**Appendix 1**

**Issued: Order #07/01-14, 10/04/2024**

**Personal Data Protection Policy**

**Tbilisi**

**2024**

# Article 1. General information

1. " International Black Sea University" LLC (hereinafter - the "University") ensures the protection of basic human rights and freedoms, including the inviolability of personal life, when processing personal data.
2. The University's personal data protection policy document sets out the personal data protection strategy, basic data protection principles, and mechanisms. Accordingly, when processing personal data, the University acts in accordance with the Law of Georgia "On Personal Data Protection", other normative acts, the recommendations of the Personal Data Protection Service, and the Personal Data Protection Policy (hereinafter - the "Policy").
3. The policy applies to persons employed by the University, students of the University, and other persons acting on behalf of the University.

# Article 2. Purpose of the policy

1. The purpose of the policy is to determine the rules and procedures for the protection and processing of personal data collected by the university, taking into account its goals and activities, to ensure that the processing process is carried out under the law, to protect the rights of individuals and to ensure the transparency of processing.
2. The University, as a higher educational institution, in each case of data processing ensures the determination of the basis of data processing and the compliance of the data processing process with the principles defined by law.

# Article 3. Definition of terms

1. The terms used in the policy are descriptive only and are interpreted based on the specifics of the University's work. The definitions are under the Law of Georgia "On Personal Data Protection" and their interpretation is not allowed in violation of the law.
	1. **Personal data (hereinafter - data)** - any information related to an identified or identifiable natural person. A natural person is identifiable when he can be identified directly or indirectly, including by name, surname, identification number, geolocation data, electronic communication identifying data, physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics;
	2. **Special category data -** data related to a natural person's racial or ethnic affiliation, political views, religious, philosophical, or other beliefs, membership of a professional union, health, sex life, status of the accused, convicted, acquitted, or victim in criminal proceedings, conviction, diversion, human trafficking or "prevention of violence against women and/or domestic violence, protection and assistance to victims of violence", under the law of Georgia is recognized as a victim of crime, imprisonment, and execution of the sentence against him, as well as biometric and genetic data, which are used for the unique identification of a natural person is being processed;
	3. **Health-related data -** information about the physical or mental health of the data subject, as well as information about the provision of medical services to him, if it provides information about the physical or mental health of the data subject;
	4. **Biometric data -** data processed using technical means, related to the physical, physiological, or behavioral characteristics of the data subject (such as, for example, facial image, voice characteristic, or dactyloscopy data), which provides the opportunity to uniquely identify or confirm the identity of the data subject;
	5. **Data processing -** any action performed on data, including their collection, retrieval, access to them, their photography, video monitoring and/or audio monitoring, organization, grouping, interconnection, storage, modification, retrieval, retrieval, use, blocking, deletion or destruction, as well as disclosure of data by transmitting, publicizing, distributing or otherwise making available;
	6. **Data processing by automatic means -** data processing using information technologies;
	7. Processing of data by non-automatic means - processing of data without the use of information technologies;
	8. **Data processing with semi-automatic means -** data processing with the joint use of automatic means and non-automatic means;
	9. **File system -** a structured set of data, in which they are sorted and accessible according to a specific criterion;
	10. **Data subject -** any natural person about whom data is processed;
	11. Consent of the data subject - after receiving relevant information from the data subject, the will to process data about him for a specific purpose by active action, written (including electronically) or orally, freely and clearly expressed will;
	12. **Written consent of the data subject -** consent that the data subject has signed or otherwise expressed in writing (including electronically) after receiving relevant information about the processing of data about him for a specific purpose;
	13. **The person responsible for processing -** a natural person, legal entity, or public institution, which individually or together with others determines the purposes and means of data processing, performs data processing directly or through a person authorized for processing;
	14. **Persons responsible for joint processing** - two or more persons responsible for processing, who jointly determine the purposes and means of data processing;
	15. **The person authorized for processing -** a natural person, legal entity, or public institution that processes data for or on behalf of the person responsible for processing. A natural person in an employment relationship with a person responsible for processing is not considered a person entitled to processing;
	16. **Data recipient -** a natural person, legal entity, or public institution to which the data was transferred, except for the Personal Data Protection Service;
	17. **Category of data recipient -** classification/grouping of data recipient according to the field of activity or organizational-legal form;
	18. **Third-party -** a natural person, legal entity, or public institution, except for the data subject, the personal data protection service, the person responsible for processing, the person authorized for processing, a special representative, and the person who is authorized to process data on the direct instructions of the person responsible for processing or the person authorized for processing;
	19. **Special representative** - an individual or legal entity registered outside Georgia, designated/appointed as a representative by the person responsible for processing or the person authorized for processing based on this law, as well as an association of persons without legal status
	20. **Personal data protection officer -** a person designated/appointed by the person responsible for processing or the person authorized for processing, who performs the functions provided for in Article 33 of the Law "On Personal Data Protection";
	21. **Data blocking** - temporary suspension of data processing (except storage);
	22. **Video monitoring -** visual image data processing using technical means placed/installed in public or private space, in particular, video control and/or video recording (except for covert investigative activity);
	23. **Audio monitoring** - sound signal data processing using technical means located/installed in public or private space, in particular, audio control and/or audio recording (except for covert investigative activity);
	24. **Profiling -** any form of automatic data processing, which involves the use of data to evaluate certain personal characteristics related to a natural person, in particular, the analysis and prediction of those characteristics that concern the quality of work performed by a natural person, his economic situation, health, personal interests, reliability, behavior, location or movement;
	25. **Depersonalization of data -** such processing of data when it is impossible to connect them to the data subject or establishing such a connection requires disproportionately large efforts, costs, and/or time;
	26. **Pseudonymization of data -** such processing of data when it is impossible to connect the data to a specific data subject without the use of additional information, and this additional information is stored separately and through technical and organizational measures, the data is not connected to an identified or identifiable natural person
	27. **Incident -** breach of data security, which leads to improper or accidental damage, loss, as well as unauthorized disclosure, destruction, modification, access to, collection/retrieval or other unauthorized processing of data;
	28. **Public institution -** an institution defined by subsection "a" of Article 27 of the General Administrative Code of Georgia (except for political and religious associations);
	29. **Current offense -** an offense provided for by the Law of Georgia "On Personal Data Protection", the commission of which begins with action and which is then carried out continuously. The current offense is terminated from the moment of cessation of the action.

