Georgian American University

Data Protection Impact Assessment Document

Contents

Preamble

This Data Protection Impact Assessment (DPIA) document has been developed by LLC Georgian American University (hereinafter – the University) in accordance with the Law of Georgia on "Personal Data Protection," the Order No. 21 of the Head of the Personal Data Protection Service of Georgia approving the "Criteria and Procedures for Determining Circumstances Requiring a Data Protection Impact Assessment," and other requirements established by law. This document (hereinafter – the "Document") is used by the University in the processing of personal data of students, academic staff, invited lecturers, contractors, and other employees, and applies to any form of data processing carried out by the University.

The Data Protection Impact Assessment (DPIA) was conducted to evaluate potential privacy risks to data subjects in connection with data processing within the University. The purpose of this document is to ensure compliance with the General Data Protection Regulation (GDPR) and the Law of Georgia on "Personal Data Protection," as well as to implement necessary measures for mitigating identified risks.

This Document represents a core element of the broader framework for data protection and confidentiality. It supports the identification of specific risks considering the nature of the organization's activities, evaluates the potential impact of those risks, and provides for the implementation of appropriate preventive measures to reduce them.

Legal and Regulatory Context

This document has been developed in accordance with the following legal frameworks:

a) Article 35 of the GDPR, which obliges an organization to conduct a Data Protection Impact Assessment when data processing, by its nature, is likely to result in a high risk to the rights and freedoms of natural persons due to potential compromise of their personal data;

b) The Law of Georgia on "Personal Data Protection", which sets forth similar requirements for the protection of personal data, including obligations related to risk assessment and ensuring principles of confidentiality.

The need to develop this document is especially crucial in cases where data processing involves:

Systematic monitoring of individuals (e.g., through video surveillance);

Large-scale processing of special categories of data, such as health or biometric data;

Use of innovative technologies that may impact data confidentiality (e.g., automated decision-making or

processing based on artificial intelligence).

The Importance of the Document in the Data Processing Lifecycle

The development of this document is essential not only for ensuring the organization's compliance with the law but also for strengthening the trust of data subjects and other interested parties. By adopting this document, the University demonstrates its commitment to transparency and accountability in data processing, reduces the risk of data breaches or misuse, and establishes a legal framework at the organizational level for the protection of personal data.

The document provides a comprehensive analysis of the accompanying and potential outcomes of data processing and assists the organization in designing and maintaining workflows, technical systems, and policies that safeguard personal data. This proactive approach not only protects the organization from regulatory sanctions but also governs its relationships with clients, users, and employees by ensuring the protection of their privacy.

The Key Areas Covered in the Document Include:

- The lawfulness of data processing;
- The necessity and proportionality of processing the information obtained by the University about data subjects;
- Assessment of potential risks to safeguard the fundamental rights and freedoms of individuals;
- Effective mechanisms for preventing identified risks;
- Measures and technical safeguards implemented by the University to ensure data protection;
- The rights and obligations of data subjects and the persons responsible/authorized for data processing.

General Information about the Data Controller

LLC Georgian American University is a higher education institution that processes the personal data of students, academic staff, invited lecturers, contractors, and other employees—including minors—in the course of fulfilling its institutional functions. To fully exercise its rights and obligations, the University requires the processing of personal data of data subjects. This process begins from the moment applicants register at the University and continues throughout the entire academic lifecycle, as well as for the duration of relevant contracts in the case of employees or other individuals.

The data processed about the subjects includes personal information of students, lecturers, and other staff members, as well as information related to students' academic performance and engagement during their studies at the University.

For the purpose of ensuring higher education services, the University operates as part of a unified system that includes the Ministry of Education, Science, and Youth of Georgia, and its subordinate legal entities under public law. These entities define the purposes and forms of data processing within their scope of authority. Accordingly, data at the University is processed through both electronic platforms and paper-based formats.

The protection of personal data is a right of every member of the university community. Therefore, data processing is a clearly regulated process, and the University ensures the protection of all members' personal data. For this purpose, it has developed a personal data processing policy and appointed a Data Protection

Officer.

