APPROVED by Order No. V-23
of the Director of Vilnius Business College
on 29 November 2022

GENERAL DATA PROTECTION REGULATION

CHAPTER 1

GENERAL PROVISIONS

1. Vilnius Business College, legal entity code 191807983, address Kalvarijų str.129-401, Vilnius (hereinafter - the College), General Data Protection Regulation (hereinafter - the Rules) are applied to automatic and non-automatic processing of personal data protection of data subjects, regulating the purposes of personal data processing, determining the rights of data subjects and the procedure for implementing their rights, the rights of employees, duties and responsibilities in the processing of protecting the personal data, establishing organisational and technical measures for the protection of personal data, the use of the data controller, etc.
2. The College is the controller of all personal data collected during the activities of the College, as well as the processor of personal data transferred by other controllers.
3. This Regulation is prepared in accordance with 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 - GDPR), the Republic of Lithuania Law on Legal Protection of Personal Data (hereinafter - LPPDL), the Labour Code of the Republic of Lithuania and other legal acts.
4. The main concepts used in this Regulation are as follows:
   - **4.1 Personal data** - any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is a person who can directly or indirectly be identified by referening to an identifier such as name, location, personal identification number or to one or more physical, physiological, economic, features of cultural or social identity.
   - **4.2 Employee** – a person working in the College under an employment contract.
   - **4.3 Data protection officer –** an employee appointed by the College to carry out duties with regard to data controlled and/or processed by the College as set out for the data protection officer under the GDPR and LPPDL.
   - **4.4 Data recipient** - a natural or legal person to whom personal data are disclosed.
   - **4.5 Data processor** - a natural or legal person who processes personal data on behalf of the controller.
   - **4.6 Data controller** - a natural or legal person who alone or in partnership with others determines the purposes and means of personal data.
   - **4.7 Data subject –** a natural person whose personal data are processed by the controller or processors.
   - **4.8 Disclosure of data** - disclosure of personal data by transmission or making them available by any other means.

4.9 Data processing - any operation or sequence of operations on personal data or sets of personal data carried out by automated or non-automated means, i.e. collecting, recording, sorting, organising, storing, adapting or modifying, extracting, accessing, using, disclosing, transmitting, distributing or otherwise making available, collating or merging with other data, restricting, deleting, destructing or any other set of operations.

4.10 Data processing by automated means – data processing operations performed in whole or in part by automated means.

4.11 Data processing by non-automated means – data processing operations performed by non-automated means.

4.12 Consent of the data subject (hereinafter – Consent) – any freely given written statement of the data subject expressing a statement or an explicit act of approval, which allows processing of personal data for an identified purpose.

4.13 Request – an application (request) of the data subject to the College requesting to provide the information on the personal data processed in accordance with the procedure established in this Regulation unrelated to a breach of personal data protection rights and legitimite interests.

4.14 Profiling – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal interests, reliability, behaviour, location or movements.

4.15 Third party – a natural or legal person with the exception of the data subject, the data controller, the data processor and persons who have been directly authorised by the data controller or the data processor to process data.

4.16 Complaint – an individual's written application reporting a breach of his/her rights to personal data protection or legitimate interests or reporting a breach of another person's rights to personal data protection or legitimate interests and requesting to protect them.

4.17 Supervisory Authority – an independent authority established by an EU Member State, is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedom of individuals with regard to the processing of personal data and to facilitate the free movement of personal data within the European Union.

5. Other concepts are used as defined in the GDPR and the Law on Science and Studies of the Republic of Lithuania (hereinafter - the Law on Science and Studies)
6. According to the Art. No. 4 of the LPPDL, when personal data is processed for the purposes of journalism or academic, artistic or literary expression, Art. No. 8, 12-23, 25, 30, 33-39, 41-50, 88-91 of the GDPR do not apply to the processing of personal data, and the relevant provisions of this Regulation.

CHAPTER II

PURPOSES OF PERSONAL DATA PROCESSING AND CATEGORIES OF DATA PROCESSORS

7. Personal data at the College are processed for the following purposes:
   7.1 The purpose of admitting students and listeners.