# Article 4. Principles of data protection

1. To legally conduct the process of personal data processing by the university, in addition to the legal basis, it is necessary to observe the principles of data processing, therefore, the university ensures the observance of the following principle stipulated in Article 4 of the Law of Georgia "On Personal Data Protection" when processing personal data:
2. Data must be processed legally, fairly, and transparently for the data subject and without violating his dignity. The obligation of transparency of data processing does not apply to exceptional cases established by the law of Georgia "On Personal Data Protection";
3. Data must be collected/obtained only for specific, clearly defined, and legitimate purposes. Further processing of data for other purposes incompatible with the original purpose of data processing is not allowed;
4. Data shall be processed only to the extent necessary to achieve the relevant legitimate purpose. Data must be proportionate to the purpose for which they are processed;
5. Data must be true, accurate and, if necessary, updated. Taking into account the purposes of data processing, inaccurate data must be corrected, deleted, or destroyed without undue delay;
6. Data may be stored only for the period necessary to achieve the corresponding legitimate purpose of data processing. After achieving the purpose for which the data are processed, they must be deleted, destroyed, or stored in a depersonalized form, unless the processing of data is determined by law and/or a subordinate normative act issued under the law and the storage of data is a necessary and proportionate measure of the overriding interests of a democratic society to protect
7. To protect the security of the data, such technical and organizational measures should be taken during data processing that adequately ensure data protection, including against unauthorized or illegal processing, accidental loss, destruction, and/or damage.
8. In addition to the above principles, the University adheres to the legal basis for processing both non-sensitive and special categories of data, in particular, processing may be based on, among other things:
	1. Consent of the data subject - oral or written consent. For the processing of personal data to be based on the consent of the data subject, it is necessary that this consent: be voluntary; be expressed in advance, before data processing; be expressed after receiving information related to data processing; express a specific, clearly defined legal purpose for data processing; be expressed in such a way that the will of the data subject is established.
	2. The requirements stipulated by the legislation, which the university is obliged to fulfill (including the obligations defined by the by-laws regulating the field of education);
	3. Public interests;
	4. Superior legitimate interests of the University;
	5. Protection of university property and security;
	6. The proper implementation of the examination process;
	7. Making decisions about labor obligations, labor relations, and employment.