General Information About Authorized Data Processors and Joint Controllers

The University engages authorized data processors who process personal data solely for the purposes of fulfilling the University's objectives. Contracts are signed between the University and these processors, which regulate the protection of personal data in detail and oblige the processors to act in full compliance with the Law of Georgia on "Personal Data Protection." These written agreements also cover the issues stipulated in Paragraphs 2 and 3 of Article 36 of the same law.

The University monitors the implementation of appropriate technological and organizational measures by the processors, as well as their data processing activities in the course of performing their functions. Upon request, the University provides data subjects with information regarding the authorized processors. Authorized processors are not themselves considered data controllers, as the processing they carry out serves the purposes of other client organizations, and the specific means of processing are determined by the instructions of those clients. Therefore, in the context of data processing, authorized processors process data on behalf of or under the instruction of the data controller.

Authorized data processors are responsible solely for the security of the data they process and for the duration during which the processing takes place.

The University also engages joint data processors. LLC Fitpass Georgia, LLC Insurance Company Euroins, and JSC Bank of Georgia provide the University with specific services. In particular:

- **Fitpass Georgia** offers corporate wellness services through which University staff members can access more than 40 sports activities at over 150 venues on a daily basis, covered by a single monthly subscription. The University ensures that data subjects give their consent to the processing and transfer of their personal data by completing an electronic form.
- **Insurance Company Euroins** provides health insurance services for University staff.
- **Bank of Georgia** cooperates with the University for the purpose of issuing salary cards for employees.

LLC Fitpass Georgia, LLC Euroins, and JSC Bank of Georgia are considered joint data processors because they process data for their own organizational purposes, and the specific means of processing are determined by their own internal policies.

Accordingly, in the context of data processing, these companies act as joint processors who process personal data on behalf of their own organizations and in their own names. Contracts (written agreements) are concluded between the joint processors and the data controller, which define the legal basis and purposes of data processing, the categories of data to be processed, the duration of processing, and the rights and obligations of both the controller and the processors. These written agreements also cover the matters provided for in Paragraphs 2 and 3 of Article 36 of the Law of Georgia on "Personal Data Protection."

As joint processors, LLC Fitpass Georgia, LLC Euroins, and JSC Bank of Georgia are responsible only for the

security of the personal data they process and only for the period during which such processing takes place.

Service Providers

Organizations that process personal data on behalf of the University—such as cloud storage providers, IT support vendors, or marketing agencies—are obligated to comply with data protection requirements through Data Processing Agreements (DPAs). These agreements ensure that the processors uphold the necessary standards for personal data protection.
Supervisory Authorities
In terms of compliance, the relevant data protection supervisory authority (e.g., the Personal Data Protection Inspector of Georgia or equivalent GDPR supervisory bodies) has the right to oversee the legality of processing activities, especially in cases involving high-risk data processing.

Data Subjects

The University processes personal data of the following categories of individuals:
a) Current and former employees, including those employed under labor contracts;
b) Candidates participating in competitions announced for vacant positions;
c) Interns;
d) Students, administrative and academic staff;
e) Invited staff;
f) Visitors;
g) Minors;
h) Other individuals captured within video surveillance areas;
i) Contractors (including legal entities under private or public law, and natural persons);
j) Individuals attending informational sessions held within the framework of various projects.

Internal Stakeholders

- Data Protection Officer (DPO): Responsible for overseeing the University's data protection strategy and ensuring compliance with privacy laws.
- Human Resources (HR): Involved in processing employee data for recruitment, employment management, and payroll purposes.
- Marketing Team: Responsible for processing customer/user data for behavioral analysis, campaign execution, and maintaining communication.
- IT Department: Manages the technical infrastructure that supports the collection, storage, and security of personal data.
- Legal Department: Provides guidance on compliance with data protection regulations, oversees data processing contracts, and handles the rights of data subjects.

Objectives of Conducting a Data Protection Impact Assessment (DPIA)

1. The Data Protection Impact Assessment (DPIA) facilitates the ability of the data controller to:
2. Proactively identify risks to personal data at the early stage of processing activities;
3. Identify, assess, and substantially mitigate threats to fundamental rights and freedoms arising from data processing;
4. Make informed, lawful, and fair decisions about whether to proceed with data processing;
5. Engage all relevant stakeholders in the data processing lifecycle and ensure they are adequately informed;
6. Ensure transparency in data processing activities;
7. Guarantee compliance with obligations outlined in the Law of Georgia on Personal Data Protection and relevant international regulations.

