.

Annex 4
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

COMMITMENT TO PERSONAL DATA PROTECTION

_____
(date)

_____
(place of conclusion)

I, _____ ,
(name, surname)

_____ ,
(job title)

I confirm that I am familiar with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data. Repealing Directive 95/46/EC (*General Data Protection Regulation*), the Law of the Republic of Lithuania on the *Legal Protection of Personal Data*, the description of the procedure for processing of personal data at Kauno kolegija HEI, and other legal acts regulating the protection of personal data, and I promise:

1. To keep personal data secret throughout the employment/contractual relationship and after the employment/contractual relationship has ended unless such personal data are intended to be made public.
2. To process personal data only for legitimate purposes.
3. To keep personal data accurate and, where necessary, to keep up to date, correct or supplement inaccurate or incomplete data and/or to suspend the processing of such personal data.
4. To process personal data only to the extent necessary for its processing and for the performance of its function (including by not retaining copies of the processed data unless required by applicable law).
5. To process personal data in such a way that the data subjects can be identified no longer than necessary for the purposes for which the data were processed, and subsequently to delete such data.
6. To implement the provisions of legislation on the protection of personal data, which provides for the protection of personal data against unlawful processing or disclosure.
7. Not to disclose, transfer or make available by any means any information processed, including passwords allowing access to personal data, to any person who is not authorised to use such information, whether inside or outside Kauno kolegija.
8. To report to my immediate supervisor any suspicious situation that could jeopardise the safety of personal data.
9. To ensure the implementation of the data subject's rights in compliance with the law.
10. To comply with other legal acts governing the processing and protection of personal data.

By signing this commitment, I confirm that I understand that non-compliance with this commitment is subject to legal liability.

_____	_____	_____
(person's job title)	(signature)	(name and surname)

The commitment signed in the presence of*:

–

_____	_____	_____
(job title of head of unit)	(signature)	(name and surname)

I am informed:

- that I shall be accountable for non-compliance with this commitment and breach of the General Data Protection Regulation and the Law on Legal Protection of Personal Data of the Republic of Lithuania following the applicable laws of the Republic of Lithuania;
- that a person who has suffered damage as a result of unlawful processing of personal data or other acts or omissions of Kauno kolegija as a data controller has the right to claim compensation for the material or non-material damage caused to him or her;
- that Kauno kolegija, after having compensated the damage caused to a person by unlawful processing of personal data, must recover the damages from the employee who processed the personal data and who was at fault for the damage.

Annex 5
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

CONSENT TO THE IMAGE USE AND PROCESSING OF PERSONAL DATA
(model)

dd/mm/yyyy
Kaunas

I _____
(Name, surname, group (for students only), place of work (for third parties only), position (for staff and third parties only)

by signing this consent, I confirm that I am informed that Kauno kolegija HEI (hereinafter referred to as Kauno kolegija or KK), legal entity code 111965284, 20 Pramonės ave. 50468 Kaunas, tel. (+370 37) 35 23 24, acts as a data controller in processing my data.

I **consent**_____/ I **do not consent**_____ that Kauno kolegija, in the performance of its functions under the Law on Science and Studies of the Republic of Lithuania and in compliance with the requirements of the EU General Data Protection Regulation and other national legislation, to inform about the studies and/or research and art and project activities carried out at KK, will take photographs and/or videos of me and use my recorded image in KK's regular communication channels (website (https://www.kaunokolegija.lt/), intranet (https://intranet.kauko.lt/), social network accounts *Facebook*, *Instagram*, leaflets, articles, billboards, etc., and to process the following personal data about me: photo(s) and/or video(s) of my image, name, surname, job title.

I **consent** _____ / I **do not consent**_____ to the use of my data - photo(s) and/or video(s), name, surname, group (for students), workplace (for third parties), position (for employees of the College, for third parties) - for the purpose stated above on Kauno kolegija's website (https://www.kaunokolegija.lt/), on Kauno kolegija's social networking sites Facebook, Instagram, in leaflets, articles, billboards, etc.

I am informed that:

- I have the right to withdraw my consent at any time (such withdrawal shall not affect the lawfulness of processing based on consent carried out before the withdrawal of consent);
- Kauno kolegija does not transfer my data to third parties, except when articles, videos, and photos are shared via *Facebook*, *Instagram*, intranet and/or when they can be found via the google.com search engine (in such a case, the recipients are *Facebook, Inc*. (US), *Google LLC* (US));
- my consent to the processing of my data and any other personal data that I have provided, i.e. photo(s), video(s) of me, name, surname, and job title, shall be retained for the duration of the contract of employment and a period of 2 years after the end of the contract of employment or the withdrawal of the consent (or, in the case of a student's consent, the contract of study), except where processing is necessary for archiving purposes in the public interest, or the purposes of scientific or historical research.