# Article 5. Data processed within the framework of the University's activities

1. The University processes personal data using automatic, semi-automatic, and non-automatic means. The University processes the following data:
	1. About administrative personnel - name, surname, photograph, date of birth, age, gender, address, personal number, copy of identity document, series and number of identity document, period of issue of identity document, copy of driver's license, autobiography, resume (CV), Information about education, information about knowledge of a foreign language, a copy of a diploma or a certificate confirming education, information about knowledge of computer programs, information about work experience, time of entering and leaving the building, phone number, e-mail address, bank account number, information about military obligation, held position (position), profession, information about compensation, information about conviction, Information on crimes against sexual freedom and integrity about the conviction for the crime, information about the state of health (form 100);
	2. About academic and invited staff - name, surname, photograph, date of birth, age, gender, address, personal number, copy of identity document, series and number of an identity document, date of issue of an identity document, copy of driver's license, autobiography, resume (CV ), information about education, information about knowledge of a foreign language, a copy of a diploma or a certificate confirming education, information about knowledge of computer programs, information about work experience, time of entering and leaving the building, phone number, e-mail address, bank account number, information about military obligation, held position, profession, information on compensation, information on conviction, information on conviction for crimes against sexual freedom and inviolability, information on health status (form 100);
	3. About the potential employee - name, surname, autobiography, resume (CV), copy of diploma or certificate of education, information about work experience, information about knowledge of foreign languages, information about knowledge of computer programs, time of entering and leaving the building, phone number, electronic mailing address;
	4. About the student - name, surname, personal number, series and number of the identity document, the expiration date of the identity document, photo, phone number, e-mail address, date of birth, knowledge of foreign languages, gender, education information, certificate, citizenship, military information about the obligation, a copy of the student's study card or its extract, all legal acts/acts determining the status of the student (enrollment order, status suspension, reinstatement), a copy of the order of the Ministry of Education, Science, Culture and Sports of Georgia on granting the right to study under the law, health conditions for determining special needs, time of entering and leaving the building, name, surname, contact information of legal representative or contact person;
	5. About the visitor - name, surname, time of entering and leaving the building;
	6. About persons participating in university projects and programs - name, surname, personal number, series and number of identity document, period of issue of identity document, photo, phone number, e-mail address, date of birth, knowledge of a foreign language, gender, education information, certificate, citizenship, state vehicle registration number; time of entering and leaving the building, name, surname, contact information of the legal representative;
	7. The terms of storage of data processed at the university are determined by the legislation of Georgia, the order of the Minister of Justice of Georgia dated March 31, 2010, N72, and the unified procedure of the " International Black Sea University" LLC.
	8. The university ensures the processing of all personal data (a file system catalog has been created) under the law, their registration in the file system catalog, indicates the purpose of processing, the basis, and the data storage period, which is then sent to the relevant state agency
	9. The University processes personal data, the basis of which is not prescribed by law, with the consent of the data subject.
	10. The University processes and issues such personal data in the form of an order, which is related to the granting, termination, suspension, and restoration of the student status, as well as the appointment of financial benefits and scholarships. The university is authorized to publish the order for public information if it is defined by law or concerns more than 50 persons.
	11. The University, in the interests of students, processes special categories of data, such as data related to health, only based on the request of the data subject and his written consent.
	12. The University has the right to process data for plagiarism prevention and detection.
	13. The university is entitled, in case of necessity, to have access to e-mails/domains created at the university level (www.ibsu.edu.ge) to detect criminals and/or ensure order in the university.
	14. The University is entitled to process personal data during disciplinary proceedings.
	15. The University is entitled to re-process personal data for career promotion for graduates. Conduct research on graduate employment rates.
	16. The University processes the data of minors based on the consent of the legal representative.
	17. The University ensures continuous monitoring of personal data protection through a personal data protection officer.
	18. The University ensures that the employee and student are informed about the processing of personal data through the contract and the data protection policy document.
	19. According to the legislation, in the event of a pandemic, epidemic, or other emergency, the university may collect information about the infection of employees regardless of the employees' will, if it serves to ensure a safe working environment and/or serves to manage the health care system.
2. The University is authorized to collect the following information: whether the employee/student has visited a country with a high risk of spreading the virus, whether the employee has symptoms of the virus, whether or not he/she has been in contact with a person(s) infected with the virus.
3. In case of doubt about the infection of an employee/student, the university applies to the relevant health agency and is subject to their instructions.
4. Disclosure of information about the infection of an employee/student by the University to another person is permissible if it is necessary to identify persons in contact with the employee/student and/or to prevent further spread of the virus.
5. The University keeps the obtained data for the period necessary for the implementation of the measures assigned to its competence. Subsequently, this data will be deleted, destroyed, or stored in a form that excludes the identification of a person.

# Article 6. Data processing during remote work

1. When conducting distance learning, the university, as an educational institution, is authorized to use modern communication systems (eg: Webex, Meet, Zoom, Teams, Classroom, Moodle, etc.) to hold distance meetings.

2. When working in remote mode, the university takes into account the following circumstances:

2.1. When working remotely from home, the employee of the university administration must use the office computer;

2.2. If necessary, the university provides remote access to the work computer from the home computer using modern and up-to-date programs.

2.3. If necessary, the university ensures that operating systems (MS Windows, MacOS) are regularly updated on the work computer;

2.4. If necessary, the university provides a complex password (containing at least 10 characters, upper- and lower-case Latin letters, numbers, and special characters) for entering the electronic systems that can be accessed under the name of an individual user. E.g.: #,$, &, @, and do not use the same password for logging into different systems. Only encrypted VPN connection means are used to access internal electronic resources of the service. Antivirus programs are used, including free versions. If requested by the user, backup copies of data or important documents are made and data are stored on the service server, confidential data is encrypted, including using free encryption programs (for example, VeraCrypt, BitLocker, etc.). No foreign USB data carriers are used. The physical security of the university computer is ensured.

2.5. When necessary, the University ensures the security of the University's wireless network equipment, namely:

a) Protecting the password of the user assigned to manage the wireless network device from unauthorized persons;

b) Access to the control panel of the wireless network device from the Internet is restricted when necessary;

c) Modern encryption methods (for example, WPA2 or WPA3) are used for wireless network connection;

d) The password for connecting to the wireless network device is complex, consisting of at least 8 characters;

e) The password for connecting to the wireless network device is periodically changed.

2.6. To protect the wireless network in the university, the following policy is implemented: the network is divided into 2 parts: 1) for students who have access only to the Internet and library databases; 2) for administration, among which users in a certain IP range have access both to the Internet and to the bases and services in the internal network.

# Article 7. Purposes of using processed data

Data processed at the University are used for various purposes, namely:

1. Organization of competitions for vacant positions, management of personal affairs of persons employed at the university, creation, and organization of reserve bases for in-demand positions, evaluation of personnel, implementation of offers for employed persons, signing of contracts, business trips, vacations, and other documents, personnel survey;
2. Legal provision of proceedings, organization, and control of document circulation, development of regulatory acts, review of statements of individuals, provision of legal advice on issues related to the educational process, representation of the university in court and third-party relations;
3. Conducting evaluations, educational, scientific, and research work, as well as improving the professional development of staff, evaluating students' activities and quality control, planning and managing library activities;
4. Electronic case management, management of student training bases, effective communication with university employees, academic and invited staff;
5. Regulation of student status (enrolment, suspension, termination) and financial situation;
6. Ensuring and preventing security on the territory of the university, improving the quality of services provided by the university, protecting the property and security of the university, and conducting the examination process on time.