7.1.1. The following personal data are processed: name, surname, former surname, personal identification number, date of birth, gender, telephone number, address of residence and / or declared residence, temporary residence permit data, department, study programme, study form, nature of funding, competitive score (if applicable), data on acquired secondary school education (code, name), in a foreign language during studies, citizenship, form of assessment, other data in the diploma document and diploma supplement, vocational or higher school academic certificate or diploma and its appendix data, personal identity document (type, number, validity date), signature, e-mail address, data on financial obligations, personal data specified in the authorization to sign the study agreement.
7.1.2. Categories of data subjects whose personal data are processed: students, persons authorized to sign study agreements, listeners.

7.2 The purpose of financing the studies of students and listeners.

7.2.1. The following personal data are processed: name, surname, personal identification number, data on the issuance and validity of an identity document, data on a person's disability (disability certificate number, person's ability to work, percentage of ability to work, level of special needs, date of issue and validity), data on military service, information on the student's origin (for expatriate Lithuanians), data on personal studies (start date of studies, year of the graduation, degree, department, form of studies, programme, semester, course, group, nature of funding, amount and year of the State-supported grant for studies, granted to the student identification number, current bank account number, data on financial obligations to the College, payments and / or payments made, their amount and dates, signature, telephone number, e-mail address, bank transfer (course fees) data.
7.2.2. Categories of data subjects whose personal data are processed: students, listeners.

7.3. The purpose of accounting for students and listeners.

7.3.1. The following personal data are processed: name, surname, personal identification number, date of birth, gender; address; citizenship; data on the person's disability (disability certificate number, date of issue and validity, level of working capacity (percentage,); data on military service; education data (name of the school graduated, code, type, year of graduation, country); information on student's origin data on personal studies (department, form of studies, study programme, semester, course, group, type of funding, amount and year of the State-supported grant for studies, data on academic debts, granted academic leave), identification numbers provided to the student, telephone number, e-mail address, signature.

7.4. The purpose of study organization and study results accounting.

7.4.1. The following personal data are processed: name, surname, signature, telephone number, e-mail address, data of the diploma supplement of the completed higher education institution (name of the school, data of credits achieved), data on the student's studies (start date, end date, degree, department, study programme, form of studies, semester studied, course, academic group, subjects studied, assessment forms and dates, assessments of study achievements, data on academic debts, data o changes in study programme and form of the studies, data on granted academic leave, participation in Erasmus + programme, acquired qualification degree), data of documents certifying graduation of the College (diplomas and their appendixes); data on the listener's studies (start date and end date of the course, the course completed); workplace, job position,

subject taught; name, surname of the head of the internship company (the person representing), start and end dates of the internship.
7.4.2. Categories of data subjects whose personal data are processed: students, listeners, lecturers, head members of student production internship, members of the final thesis defense committee.

7.5. The purpose of employee relationship management.

7.5.1. The following personal data are processed: name, surname; citizenship; personal identification number; gender; a photo of the person; signature; data on marital status, names and surnames of family members, dates of their birth; personal social security number; period of insurance with state funds; data on the retirement fund; current bank account number; description of life and activities; data of documents certifying education and qualification; job position; data on employment, dismissal, employment contract conditions; data on length of service; tabular employer identification number; pedagogical names; holiday data; data on business trips; data on a separate work schedule; data on wages, benefits, compensations, allowances; information on working hours, workload, information on employee promotion, penalties, breaches of work responsibilities, data on employee performance appraisal; special categories of personal data relating to a person's health; data of an identity document; data of the residence permit in Lithuania; previous, current and next job and position; former surname (s); other personal data provided voluntarily by the person to the College.
7.5.2. Category of data subjects whose personal data are processed: employees.

7.6. Candidates and applicants for jobs, purpose of administration.

7.6.1. The following personal data are processed: name, surname; personal identification number; birth data; signature; data provided in the curriculum vitae: telephone number, e-mail address, current and former place of work, study institution (current or former), job position, data on education, degree and other personal data voluntarily provided by the candidate to the College.
7.6.2. Categories of data subjects whose personal data are processed: job candidates; candidates to work as lecturers.

7.7 Purpose of financial settlements with the staff of the College.

7.7.1. The following personal data are processed: name, surname; citizenship; home address; telephone number; e-mail address; personal identification number; date of birth; gender; signature; personal social security number; amount of wages and social insurance contributions; amounts of revenue; voluntary social insurance data; period of insurance with state funds; data on participation in a retirement fund; current bank account number; data of documents certifying education and qualification; job position; data on employment, dismissal, employment contract conditions; data on length of service; tabular employee identification number; pedagogical names, date of data entry (any modification); holiday data; data on business trips; data on a separate work schedule; data on wages, benefits, compensations, allowances; data on financial liabilities; court case data; data of enforcement orders, other procedural documents; information on working hours, workload, information on employee promotion, special category personal data related to personal health; data of an identity document; former surname (s).
7.7.2. Categories of data subjects whose personal data are processed: employees, students.