_____ _____
(signature) (name, surname)

_____

(a description of what actions have been taken/not taken; what data have been lost/disclosed/altered/unlawfully collected/misused, etc.; who may have gained unauthorised access to the personal data being processed; what has been done urgently to avoid the consequences; any other considerations)

The person responsible and the contact details are indicated: _____

_____

(alteration/unlawful collection/unlawful use, etc.); who may have gained unauthorised access to the personal data processed; what was done urgently to avoid consequences; other circumstances)

The person responsible and the contact details are indicated: _____

_____

_____

Annex 6
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

PROCEDURE FOR RESPONDING TO PERSONAL DATA BREACH

CHAPTER I
GENERAL PROVISIONS

1. This *Procedure for Responding to Personal Data Breach* (hereinafter referred to as the Procedure) covers the occurrence of a personal data breach in compliance with Articles 33 and 34 of the GDPR. The Procedure includes the following steps:

1.1. identification and analysis of a data breach;

1.2. limiting, eliminating and recovering after a data safety breach;

1.3. notification by the controller to the supervisory authority and/or the subject of a data breach (if required under the GDPR);

1.4. documenting a data breach.

2. This Procedure should be followed in response to a data breach, considering the factual circumstances of the specific situation.

3. All persons who have access to personal data processed by Kauno kolegija HEI are obliged to be aware of and follow this Procedure in the case of a data safety breach.

CHAPTER II
DATA BREACH IDENTIFICATION AND ANALYSIS

4. A data safety breach is defined as a security incident that results in (a specific breach may fall into more than one category):

4.1. breach of confidentiality is the unintentional or unauthorised disclosure of personal data or the granting of access to unauthorised persons. Examples of such a breach could include sending a copy of the data to a third party who has no legal right to receive it, disclosing the password to a database, etc;

4.2. breach of availability is the unintentional or unlawful loss of access to personal data or destruction of data. A breach of this nature could be the deletion of a database without a backup copy from which to recover the lost data. A breach of availability that should be described would also include a temporary loss of access to data that disrupts the normal activities of KK;

4.3. breach of integrity is an unintentional or unlawful alteration of personal data. This could include modifications to the records in the database by a third party who has gained unauthorised access to the database.

5. When a data protection breach is detected, the employee who detected it must inform his/her immediate manager and the Data Protection Officer as soon as possible, in person, by email, by telephone and/or by other means of communication.

6. The Data Protection Officer carries out an initial assessment to decide on an appropriate action plan. This assessment should include the following key factors:

6.1. the extent of the impact on information technology (IT) infrastructure;

6.2. information resources that may be or have been compromised (what databases are or may be affected);

6.3. the likely duration of the data protection breach (when the breach started and when it was stopped, or how soon it could be fixed);

6.4. the data subjects affected and the scope of the impact on them (whether only a specific group of data subjects is affected, what part of a specific group is affected, etc.);

6.5 initial indications of the consequences of a data security breach (e.g., loss of access to data, unauthorised alterations to data, discovery of compromised data, etc.).

7. The above information should be recorded so that a clear chronological understanding of the progress of the situation and the measures taken can be obtained at the time of the subsequent review.

8. Based on the initial analysis described above, the Data Protection Officer shall assess, in compliance with the criteria specified in Article 6 of the Procedure, whether the scope of the data protection breach and the actual or potential impact of the data breach triggers the initiation of the Data Breach Response Procedure.

CHAPTER III
INITIATING A DATA PROTECTION BREACH RESPONSE PROCEDURE

9. A formal response to a data breach should in all cases be initiated if any of the following circumstances apply:

9.1. a significant amount of personal data has been or may be lost;

9.1. a data breach is likely to result in a serious risk to the rights and freedoms of natural persons;

9.2. a large number of data subjects are affected;

9.3. any other situation that may have a significant impact on Kauno kolegija HEI and/or data subjects.

10. If the decision is made not to initiate the procedure, then the assessment described in Article 6 of the Procedure must be properly documented and the procedure closed.

CHAPTER IV
LIMITING, ERADICATING AND RESTORING A DATA BREACH

11. The first step in dealing with a data breach is to limit it. The specific steps to be taken to achieve this depend on the circumstances of the specific breach but could include actions such as:

11.1. remotely deleting data from a lost or stolen device;

11.2. contacting the person to whom the data was sent by mistake as soon as possible to ask them not to open the data sent and to delete it without the possibility of recovery;

11.3. changing the password for accessing the database, which has been disclosed to third parties;

11.4. restoring lost data from an existing backup.