# Article 8. Entities with the right to access data

Within the scope of the relevant purpose and proportions, access to the data processed at the university within the scope of its competence is possible to have:

Rector, Governing Board, Rector's Advisor, International Relations Department, Marketing and Public Relations Department, Ombudsman, Vice-Rectors, Academic Process Quality Assurance Council, Strategic Development Service, Human Resources Management and Development Service, Student Services and Registry Service, Case Management Department, Archives, Student and Alumni Development Department, IBSU Academy, Innovation and Entrepreneurship Center, Student Extracurricular Activities Service, Alumni Relations Service, Career Planning and Development Service, Learning Process Monitoring Service, Information Technology Service, University Schools, Language Center, Academic Writing Center, Research Promotion and Project Management Office, Publishing House, Library, Finance Department, Finance Office, Student Financial Services Office, Accounting, Legal Office, Procurement and Logistics Department, Procurement Office, Technical Office, Labor and safety service, medical station, cleaning service, quality assurance service, internal quality assurance service, school deans, administrative director of educational programs, academic head of educational program, School Board, School Dissertation Board, Research Center (if any), Administrative Affairs Manager, Academic and Invited Staff.

# Article 9. Administration of the electronic system for managing academic processes

1. To effectively manage the educational process, the university administers an electronic system for managing academic processes.
2. The administration of the electronic system for managing academic processes can be carried out by involving the appropriate structural unit in the university or an authorized person (external source).
3. For the purpose given in the first paragraph, the involvement of the authorized person in the process is allowed based on the contract, where the rights and duties of the authorized person are defined.
4. To ensure the legal processing of data by the authorized person, periodic control of his activities is carried out within the framework of the administration of the electronic system for managing academic processes.
5. An appeal to the authorized person on matters related to the protection of the right of the data subject and the processing of his data can be carried out by the university on its initiative or the basis of the application of the data subject.

# Article 10. Implementation of video control and audio control

1. To ensure the safety of students and other persons, protect minors from harmful effects, protect property, and/or protect confidential information, video surveillance is carried out on the outer perimeter of the university building, in the entrance and corridors of the building, and the auditoriums.

2. On the outer perimeter of the university, in corridors and auditoriums, a warning sign is placed in the appropriate visible places, as well as for the persons employed at the university and students, the notification about the video control is carried out in writing;

3. In the university, the production of video control to report to work, working time, leave the university, or evaluating the quality of work is not allowed;

4. The implementation of audio control is allowed only during the implementation of remote services by the university, or depending on the goals of service improvement, in case of prior informing of the subject;

5. Records obtained as a result of video monitoring and audio monitoring are stored to conduct the exam process for 7 days, and for property and security protection - for 30 days.

6. The university has placed warning signs of video monitoring in a visible place.

7. The rector, vice-rector in the field of administration, educational process monitoring service, and guards of a private security organization have access to the video surveillance system of the university.

8. For operative-search measures and crime investigation, upon request, the University shall hand over the video recording to the relevant agencies, only based on the judge's ruling, or in the case of urgent necessity, based on the motivated resolution of the prosecutor.

# Article 11. Registration of entry and exit to the building

1. Turnstile systems are installed in the university, which records the cardholder's identity, entry/exit time, and date, for timely reporting to the workplace and leaving at the appropriate time, as well as calculating working hours.

2. Registration can be done with an identity card or using electronic cards, on which the name, surname, and unique card number of the person employed at the university will be printed.

3. In addition to the information specified in the second point, as a result of the registration, the dates and times of entering and leaving the university building will also be obtained.

4. For control, the University collects the following data: name, surname, identification document number, entry and exit dates, time, and reasons.

5. The Human Resources Management and Development Service has access to the access system to record entry and exit from the university building.

6. Entry-exit control of students/academic staff through fingerprint is not allowed.

7. The employee is obliged to report to work and leave the workplace on the device at the workplace, which is located at the entrance of the university.

8. The Human Resources Management and Development Office is responsible for monitoring punctuality and producing timekeeping reports at the university, which will submit the relevant report to the rector or vice-rector in the field of administration upon request.

# Article 12. Use of e-mail and telephone number

1. For efficient and quick communication, the university processes e-mails and phone numbers of employees, academics, invited staff, interns, service persons, students, graduates, and persons participating in university projects.
2. The use of e-mail and telephone numbers to provide news and send advertising messages (direct marketing) is allowed only with the subject's consent.
3. The data subject has the right to request the termination of the use of the e-mail and/or telephone number for marketing purposes, which must be complied with immediately.

# Article 13. Rights of the data subject

1. The data subject has the right to request the person responsible for the processing to confirm whether the data about him or her is being processed, whether the data processing is justified or not, and to receive the following information free of charge under the request:

a) About the data that is being processed, as well as the basis and purpose of this data processing;

b) About the source of data collection/retrieval;

c) About the period (time) of data storage, and if it is impossible to determine a specific period, about the criteria for determining the period;

d) About the rights of the data subject;

e) About the legal basis and purposes of data transfer, as well as appropriate data protection guarantees, if the data is transferred to another state or international organization;

f) About the identity of the data recipient or the categories of data recipients, including information about the basis and purpose of the data transfer, if the data is transferred to a third party;

g) About automated processing, including the decision made as a result of profiling and the logic used to make such a decision, as well as its impact on data processing and the expected/probable result of processing.

2. The person responsible for the processing is entitled to provide the data subject with any information as necessary to ensure the transparency of the data processing.

3. Unless otherwise stipulated by the legislation of Georgia, the data subject has the right to choose the form of information provision. In addition, if the data subject does not require the provision of information in another form, the information will be provided to him in the same form in which the information was requested.