7.8. The purpose of processing the personal data of current and former employees and students in the field of internal administration of the library.

7.8.1. The following personal data are processed: name, surname; former surname (s); citizenship; address; telephone number; e-mail address; personal identification number; date of birth; gender; job position; tabular employee identification number; pedagogical names, previous, current and other job position; date of data recorded (any modification).

7.8.2. Categories of data subjects whose personal data are processed: current and former employees, teachers, students.

7.9. Purpose of authentication of data subjects in the information systems.

7.9.1. The following personal data are processed: name, surname; personal identification number; personal telephone number; personal e-mail address; College email address; given username; password reminder data.

7.9.2. Categories of data subjects whose personal data are processed: employees, students.

7.10. User account administration and purpose of authentication.

7.10.1. The following personal data, access to e-mail, databases, etc. are processed: name, surname; personal identification number; employee identification number (for employees); personal telephone number; personal e-mail address; College e-mail address, job position (s); given username; work and / or research institution, department, group, department.

7.10.2. Categories of data subjects whose personal data are processed: employees, students.

7.11. The purpose of organising conferences and other events.

7.11.1. The following personal data are processed: name, surname; telephone number; signature; current bank account number; bank transfer details; e-mail address; country; (work or study) institution, division of (work or study) institution, job position, degree, language of the research paper, summary of the research paper in Lithuanian and a foreign language, electronic access to the research paper, date of publication, current account number and other banking data .

7.11.2. Categories of data subjects whose personal data are processed: students, lecturers, employees, representatives of foreign institutions, representatives of business enterprises and organizations.

7.12. Purpose of communication.

7.12.1. The following data are processed: name, surname; telephone number; date of birth; home address; Email address; the represented workplace or educational institution, its subdivision, position; image, including, but not limited to, photographs and / or videos of this type taken and trips, celebrations, commemorations, meetings, meetings, etc. organized at the College. years.

7.12.2. Categories of data subjects whose personal data are processed: students; students; teachers who accompany students; teachers; employees; parents of students; guests.

7.13. Purpose of handling complaints, requests and other appeals.

7.13.1. The following personal data are processed: name, surname; date of birth; personal identification number; home address; telephone number; email address; position; signature; the date of the complaint, application or other appeal submitted in

the College, the registration number; current bank account number; data of an identity document; data of the notary certifying the identity document, personal data specified in the power of attorney; the information provided by the person in the complaint, request or appeal, including special categories of personal data, if any; response to a complaint, appeal or other request; additional information obtained during the investigation of the complaint, appeal or other request.

7.13.2. Categories of data subjects whose personal data are processed: employees; students; natural persons.

7.14. Purpose of the security of persons and property, including but not limited to the conduct of video surveillance systems, as well as the passage control.

7.14.1. The following personal data are processed: name, surname; position; signature; telephone number; image, including but not limited to the license plate number of the car.

7.14.2. Categories of data subjects whose personal data are processed: employees, students; other persons gotten into video surveillance systems.

7.15. Purpose of concluding, executing and administering contracts (except contracts with employees, students and listeners).

7.15.1. The following personal data are processed: name, surname; date of birth; personal identification number or an identity document number (if the person does not have a personal identification number); home address; e-mail address; telephone number; signature; job title; job position; work address, details of the powers of attorney (representation), including the personal identification number and addresses of the representatives; current bank account number; terms of the contract; data of the documents allowing to engage in the relevant activity (date of validity of the document, number, institution issuing the document, other data contained in the document); data on participation in the accumulation of retirement supplementary fund; data of representation documents; data of documents certifying education and qualification; details of correspondence between the parties; other data formed during the conclusion, execution and administration of contracts.

7.15.2. Categories of data subjects whose personal data are processed: representatives of legal entities who sign agreements with the College; natural persons who interacts with the College and sign agreement.