Legal Grounds for Conducting a DPIA

Conducting a Data Protection Impact Assessment is mandatory when:
Due to the introduction of new technologies, data categories, scale, or the purposes and methods of processing, there is a high likelihood of infringement on the fundamental rights and freedoms of individuals;
The data controller makes fully automated decisions, including profiling, which produce legal, financial, or otherwise significant consequences for the data subject;
The data controller processes large-scale special category data of numerous data subjects;
The data controller systematically and extensively monitors individuals' behavior in publicly accessible areas.

Timing of the DPIA

A DPIA must be carried out prior to the initiation of any data processing activity, or in the event of significant changes or updates to existing processing operations.

Retention Period of the DPIA Document

The University is required to retain the DPIA document throughout the duration of the data processing activity. If the processing is terminated, the document must be preserved for a minimum period of one (1) year following the cessation of data processing.

Publication of the Data Protection Impact Assessment (DPIA) Document

In the interest of building a reputation as a trusted institution, ensuring compliance with applicable laws, and upholding the principles of accountability and transparency, the Data Protection Impact Assessment (DPIA) document is subject to public disclosure, except in cases where such disclosure could endanger:

a) State security, information security, cybersecurity, and/or national defense interests;
b) Public safety;
c) Prevention of criminal activity;
d) Operational or investigative activities;
e) Criminal investigations;
f) Criminal prosecution;
g) Administration of justice;
h) Enforcement of custodial sentences;
i) Execution of non-custodial penalties and probation measures;

j) Significant national financial or economic interests, including monetary, budgetary, tax-related, public health, and social protection concerns;
k) The overriding legitimate interests of the data controller or data processor.

Data Controller	
Title	Georgian American University
Legal Form	LLC
Data Protection Officer	LLC „Safety Corp”
Contact Person	(+995 32) 220 65 20; tamarrobakidze@gau.edu.ge; info@gau.edu.ge

Part I – Data Processing Activities

Description of the Data Processing Process
Sources of Data Collection: The sources of personal data collection for the University are: a) Data provided based on the data subject’s explicit and actively expressed consent (including recruitment, contractual agreement, or student registration); b) Data obtained through video surveillance; c) Data received from the University's website, where the subject provides their name, surname, phone number, and email address; d) Data received from foreign student agents who carry out enrollment-related procedures at the request of prospective students; e) Data received from the Higher Education Management Information System; f) Data generated during the learning process (via personal files, the electronic academic management system “Goni,” distance learning modules, and other tools); g) Data received through Google application forms; h) Data received from foreign applicants’ registration forms (Google Form link);

i) Data sent via email from consulting agencies to the admissions group (admissions@gau.edu.ge), including scanned copies of student passports and academic documents;
j) Data received through registration via the website of GeoLab LLC by completing a registration form;
k) Data obtained from any lawful source for purposes defined by the University's "Personal Data Processing Policy" and/or the law.

Data Retention and Storage Periods:
1. The University retains only the data necessary to achieve a specific and lawful purpose of data processing.
2. Personal data is stored in file systems for a period necessary to fulfill the legitimate purpose, as defined by the grounds applicable to the data controller and data subject.
3. Special category data is stored using both automated and non-automated means for a period necessary to achieve the legitimate purpose, as defined by the grounds applicable to the data controller and data subject.
4. Data is stored in accordance with legally defined timeframes. Where it is necessary to determine the retention periods and procedures, the University considers the principles of personal data processing.
5. The following retention periods apply to data stored in physical (material) form at the University:
a) Student personal files – retained for 75 years;
b) Employee personal files – retained for 75 years;
c) Bachelor's, Master's, and Doctoral theses – retained for 75 years;
d) Employee working time records – retained for 3 years; working time sheets and logs – retained for 1 year;
e) Student exam papers – retained for 3 years;
f) Student applications – retained for 3 years;
g) Decisions of collegiate bodies (Academic and Administrative Councils) – retained permanently.
h) Minutes of meetings of collegiate bodies – Academic Council and Administrative Council – retained for **3 years**;
i) Orders related to core activities – retained **permanently**;
i.1) Orders regarding personnel – retained for **75 years**;
i.2) Orders on administrative and economic matters – retained for **5 years**;
j) Contracts – retained for **5 years**;
j.1) Employment contracts – retained for **75 years**;
j.2) Contracts/agreements on procurement/sales – retained for **6 years**;
j.3) Service contracts – retained for **6 years**;
k) Outgoing correspondence – retained for **5 years**;
l) Acceptance-transfer acts – retained for **6 years**;
m) Employee applications – retained for **75 years**;
n.1) Applications not included in the employee's personal file – retained for **5 years**;
o) Applications for participation in a vacancy competition – retained for **3 years**;
p) Orders on vacancy announcements – retained for **3 years**;
q) Financial reports – retained for **5 years**.
Note: After the expiration of the retention period, documents in physical (material) form are destroyed, and a corresponding destruction act is drawn up.