4. The data subject has the right to get acquainted with the person responsible for the processing of the personal data about him and to receive copies of this data free of charge.

5. The data subject has the right to get acquainted with the data and/or receive their copies no later than 10 working days after the request, except for the case when a different period is established by the legislation of Georgia and/or in special cases. In special cases, with proper justification, the mentioned period can be extended by no more than 10 working days, about which the data subject must be notified immediately.

6. The data subject has the right to get acquainted with the data provided in the first paragraph of this article and/or to receive their copies in the form in which they are kept at the university. The data subject also has the right to request the provision of copies of the data about him in a different form, in exchange for a reasonable fee set by the University for processing if this is technically possible.

7. The data subject has the right to request the university to correct, update, and/or fill in false, inaccurate, and/or incomplete data about him.

8. No later than 10 working days after the submission of the request stipulated by the first paragraph of this article by the data subject (if no other period is established by the legislation of Georgia), the data must be corrected, updated, and/or filled in, or the data subject must be informed of the grounds for refusing the request and explain the procedure for appealing the refusal.

9. If the University independently discovers from the data subject that the data in its possession is false, inaccurate, and/or incomplete, it must correct, update, and/or supplement the data within a reasonable time and notify the data subject within 10 working days of the data correction.

10. The data subject has the right to request the University to stop processing (including profiling), delete, or destroy data about him. No later than 10 working days from the request stipulated in this paragraph (unless otherwise established by the legislation of Georgia), data processing must be stopped and/or data must be deleted or destroyed, or the data subject must be informed of the grounds for refusing the request and explain the procedure for appealing the refusal.

11. The data subject has the right, in case of processing of data about him in a publicly available form, to additionally request the university to limit access to data and/or delete copies of data or any Internet link connecting to data.

12. The data subject has the right to request the University to block the data if one of the following circumstances exists:

a) The data subject disputes the validity or accuracy of the data;

b) Data processing is illegal, although the data subject opposes their deletion and requests data blocking;

c) The data are no longer needed to achieve the purpose of their processing, although the data subject needs them to submit a complaint/lawsuit;

d) The data subject requests the termination, erasure, or destruction of data processing and this request is being considered;

e) There is a need to store data for evidence.

The data subject has the right to receive information about the decision to block data or the grounds for refusal to block data, immediately, but no later than 3 working days after the request.

13. The data subject has the right, at any time, without any explanation or justification, to withdraw the consent given by him. In this case, at the request of the data subject, the data processing must be stopped, and/or the processed data must be deleted or destroyed no later than 10 working days after the request if there is no other reason for the data processing. The data subject has the right to express consent in the same form in which consent was given.

14. The data subject has the right, in case of violation of the rights provided for by this law and established rules, by law

to apply to the personal data protection service, the court, and/or the higher administrative body in the prescribed manner.

# Article 14. The person responsible for personal data processing at the University

1. To effectively protect the subject's rights and fulfill the requirements of the personal data protection legislation, the person responsible for personal data processing is defined in the university - the personal data protection officer (hereinafter - the officer).
2. The officer's rights and duties are:
	1. Providing advice and assistance to the University, authorized person, administrative academic, and invited staff, students, and alumni on data protection issues.
	2. Analyzing the university's internal regulatory document related to data processing and the processing process at periodic intervals of 3 months for compatibility with the legislation.
	3. Responding to incoming applications and complaints regarding data processing.
	4. Create a file system catalog and submit it to the state inspector.
3. The officer is independent in the performance of his rights and duties and is accountable for their performance directly to the rector. It is not allowed to create an obstacle or interfere with the work of the officer.

# Article 15. Technical and organizational provision of security

1. The technical and organizational security standard of data processing is provided at the university, which applies to the entire cycle of data processing;

2. Safety standards are based on the following principles:

2.1. Data protection is an integral feature of the processing process;

2.2. The full functionality of the procedures implemented for the security of the processing, without compromising the purposes of the processing or the rights of the subject;

2.3. Operation during the full processing cycle;

2.4. Transparency and accountability to the subject;

2.5. Orientation of the processing process depends on the priority of protecting the rights of subjects.

3. The University ensures the recording of all actions performed concerning the data available in electronic form, and for the data available in non-electronic form, it ensures the recording of all actions related to their disclosure and/or change.

4. The university, with an interval of no more than 6 months, evaluates the adequacy and effectiveness of the adopted technical and organizational security standards, and if necessary, ensures their renewal.

5. Security measures include the following:

5.1. Raising staff awareness in terms of information security. conducting awareness-raising meetings and relevant training for persons employed at the university (including academic and invited staff), authorized persons, as well as students;

5.2. Establishing minimum password complexity requirements for academic, invited, or administrative personnel to access their account in the electronic data system;

5.3. Use of licensed software and regular updates of security measures;

5.4. Prohibition of leaving documents and files containing personal data unattended.

6. Any person employed by the university is obliged to be aware of the responsibility assigned to him and not to allow the processing of personal data, including disclosure, without the existence of a basis provided by law.

# Article 16. Responsibility of staff and students

1. University employees and students are obliged to follow the University's data protection policy document.

2. The university informs the administrative, academic, and invited staff in pre-contractual relations about what kind of personal data the university processes about them.

3. Persons employed at the university are prohibited from leaving documents and files containing personal data unattended.

4. University staff is obliged not to disclose and not to transfer personal data of others to other persons. They should protect personal data even if they are no longer employed by the university.

5. If persons are no longer employed by the university and violate the specified rule, the university is entitled to demand compensation for damages by way of recourse.