CHAPTER III

PROCESSING OF PERSONAL DATA

8. When processing personal data, the management of the College shall comply with the requirements of personal data processing established in the GPDR and the LPPDL, these Rules and other legal acts regulating safety documents of personal data personal data. All personal data shall be processed by the College in accordance with the principles of lawfulness, fairness and transparency, purpose limitation, data reduction, accuracy, limitation of the retention period, integrity and confidentiality set out in Art. No. 5 (1) of the GPDR. Personal data shall be processed by the College only under at least one of the conditions provided in Art. No. 6 (1) of the GPDR and only to the extent of a such condition applying.

9. At the College personal data are processed by automated and non-automated means only for the necessary purposes, required for the activities of the College or by legal acts.
10. The College shall receive personal data directly from the data subject, on the basis of contracts or legal acts, from third parties entitled to provide personal data to the College in the process.
11. The processing of personal data applied to special categories is prohibited unless one of the conditions set out in Art. No. 9 (2) of the GDPR is met.
12. The College, as data controller:
    12.1. ensures the implementation of the data subject's rights and performs the duties of personal data controller established in the GDPR and other legal acts regulating the processing of personal data;
    12.2. appoints a data protection officer on a mandatory basis;
    12.3. approves legal acts regulating personal data protection;
    12.4. ensures training of employees in the field of personal data protection;
    12.5. ensures that personal data in the College are processed only by the persons who find it necessary for the execution of their work functions and only to the extent necessary to achieve the goals set;
    12.6. ensures that personal data are:
    12.6.1. collected for specified and legitimate purposes and not further processed for purposes incompatible with those established prior to the collection of the personal data;
    12.6.2. accurate and, where necessary for the processing of personal data, kept up to date; inaccurate or incomplete personal data are corrected, supplemented, erased or suspended;
    12.6.3. identical, appropriate and only to the extent necessary for their collection and further processing;
    12.6.4. processed in such a way that the data subject can be identified for no longer than is necessary for the purposes for which the personal data were collected and processed;
    12.6.5. processed in accordance with GDPR, LPPDL, these Rules and other legal acts regulating the protection of personal data.
13. Employee:
    13.1. prepares and submits records of the data processing operations to the Data Protection Officer of the College;
    13.2. before each personal data processing operation (action) must assess whether such processing of personal data complies with the requirements established in these Rules, including, but not limited to compliance with the conditions specified in Art. No. 12.5 of the Rules;
    13.3. comply with the organizational and technical measures established by the College to protect the processed personal data from accidental or unlawful destruction, alteration, disclosure as well as against any illegal processing;
    13.4. at the end of the retention period, documents containing personal data or copies thereof stored manually shall be destroyed in such a way that the information contained therein is not recognizable, and automatically collected data shall be destroyed by

deleting obsolete personal data files from the storage medium in such a way that cannot lead to recovery of the personal data.

14. The College performs the following personal data processing functions:
    14.1. ensures that personal data in the information systems managed by the College are processed only by the people for whom it is necessary for the performance of work actions and only to the extent necessary to achieve the intended purposes of work functions and goals;
    14.2. ensures the lawful processing of personal data, the implementation of the rights of data subjects and the necessary technical data protection measures by means of the information systems maintained by the College by all available means;
    14.3. ensures that personal data which is deleted is also destroyed from the storage places of backup copies of the College's information system (if there are any);
    14.4. carries out impact assessments on the personal data processing in the College's information systems at least once a year and on these issues as well consult the Data Protection Officer;
    14.5. establishes requirements for the selection of data processors related to the maintenance of information technology of the College and control the compliance of such data processors with the established requirements;
    14.6. establishes and implements other technical and organizational data protection measures of information technology managed by the College, ensuring data protection in accordance with GDPR and other applicable legal acts.
15. In cases where the College acts as a data controller:
    15.1. personal data are processed in accordance with the instructions established in the data controller's documents (including, but not limited to contracts with the data controller) and the requirements provided by legal acts only apply to the extent for the purpose specified in such documents;
    15.2. The College ensures the security of personal data processed in accordance with the GDPR, LPPDL and other legal acts regulating the security of personal data;
    15.3. The College, having achieved the purpose of processing the personal data received from the controller, shall destroy them or, if authorized by contracts or legislation, store them in accordance with the retention periods and apply appropriate technical and organisational data protection measures.
16. Personal data breach management (hereinafter: PDB, personal data breach):
    16.1. in the event of any PDB, College staff who become aware of a PDB must immediately, but not later than within 3 hours of the PDB become apparent, inform the management, and notify the College Data Protection Officer. The College must eliminate the damage made by the PDB as soon as possible, eliminate its consequences and take measures to reduce or eliminate the risk or potential damage to the rights and freedoms of data subjects;
    16.2. In case of violation of personal data and no later than 72 hours after the College became aware of the PDB, the College shall, in accordance with the established operations and conditions, notify the State Data Inspectorate by submitting a notification. The conditions apply in accordance with the provisions of the Art. No. 33 of the GDPR and the description of the procedure for submitted on 27th of July by order no. 1T-72 (1.12. E) “On the Approval of the Description of the Procedure for Giving of the Notification of a Personal Data Breach to the State Data Protection Inspectorate”.