Access to Data:
1. Employee Access: Employees have access only to the data necessary for the fulfillment of their duties. In case of an employee's leave or inability to fulfill duties for any reason, the substitute employee may access data within the same scope as the person being substituted, in accordance with the scope and rules defined in the order assigning the duties.
2. Access to the University's Academic Management System is granted to:

a) Dean's Office staff;
b) Academic Process Management Service;
c) Legal Department (restricted access);
d) Finance Department (restricted access);
e) Human Resources Management Department (restricted access);
f) Administrative Office (restricted access);
g) Marketing and Communications Department (restricted access);
h) Strategic Development Department (restricted access).
3. Access to the University's Financial Accounting System is granted to the Finance Department, which may also access employment-related data necessary for payroll purposes with authorization from the Head of Human Resources.
4. Access to the Student Card System is granted to the relevant School Dean and administrative staff, IT Department, Marketing Department, and Examination Center staff.
5. Access to the admissions.gau.edu.ge email group is limited to Student Admissions Office managers.
6. Data of the University's Learning Center – GeoLab LLC is stored in the University's Google Drive, which is accessible to University employees.
7. Access to Google Meet for remote meetings is available to students, lecturers, and any other person using the University's corporate email.
8. Access to employee personal files (physical documents) and materials in those files is granted to the Human Resources Department for file maintenance and information management.
9. Access to minutes of collegiate body meetings is granted to the Registry Office (Chancellery) for recording and archiving purposes.
10. Access to the document flow system and its contents:
a) Full access is granted to the Registry Office and Legal Department for the purpose of distributing incoming correspondence and ensuring proper response;
b) Restricted access is granted to the Human Resources and Finance Departments for reviewing assigned correspondence and preparing responses.

Data Transmission / Disclosure

1. In the presence of a legal basis, data processed by the University may be transferred to the following third parties in accordance with procedures and scope defined by law:
a) Law enforcement agencies;
b) Courts;
c) The Personal Data Protection Service;
d) Other authorities as stipulated by legislation.
2. Data may also be disclosed to:
a) The Ministry of Education, Science, and Youth of Georgia;
b) The Ministry of Justice;
c) The Ministry of Defense;
d) Law enforcement bodies;
e) Governmental and/or local self-government authorities, in cases defined by law;
f) International organizations, when necessary for academic or administrative purposes in the best interests of students and staff;
g) Organizers of higher education activities;
h) The National Center for Educational Quality Enhancement (a LEPL under the Ministry of Education);
i) The Education Management Information System (EMIS);
j) The Revenue Service (LEPL);
k) Auditing companies;
l) The company "Fitpass" (in such cases, the University ensures the data subjects' consent for data transmission