6. Violation of the established rules on personal data processing is the basis for initiating disciplinary proceedings against university staff and students.

7. Before signing an educational service contract with the university, the university provides information to students about what kind of personal data the university processes about them.

8. Students are obliged to comply with the University's Personal Data Protection Policy document when they represent the University and participate in various activities on behalf of the University.

9. Students are obliged to promptly notify the university about changes in their personal data.

10. Violation of the rules established by the University's personal data protection policy is the basis for initiating disciplinary proceedings against the student.

# Article 17. Incident

1. "International Black Sea University" LLC is obliged to record the incident, the resulting result, and the measures taken, no later than 72 hours after the discovery of the incident, to report it in writing or electronically to the Personal Data Protection Service, unless it is unlikely that the incident will cause significant damage or/and will create a significant threat to basic human rights and freedoms.

2. The person authorized for processing is obliged to record information related to data processing, including information about the incident. This obligation is manifested for all detected incidents, regardless of whether or not the incident is subject to notification to the Personal Data Protection Service and/or to the data subject.

# Article 18. Evaluation of the incident

1. The severity of the violation of human rights and freedoms as a result of the incident must be assessed by the university or the person responsible for the processing, taking into account the following criteria:

1.1. Type of incident

The incident is always related to personal data and according to the generally recognized principles of information security, it is divided into the following types:

a) Violation of privacy;

b) Violation of integrity;

c) Violation of availability.

1.2. The category of personal data affected by the incident;

a) Persons in need of special social or legal protection as data subjects;

b) Degree of ability to identify data subjects;

c) The consequences for the rights and interests of the data subject(s);

d) Special nature of the activity of the person responsible for processing;

e) Scale of the incident, in terms of the number and/or volume of the data subject and/or personal data;

f) Other circumstances.

# Article 19. International data transfer

1. Depending on the goals of the university's activity and taking into account the relevant grounds, the processed data can be transferred to an international organization and/or to a person located/established in another state, including private or public organizations;

2. The University is authorized to send personal data only to those countries whose list has been approved by the relevant order of the Personal Data Protection Service - "On approval of the list of countries with appropriate guarantees of personal data protection".

3. For the international transfer of data, the University takes appropriate measures to ensure the protection of the subject's rights and the security of the transfer.

4. For the purpose stipulated in the third point, the university takes the following measures for international transfer:

4.1. Assesses the risks associated with the international transfer of data;

4.2. Signs a relevant contract with the receiving party, which, among other things, provides for the rights and obligations of the university and the receiving party, guarantees of protection of the subject's rights and appropriate methods of transfer;

4.3. If necessary, agrees and obtains permission from the Personal Data Protection Service regarding international transfer;

4.4. If necessary, monitor the processing of the transferred personal data to comply with the law, including requesting information regarding the processing process.

4.5. The University registers the facts of providing information to third parties, what data was provided, to whom, when and on what legal basis.

# Article 20. Final Provisions

1. This document is valid upon its approval by the Rector.

2. This policy document is accompanied by a list of personal data protection documents taken into account by the personal data protection policy document of the LLC, which comes into force upon approval of the same policy document.

3. Amendments and additions to the policy document are made according to the rules established by the current legislation of Georgia and by the order of the rector

**Appendix 1**

**Informational banner for the site**

Who are we?

" International Black Sea University" LLC is a higher educational institution registered under the legislation of Georgia

Identification code: 229275405

Address: d. Agmashenebeli Avenue, 13th km, #2; Tbilisi 0159, Georgia.

Web. Page: <https://ibsu.edu.ge>

**Introduction**

As a leading university, it is important for us to provide a consistent and high standard of protection and security of the personal data of our students and employees.

Please familiarize yourself with the information about the legal and technical mechanisms for obtaining and processing your personal data, the data subject's (your) rights, and their protection.

Who is the addressee of this document?

Addressee of the document:

• University administrative staff;

• Academic and invited staff;

• Students and graduates;

• Service providers;

• Legal representatives or contact persons of minor students;

• Any person who participates in university projects and events.

How do we collect your data?

The source of your data for the University is:

• Contacting you for service purposes (including telephone communication, electronic contact, and/or visit);

• Your use of our services;

• Using remote channels of the university;

• Your use of the official website of the university and its functions;

• We also receive information about you from public sources and third parties, in the presence of a relevant legal basis and, if necessary, based on your consent (eg from the Ministry of Education, Science and Youth of Georgia and legal entities of public law included in its system).

What kind of information do we process about you?

The information we process may include the following categories of data in proportion to the purpose of their processing:

**Identification data** - name, surname, date of birth, personal number, identity and/or citizenship document data, gender, citizenship, place of birth, address (registration and actual), nationality, photograph, sample signature, and others;

**Documentary** - identity card, passport, driver's license, birth certificate, certificate of compatriot living abroad, residence certificate, temporary identification card, form 100, a certificate from state agencies (e.g.: certificate of conviction), document confirming the right to representation and others;

**Contact information** - address (legal and actual), e-mail, phone number, and others;

**Socio-demographic information** - information about service/profession, citizenship, education, as well as information about social status and income, etc.;

Financial information - information about the economic and financial situation, about the payments and/or transfers;

**Contractual information** - about the services provided by the university;

Special category data - information about health status, information about administrative detention, conviction, accusation, and others;

**Data about the technological device** - IP address, ready records (cookies).

**Recordings** - audio and video recordings;

**Data obtained during communication** - data obtained through e-mail, telephone, chat, social media, or other communication channels;

**Public data** - information obtained from public sources;

**Data created by the University** - data created as a result of data analysis. data that the university should process by law;

**Ready-made records (Cookies)** - to improve the university's services, we collect the so-called cookies when using the website and other remote platforms. ready records about you. Cookies are used to personalize, improve, and protect your experience while using the website and other remote platforms. In particular, to simplify navigation, offer information in the desired format, improve search parameters, secure user authentication, and marketing, optimize the design of web pages, and better adapt to the user.