Notification to the State Data Protection Inspectorate is not provided when the PDB does not endanger the rights and freedoms of natural persons;

16.3. the notification of the PDB to the data subject shall be made in accordance with the provisions of Art. No. 34 of the GDPR;

16.4. if the College becomes aware of an PDB while acting as a data controller, it shall immediately notify the controller in writing;

16.5. The College, in accordance with the form approved by the College, maintains a separate register of PDB, in which all PDB are registered. The Data Protection Officer is responsible for completing the PDB register. The register of PDB is provided to the State Data Protection Inspectorate upon its request. The PDB infringement register may be written in paper or electronically.

CHAPTER IV

DATA PROTECTION OFFICER

17. The Data Protection Officer shall:

17.1. inform the College management and the employees concerning personal data about their obligations under the GDPR, LPPDL. These Rules and other legal acts regulating data protection of the European Union (hereinafter - the EU) or the Republic of Lithuania and advises on these issues;

17.2. monitor compliance with the provisions of GDPR, LPPDL and other EU or Lithuanian legal acts regulating data protection, raising awareness and training of the College staff involved in data processing operations, which include assignment of duties, and carry out audits related to personal data;

17.3. give consultations to data subjects whose personal data are processed by the College on all issues regarding the processing of their personal data and the exercise of rights under the GDPR;

17.4. cooperate with the supervisory authority, act as a contact person for the supervisory authority in matters related to data processing, which includes prior consultations referred in the GDPR, advise on other issues if necessary;

17.5. assess the risks associated with the data processing operations (perform a risk assessment), taking into account the costs of the nature, scope, context, and purposes of processing.

17.6. manage the records of data processing operations, which are prepared and submitted by the employees of the College;

17.7. ensure secrecy or confidentiality related to the execution of its tasks in compliance with the requirements established in the legal acts of the EU and the Republic of Lithuania;

17.8. notify the State Data Protection Inspectorate in writing if it establishes that personal data are processed in violation of the provisions of legal acts regulating data protection or refuses to execute direct instructions to eliminate such violations;

17.9. carry out other tasks and responsibilities assigned to the GDPR, the Rules and other legal acts regulating the protection of personal data;

17.10. prepare the annual activity report and reports directly to the management of the College.

18. The College:
    18.1. ensures that the Data Protection Officer is properly and timely involved in all matters relating to the protection of personal data and in the drafting of internal legislation;
    18.2. ensures that the Data Protection Officer is involved in the College's response to requests and complaints from data subjects concerning the protection of personal data;
    18.3. assists the Data Protection Officer in carrying out the tasks specified in the GDPR by providing them with the necessary resources to carry out those tasks, as well as access to personal data, participation in data processing operations and the retention of their expertise;
    18.4. ensures that the Data Protection Officer does not receive any instructions regarding the execution of his or her tasks and is able to carry out those tasks independently.

CHAPTER V

DATA COLLECTION, DATA SUBJECT CONSENT AND DATA TRANSFER

19. In the case of direct collection of personal data from the data subject, the following information shall be provided to the data subject during the data collection (unless the data subject already has such information):
    19.1. Name of the College, legal entity code, address, telephone number, e-mail address;
    19.2. Contact details of the College Data Protection Officer;
    19.3. the purposes for which the personal data of the data subject are intended to be processed and the legal basis for the personal data processing;
    19.4. what personal data of the data subject are required;
    19.5. to whom (data recipients, categories of data recipients) and for what purposes the personal data will be provided;
    19.6. the period for which the personal data will be stored or, if this cannot be determined, the criteria for envisaging that period;
    19.7. the legitimate interests of the College when the processing is carried out in the legitimate interests of the College;
    19.8. the right of the data subject to access his or hers personal data and the right to request the correction or erasing of incorrect, incomplete, inaccurate personal data, to restrict the processing of data, the right to object the processing of data, the right to data portability;
    19.9. where the processing is based on the data subject's consent, the right to withdraw the consent at any time, without prejudice to the lawfulness of the data processing prior to the withdrawal of the consent;
    19.10. the right to apply to the supervisory authority;
    19.11. the existence of automated decision-making, including profiling;
    19.12. stating the consequences of not providing personal data.
20. When personal data of data subject is received indirectly from the data subject and with the intention on providing personal data to third parties or use for communication with the data subject. The data subject shall be informed thereof by providing him / her the