12. This procedure should take precautions to ensure that the most accurate data and evidence of the data breach are gathered (e.g., recording who accessed the database, when and from which device, who exactly the personal data was mistakenly sent to, and the circumstances under which the device containing data was lost).

13. Actions to repair the damage caused by a data breach should not only address the cause of the existing breach but should also be aimed at preventing the recurrence of a data breach. Any vulnerability that could be exploited to commit a breach should be identified.

14. IT specialists or lawyers may be involved if necessary.

15. During the recovery phase, systems should be restored to their previous state as far as possible, but the necessary steps should be taken to address the weaknesses and data processing vulnerabilities that were exploited in the data breach.

CHAPTER V
DATA BREACH NOTIFICATION BY THE DATA CONTROLLER TO THE SUPERVISORY AUTHORITY

16. Kauno kolegija HEI, as a data controller, is obliged to inform the Supervisory Authority about a data breach without undue delay if the Data Protection Officer determines that the data breach is likely to jeopardise the rights and freedoms of the data subjects affected by the data breach. A breach is of such a nature as to be likely to result in bodily harm, material or non-material damage, restriction of rights, discrimination, theft or falsification of identity, financial loss, unauthorised use of aliases, damage to reputation, loss of confidentiality of personal data subject to professional secrecy or other economic or social damage.

17. If a data breach jeopardises the rights and freedoms of data subjects, the Data Protection Officer shall provide the Supervisory Authority with the information no later than 72 hours after KK becomes aware of the breach:

17.1. the nature of the data breach, including, where possible, the categories and approximate number of data subjects affected and the categories and approximate number of personal data records concerned;

17.2. the name and contact details of a contact person who can provide further information;

17.3. a description of the likely consequences of a data protection breach;

17.4. the measures taken or planned by Kauno kolegija to remedy the data breach, including, where appropriate, measures to minimise its possible negative consequences.

18. If all information cannot be provided in full at the same time, further information may be provided in stages without undue delay.

CHAPTER VI
NOTIFICATION BY THE DATA CONTROLLER TO THE DATA SUBJECT ABOUT A DATA PROTECTION BREACH

19. When a data breach is likely to result in a serious risk to the rights and freedoms of natural persons, Kauno kolegija shall, without undue delay, inform the data subjects of the personal data breach. Any breach that risks the consequences referred to in Article 17 may be considered to constitute a high risk where such consequences are highly probable, where sensitive personal data (such as health data) are processed, and where the breach has an unfavourable impact on many data subjects, etc.

20. The Data Protection Officer shall describe to the subject, in clear and plain language, the nature of the data breach and shall provide at least the following information:

20.1. the name and contact details of a contact person who can provide further information;

20.2. a description of the likely consequences of a data protection breach;

20.3. the measures taken or planned by KK to resolve the data breach, including, where appropriate, measures to minimise its possible negative consequences.

21. The communication with the data subject referred to in Article 20 of this Procedure will not be required if any of the following circumstances exist:

21.1. Kauno kolegija has implemented appropriate technical and organisational protection measures and those measures have been applied to the personal data affected by the data breach, in particular measures to ensure that the personal data are incomprehensible to an unauthorised person, such as encryption measures;

21.2. Kauno kolegija has subsequently taken measures to ensure that the rights and freedoms of data subjects are not seriously jeopardised in the future;

21.3. it would require a disproportionate effort. In such a case, the occurrence of the data breach shall be made public or a similar measure shall be taken to inform data subjects in the same efficient manner.

22. The supervisory authority may, after considering the likelihood of a data protection breach resulting in a serious risk, require Kauno kolegija to inform data subjects about the data protection breach. The DPO shall comply with such an instruction without delay.

CHAPTER VII
DOCUMENTING THE DATA PROTECTION BREACH AND COMPLETING THE PROCEDURE

23. The DPO, with the approval of the KK Director, who has been informed about the context of the data breach and its rectification, shall decide to close the Procedure when the data breach is assessed to have been resolved, and the breach has been communicated to all relevant parties.

24. All actions taken during the Procedure shall be described and all relevant records of the data breach shall be reviewed to ensure their completeness, accuracy and compliance with the relevant legal framework.

_____

Annex 7
to *Description of the Procedure for Processing Personal Data at Kauno kolegija HEI*

REGISTER OF PERSONAL DATA PROTECTION BREACH

No., date	Grounds for the breach (what happened and what personal data were compromised)	Impact and consequences of the breach	Corrective actions (technical measures) taken	Reasons for deciding on a breach (why it was decided not to report to the SDPI and/or to the data subject; why it was decided that the breach was unlikely to result in a risk to natural persons rights and freedoms, or which condition was met where no reporting is required)	Grounds for the delay in submitting the notification to the SDPI	Information related to the notification to the data subject	Other relevant information Breach/ safety incident

_____