When visiting the University's website and remote channels, you have the opportunity to accept/opt out of the use of ready-made recordings and/or manage the purpose of using ready-made recordings according to your wishes (for example, you can opt out of the use of ready-made recordings for analytical and/or marketing purposes).

Purpose of data processing:

We process your data only for lawful purposes and to the extent appropriate to them.

Basics of personal data processing

The basis for processing your data is:

• Your voluntary consent to data processing;

• Obligations stipulated by legislation;

• The need for data protection to enter into a contract with you or to fulfill an existing contract;

• The need to process data to provide services to you/review your application;

• The need to process data to protect the legitimate interests of the University or third parties;

• Publicly available data

• The video surveillance system is used for crime prevention, detection, protection of personal safety and property, as well as protection of confidential information.

• We process special category data only with your written consent.

When we share your data with third parties

To comply with a legal or contractual obligation, where there is a relevant legal basis, we may share your data with:

• To your representative/legal representative;

• Bodies defined by legislation;

• To other third parties with your consent.

We may share your data in another state if there are grounds for data processing provided by the Georgian Law "On Personal Data Protection" and appropriate guarantees of data protection and protection of the data subject's rights are provided in the respective state.

To properly protect your data, before transferring personal data to third parties, we check whether they have adopted appropriate organizational and technical data protection measures.

You have the right to:

• To receive information about the data processed about you, in particular, what data is processed, what is the purpose and legal basis of their processing, information about the source of data collection and data transfer;

• Get acquainted with the protected data about you and receive copies of documents/records containing your personal data following the procedure established by the legislation of Georgia;

• Request correction, update, and/or completion of erroneous, inaccurate, and/or incomplete data;

• Request the termination, erasure, or destruction of data processing if:

* Ask for consent, which is the sole basis for data processing; The processing of the data is no longer necessary for the purpose for which it was processed;
* Data processing is illegal.
* Request data blocking if the authenticity or accuracy of the data is disputed;
* The processing of data is illegal, although you do not want them to be deleted and you only ask for them to be blocked;
* The data is no longer necessary to achieve the purpose of its processing, although you need it for legal proceedings;
* The request for termination of data processing, erasure, or destruction is under review;
* There is a need to store data for evidence.
* You have the right to withdraw/refuse your consent to data processing at any time and request the deletion of data processing based on it. We will stop processing the data and delete the data that has already been processed unless there is another basis under the data processing law. If the data processing is based on your consent and it is technically possible, request the porting of the personal data provided by you, i.e. receive it in a structured, usable, and electronic form or transfer it to another processor;
* In case of violation of your rights, you have the right to apply to the Personal Data Protection Officer, the Personal Data Protection Service, and/or the court;

**Limitation of your rights**

Your rights may be restricted if their exercise is jeopardized by:

• State security, information security, and cyber security and/or defense interests;

• Public safety interests;

• Crime prevention, crime investigation, criminal prosecution, and justice implementation;

• Detection of violations of professional, including regulated professional, ethics norms by the data subject and assigning responsibility to him;

• Your or others' rights and freedoms;

• Protection of state, commercial, professional, and other types of secrets stipulated by law;

• Justification of the legal claim or objection.

The measure of restriction of rights is used by the university only in an adequate and proportionate scope for the restriction.

**Data security protection**

We store the processed data about you under the requirements of the law. The University provides physical, technical, and organizational safeguards to protect your data. The University protects the security of electronic devices, files, and buildings. The University also implements physical, electronic, and procedural controls to protect your data from unauthorized access, use, transfer, loss, or destruction.

University employees adhere to data privacy, security policies, and procedures under legislation and internal organizational documents.

Data retention period

We store your data:

• To follow the terms defined by the legislation of Georgia;

• Or for a period that is necessary to achieve a specific purpose of processing, established within the scope of service provision and/or in the contract.

**Your obligations**

It is necessary for us to have complete and correct information about you, therefore, please notify us in case of any change in your contact or other information.

If you want to receive information about your data or take additional action, please contact us by e-mail (info@ibsu.edu.ge). Your request will be reviewed and you will receive a response within 10 days.

**Contact information:**

In addition to matters related to personal data protection, you can contact us at: +995 555 85 91 91

**Changes:**

Changes may be made to the Personal Data Protection Policy from time to time. The updated document indicating the date of change will be published on the university website. on the page.