information specified in Art. No. 19.1-19.11 of these Rules with the source of the data and, if applicable, whether the data are obtained from publicly available sources. When personal data about the data subject are obtained indirectly from the data subject, the College shall provide the information to the data subject no later than within 30 calendar days. When personal data are obtained indirectly from the data subject and provided to third parties or used to communicate with the data subject, the data subject should be informed before the first time when the personal data are disclosed to third parties or contacted by the data subject. Information shall not be provided to the data subject when: the data subject already has such information; data transfer is regulated by other legal acts; the provision of such information is impossible or would require a disproportionate effort due to the large number of data recipients, the possibility for data to be outdated and the unreasonable cost.

21. Information on data processing shall be provided to the data subject in writing and / or by electronic means of communication, as well as published on the website of the College: www.kolegija.lt
22. In cases and in accordance with the procedure established by legal acts personal data processed the College shall be disclosed to the Ministry of Education, Science and Sport of the Republic of Lithuania, Ministry of Finance of the Republic of Lithuania, Office of the Ombudsman for Academic Ethics and Procedures, State Tax Inspectorate, the State Security Department of the Republic of Lithuania, the Board of the State Social Insurance Fund under the Ministry of Social Security and Labour, the National Cyber Security Centre under the Ministry of National Defence, the Communications Regulatory Authority of the Republic of Lithuania and other third parties according to legal acts or under a personal data provision agreement (in the case of multiple personal data collection).
23. 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 in accordance with the same procedure as to data recipients located in the Republic of Lithuania.
24. Personal data processed or intended to be processed after a transfer to a third country or to an international organization shall be transferred only if the College and the processor comply with the provisions of the GDPR.
25. When processing data on behalf of the College, the College shall use those processors who sufficiently ensure that the appropriate technical and organizational measures are implemented in such a way that the processing complies with the requirements of the GDPR and the protection of data subjects' rights is ensured. The processing of data by the controller shall be governed by a contract, agreement or legal act which is binding on the controller on behalf of the College and the main provisions of which are set out in Art. No. 28 of the GDPR

CHAPTER VI

RIGHTS OF THE DATA SUBJECT

26. A data subject whose data are processed in the activities of the College has the following rights:

26.1. to know (be informed) about the processing of his/her data (right to get acquainted);
26.2. to access his/her personal data and how they are processed (right to get acquainted);
26.3. to request rectification or, depending on the purposes for which the personal data are processed, to supplement incomplete personal data (right to rectification);
26.4. to demand the erasure of his/her personal data (right to be forgotten);
26.5. to require the College to restrict the processing of personal data (right to restrict processing);
26.6. to data portability (right to transfer);
26.7. to object the processing of personal data;
26.8. to oppose its application in a fully automated manner when decision making, including profiling.
27. The rights of the data subject are not absolute, they are implemented in accordance with the legal obligations and legitimate interests of the College. The rules for the implementation of data subject's rights in the College were approved by the Director of Vilnius Business College in 29 November 2019, Order no. V-24 "On Approval of the Rules for the Implementation of the Rights of the Data Subject of Vilnius Business College".
28. The data subject shall have the right to submit a written request (including, but not limited to electronic means) to the Director of the College regarding the exercise of the data subject's rights, as well as all issues related to the processing of the data subject's personal data and exercise of his / her rights by contacting security officer via e-mail: dap@vvk.lt or address: Kalvarijų st. 129-401, Vilnius.
29. A data subject who has submitted a request or complaint not later than within 30 (thirty) calendar days from the submission of the request or complaint shall be provided with information on the action taken in response to the received request or complaint. The time limit for replying to a request or complaint may be extended in accordance with the conditions laid down by law.
30. A copy of personal data processed once a calendar year (in the form chosen by the College) shall be provided to the data subject free of charge, in other cases a fee calculated according to the administrative costs incurred by the College may be charged.