and processing is obtained via electronic questionnaires);
m) The insurance company "Euroins" (consent is expressed by signing the agreement);
n) The digital HR management portal HR Digital Co.;
o) Banks, for the purpose of issuing salary cards;
p) The National Assessment and Examinations Center (LEPL);
q) Other higher education institutions for the purpose of student mobility.
2[1]. The University's Research Development and Support Office provides donor organizations with participant registration lists and photos from University-organized events and courses, within the framework of the project.
2[2].The University also processes data for **statistical purposes**:
The Strategic Development Office conducts various types of surveys throughout the year. A self-administered questionnaire is used for semester evaluations and is linked to the student portal.
For analytical purposes, data is grouped by citizenship, academic level, program, course, and group.
Annual surveys are conducted via Google Forms, which are distributed to students via email.
Following statistical analysis, the University prepares a report and sends it via email to relevant donors, schools, departments, and offices.
2[4]. The University's International Student Admission Office grants consulting companies access to marketing materials. The level of access is determined by management and is subject to monitoring by the system administrator.
3. The University involves third parties to assist in service provision, ensure smooth functioning of internal information technology systems, and manage them properly.
4. In all cases outlined in paragraphs 1–2[3], when information is disclosed, the University informs the data subjects. It also records what data was disclosed, to whom, when, and on what legal basis. This information is stored together with the subject's data for the duration of its retention period.
5. The University uses the platform **DHR.ge**, which provides access to an electronic database used for human resource management.
This includes the sharing of information necessary for HR purposes such as personal and contact details, remuneration, work hours, attendance records, and leave tracking.

Video Surveillance

1. The University uses a video surveillance system to fulfill its legal obligations — for the purpose of ensuring personal safety, protecting property, and safeguarding minors from harmful influence.
2. To inform data subjects about data processing, appropriate warning signs and the contact details of the person responsible for personal data processing are displayed in visible locations throughout the building.
3. The University ensures that employees whose workspaces fall within the range of the video surveillance system are properly informed.
4. The video surveillance system and its recordings are protected against unauthorized access and use. The head of the security service is the authorized person with access. Access is protected through a username and password. The University logs each access to the video recordings, including the time of access and the username, enabling identification of the person who accessed the data.
5. The video surveillance system is encrypted and equipped with a self-destruction mechanism. Camera monitors are located in a locked security room. A list of authorized individuals who have access to keys and surveillance data has been established, consisting of security staff. Additionally, during examination periods, exam rooms are monitored via video surveillance by a representative of the Examination Office.
6. The retention period for video surveillance data is **30 calendar days**, after which the data is automatically deleted by the system. Only video recordings that are part of disciplinary case documentation are exempt from deletion.
7. The video surveillance coverage area includes:
a) General areas of the University;
b) Hallways;
c) Building entrances;

d) Certain classrooms equipped with high-value equipment;
e) Examination rooms;
f) Stairwells;
g) The cafeteria;
h) The external perimeter of the University, including outdoor areas, gates, fences, entrances, and the parking lot;
i) Passageways between buildings;
j) The library.
8. Video surveillance is **not conducted** in changing rooms, hygiene areas, or in any space where individuals have a **reasonable expectation of privacy** or where video monitoring would **contradict universally accepted moral norms**.

Access Control to the Video Surveillance System

Within the University's proprietary video surveillance system, the following types of access are defined:
a) Live (real-time) monitoring of video cameras – Users with this level of access are only allowed to view live footage. They are restricted from rewinding or downloading recordings (to a computer or any other data storage device).
b) Rewinding and viewing of recorded footage – Users with this level of access can both monitor live footage and rewind and view previously recorded video. However, they are restricted from downloading recordings (to a computer or any other data storage device).
c) Downloading recorded footage – Users with this level of access are allowed to monitor live video, rewind and view recordings, and download footage to the local network. Downloads must be delivered to an authorized person upon appropriate approval.
d) Technical support access – Users with this level of access are authorized to: create new users in the video surveillance system, remove existing users, monitor electronically logged activities within the system (logs), take necessary actions to resolve technical issues and modify system configurations.
Note: A user is any individual who has access to the video surveillance system.
Access to the video surveillance system is granted exclusively through an individual username and password.

Direct Marketing

1. The person responsible for data processing conducts direct marketing by meeting with final-year school students in various regions. During these promotional meetings, information is collected for the purpose of future marketing campaigns. This information is then shared with the students via email and SMS.
1[1]. The university also conducts direct marketing in the form of SMS communication. Throughout the study period, students periodically receive various types of informational messages via SMS. Receiving such information is stipulated in the terms of the contract.
2. During the university's open days and model lectures, applicants and students provide their personal information, which the university subsequently uses to communicate with them and offer other related events.
3. The university carries out direct marketing activities in schools, training centers, on social media platforms, and during its own events.
4. GeoLab LLC, as the university's training center, conducts direct marketing by sending information via email about job vacancies, internship programs, and various free programs or activities.
5. The university ensures that it obtains the consent of the data subject(s) for the further processing of their data for direct marketing purposes, in accordance with Georgian legislation.
6. If it becomes necessary to process data beyond the data subject's name, surname, address, phone number, and email address for direct marketing purposes, the university will obtain written consent from the data subject.
7. Before obtaining consent and during the implementation of direct marketing, data subject(s) will be clearly informed, in a simple and understandable language, of their right to withdraw consent at any time, as well as the mechanism/rule for exercising this right.
8. When processing data for direct marketing purposes, the university records the time and fact of the data subject's