**Appendix 2.**

**Use/Processing/Sharing of Personal Data**

**Typology Possible relationships of purpose**

This table presents the purpose of personal data processing with reference to the relevant legal grounds in each specific case.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Type of personal data | Purpose of use/what we use it forin your personaldata | Legal basis | Data subject | Storage period | Our legitimateinterest | How we collect personal data/where and with whom it is stored |
| Documentary: identity document, photo, birth certificate, contact information, bank details and other personal identification documents | Signing a labor or one-time service contract | Legal and contractual obligation | Administrative and academic staff, invited lecturers, students, potential employees, visitors, and participants in university projects and programs | During the period of validity of labor, service/other type of legal relationship. | Effective performance of legal duties and contractual obligations of the University; | From the data subject, stored at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. Student Services and Registry Office:Vefkhia Kamadadze, Tamta Chkhenkeli, and Natia Maisuradze and accounting: Megi Kvitsiani, Yana Grigolaia, Aeti Abashidze. |
| Autobiography, resume (CV), information about education, information about work experience, information about research, certificate of scientific-pedagogical activity. | Signing a labor or one-time service contract | Legal and contractual obligation | Administrative and academic staff, invited lecturers, potential employees, participants in university projects and programs | During the period of validity of labor, service/other type of legal relationship. | Effective performance of legal duties and contractual obligations of the University; | From the data subject, stored at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. |
| Data related to health status | Considering work, lectures, exams, and university projects as an honorable reason for missing/not showing up, determination of special need | Legal and contractual obligation | Administrative and academic staff, invited lecturers, students, and participants in university projects | During the period of validity of the agreement concluded with the data subject. | Effective performance of the university's statutory duties and contractual obligations; | From the data subject, stored at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili, and Ia Kojuri. with the head of the training process monitoring service. |
| Notice of conviction for a crime against sexual freedom and inviolability and deprivation of the right | Signing a labor or one-time service contract | Legal and contractual obligation | Administrative, academic staff, and invited lecturers | During the period of validity of the agreement concluded with the data subject. | Effective performance of legal duties and contractual obligations of the University; Ensuring compliance with relevant regulations for us. | From the data subject, stored at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. |
| Time to enter and leave the building | Accounting for working time, compliance with safety norms | Legal and contractual obligation | Administrative Staff | During the period of validity of the agreement concluded with the data subject. | Effective performance of legal duties and contractual obligations; | The system of turnstiles is kept at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. |
| Vehicle registration number | Ensuring entry into the university building, | Contractual obligation | Administrative Staff | During the period of validity of the agreement concluded with the data subject. | Effective performance of legal duties and contractual obligations; Ensuring compliance with regulations | The data subject is stored by the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili, by the Security Service: Shota Tskhakaia, Ioseb Gagua, Jhony Atanasiani, Merab Sakvarelidze, Giorgi Kochladze, Levan Kvashilava. |
| Information about education, certificate, citizenship, copy of military registration certificate, copy/extract of study card, all legal acts/acts determining student status (enrollment order, status suspension, restoration), information of legal representative or contact person, | Determination of compliance of the student's data with the criteria defined by the university | Obligation established based on legal, intra-university regulations | Student | During the validity period of the agreement signed between the student and the university | Effective performance of legal duties and contractual obligations; Ensuring compliance with relevant regulations for us | From the data subject, stored at the case management department: Svetlana Kevkhishvili, Mariam Shanidze. At the Student Services and Registry Office: Vefkhia Kamadadze, Tamta Chkhenkeli and Natia Maisuradze |
| Information related to social relations: about family members | Use of an insurance policy, use of non-standard fees during the study period, and determination of the criteria necessary for the appointment of scholarships. | Statutory and internal university regulations | Administrative and academic staff, student | During the period of validity of the agreement signed between the student and the university, the administrative staff and the university | Effective performance of legal duties and contractual obligations; Ensuring compliance with relevant regulations for us | From the data subject, stored at the Human Resources Management and Development Service: Tamar Churadze and Nino Mchedlishvili. At the Student Services and Registry Office: Vefkhia Kamadadze, Tamta Chkhenkeli, and Natia Maisuradze, Manager of the Student Financial Services Service: Mariam Imnaishvili |
| Lectures and exams | Regular implementation of the educational process, protection of property | Statutory and internal university regulations | Administrative and academic staff, invited lecturers, students | To conduct the examination process promptly, for 7 days, and to protect property and security - for 30 days. | Effective performance of legal duties and contractual obligations; Ensuring compliance with relevant university regulations | Based on video monitoring, is kept with the heads of the training process monitoring service and the security service: Natia Bezhashvili, Besiki Barateli, and Ioseb Gagua. |
| Trainings organized by the relevant structural units of the university | Raising qualifications for university staff | Statutory and internal university regulations | Administrative and academic staff invited lecturers | Until the end of the training | Effective performance of contractual obligations | Based on the attendance sheet, it is kept at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili/ IBSU Academy: Sofio Maglakelidze |
| Master's and doctoral thesis defenses | Confirmation of academic degree | Statutory and internal university regulations | Master's and Ph.D student  | Constantly | Effective performance of statutory duties, ensuring compliance with relevant university regulations | With the respective schools of the university |
| Academic competition interviews | Determination of the suitability of the skills and qualifications of the staff to the position to be held | Legal regulations of the previous contractual relationship | academic staff | Before the end of the pre-contractual stage | Effective performance of legal duties | Based on the evaluation sheet, is kept at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. |
| Invited lecturer academic competition interviews | Determination of the suitability of the skills and qualifications of the staff to the position to be held | Legal regulations of the previous contractual relationship | Invited lecturer  | Before the end of the pre-contractual stage | Effective performance of legal duties | Based on the evaluation sheet, is kept at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. |
| Interviews for the administrative staff recruitment competition | Determination of the suitability of the skills and qualifications of the staff to the position to be held | Legal regulations of the previous contractual relationship | Administrative Staff | Before the end of the pre-contractual stage | Effective performance of legal duties | Based on the evaluation sheet, is kept at the Human Resources Management and Development Service: Tamar Churadze, Nino Mchedlishvili. |