CHAPTER VII

ORGANISATIONAL AND TECHNICAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

31. For all personal data processed the College shall implement organisational and technical measures to protect personal data against accidental or unlawful destruction, alteration, disclosure, as well as against any unlawful processing: infrastructure measures (proper layout of premises, proper layout and maintenance of technical equipment, strict compliance with fire safety standards, controlled access to the College's buildings, lockable premises (access of unauthorized persons to the relevant premises is restricted, the premises are used only by the employees of that department, etc.) and cabinets containing personal data, etc.); administrative arrangements (proper

organization of work, proper and timely information and training of staff and advice on personal data processing; obligation and written commitment of staff authorized to process personal data to ensure the confidentiality of personal data; review and, if necessary, amendment of the College's internal legislation for the purpose of improving data protection measures, proper storage of documents in accordance with the storage terms specified in the Documentation Plan, etc. Upon expiry of the storage period, destruction of documents in a safe and irreversible manner is done in accordance with the established procedure.

32. Organisational and technical measures are applied for the protection of personal data using the information technologies of the College:

32.1. access to personal data shall be granted only to the extent for those persons who need it for the performance of their operational functions;

32.2. personal data may be processed in information systems only for those actions for which the user of the information system has been granted access rights;

32.3. ensuring the protection of personal data against illegal connection to the internal computer network;

32.4. ensuring protection of computer equipment from malicious software (installation and update of antivirus programs, etc.);

32.5. controlled access is applied to personal data security by such organisational and technical means, which is taking records and controlling attempts to register and obtain access rights;

32.6. personal data shall be deleted from all systems upon achievement of the purpose of their use, except for their storage in accordance with the procedure established by legal acts.

33. Other organisational and technical measures applicable to the protection of personal data using the information technologies of the College are established in the internal legal acts regulating the security of information technologies of the College.

CHAPTER VIII

VIDEO DATA PROCESSING

34. Video surveillance on the premises of the College is carried out based on a legitimate interest in order to ensure the safety of all persons and property in the College and to maintain public order. Security cameras shall film the premises of the College (entrance, lobby, corridor (1a), corridor (2a)).

35. More detailed processing of personal data through video surveillance is defined in a document signed by the Director of Vilnius Business College in 29 November 2019 by Order V-25 “On Approval of the Video Data Processing Rules of Vilnius Business College” and other documents approved by legal acts of the College regulating video surveillance.

36. The College is the controller of video data and manages the video data of data subjects recorded in the territory and premises managed by the College.

37. Video surveillance data may be provided to institutions and officials entitled to receive such video data in accordance with legal acts.

38. Video surveillance data is recorded in a stationary video recording device located at the College. The term of storage of video surveillance data is established in the legal acts of the College regulating video surveillance.
39. Recording of video surveillance data is carried out around the clock.
40. Director of the College is appointed a staff member or members of the College who shall be responsible for reviewing the video surveillance data and controlling the video surveillance equipment.
41. Events are organized in the premises and territory of the College, during which data subjects may be photographed and/or filmed. The College shall process this video data for publicity purposes with the consent of the data subject when the data subjects are informed about the video surveillance and photography before the start of the event and by public information signs.
42. Video data of data subjects (including, but not limited to photos) captured during events organized by the College may be published in such places as the College's social network account, website, media portals, other social media, including advertising booklets.
43. Visitors of an event organized by the College have the right to withdraw their consent to the processing of video data for the purpose of publicising the event.
44. A declaration of expression of will regarding the processing of such data may be submitted by contacting the Data Protection Officer of the College by e-mail: dap@vvk.lt, or the address: Kalvarijų st. 129-401, Vilnius.
45. Persons entering the field of video surveillance shall have all the rights of data subjects specified in Chapter VI of these Rules.
46. Video data recorded during events organized by the College shall be stored for no longer than is necessary to achieve the purpose of data processing.

CHAPTER IX

FINAL PROVISIONS

48. The Rules shall be reviewed at least once a calendar year and updated if necessary.
49. The updating of these rules shall be initiated as necessary by the Director of the College and / or the Data Protection Officer of the College.
50. The employees of the College must get acquainted with these Rules and comply with them by signing or in another way that ensures the recording of the fact of acquaintance.
51. Employees who violate the requirements for the processing and protection of personal data established in the GDPR, LPPDL, legal acts, these Rules and other legal acts of the College shall be liable for non-compliance in accordance with the rules of the College work procedure and other legal acts.