consent and consent withdrawal. This information is retained for the duration of the direct marketing campaign and for one (1) year after the termination of the campaign.
9. After giving consent and registering a phone number for direct marketing purposes, if the phone number is changed, the data subject has the right to contact the person authorized for processing using the provided contact details and notify them of the change to ensure accurate and correct data is maintained.

Data Subject Rights
1. The data subject is entitled to:
a)Receive information regarding the processing of their data;
b)Receive information about the data co-processor and/or authorized person;
c)Receive information on the purposes, legal bases, and categories of data processing;
d) Receive information about the identity or category of the recipient to whom the data has been or will be disclosed;
e) Receive information about the period for which the data will be stored, or, if it is not possible to specify the period, the criteria used to determine that period;
f) Receive any available information about the source of the data, if the data were not collected directly from the data subject;
g)Request access to and a copy of their processed data;
h) Request the immediate correction, updating, transfer, or completion of incorrect/inaccurate or incomplete data processed about them, considering the purpose of processing — including by providing additional information/documents;
i) Request the termination of processing, deletion, or destruction of their data by withdrawing consent;
j) Request the blocking of their data.

Update of the Impact Assessment Document and Additional Information
In the case of essential changes regarding specific issues or processes related to data processing, the person responsible for processing — with the active involvement of the Personal Data Protection Officer — is obliged to update the impact assessment document.

Participants and Opinions Involved in the Process
The university ensures the involvement of the following individuals in the impact assessment process:
a) The relevant structural unit or individual responsible for the creation or update of a specific product or service under which the data processing is carried out;
b) The Personal Data Protection Officer;
c) The structural unit or individual responsible for information technologies.

Additionally, the university ensures the involvement of the following persons in the impact assessment process:
a) An expert with specific knowledge of the processes;
b) Data subjects or their representatives;
c) Any other individual whose participation is important in the impact assessment process.

Additional Information Related to the Scale of Data Processing

Data Category

Depending on the nature of the relationship with the data subject and the purpose of data processing, the following personal data may be processed, as necessary:

a) Identification data – name, surname, personal identification number, date of birth, gender;
b) Contact information – legal and actual addresses, telephone number, email address;
c) Special category data – information about citizenship, the student's or employee's health status, criminal record, and convictions related to crimes against sexual freedom and inviolability;
d) Certified copies of diplomas;
e) Employment status;
f) Education;
g) Any other information required under the relevant service or by regulatory acts governing the University's authority;
h) Personal data of hotline users, which is processed only after informing the subscriber (beneficiary);
i) Work experience – position, title, job-related benefits, qualifications, salary;
j) Statement and/or document confirming the employee's intention to establish an employment relationship;
k) Copy of an identification document or passport;
l) Copy of an educational or professional qualification certificate;
m) Student's high school diploma (attestat);
n) Curriculum Vitae (CV);
o) One digital photograph;
p) Official bank account details;
q) Document confirming exit from the pension scheme under the cumulative pension reform, if applicable;
r) Document confirming eligibility for income tax exemption – certificate from the Revenue Service;
s) For individuals aged 17 or older (excluding those not subject to conscription), a document confirming registration or deregistration for military conscription;
t) Photos of minors and registration data for events and courses, shared with donors as required;
u) Link to social media profile;
v) Images of other individuals captured in the video surveillance coverage area;
w) Military registration certificate (for male employees/students);
x) Transcript of records from the previous educational institution;
y) Contact information for a student's parents or emergency contact persons;
z) Information about the student's academic performance;
aa) Information about the student's previous university/universities;
bb) Legal acts defining the student's status;
cc) Identification data of deceased individuals – for issuing a status termination order of a deceased student or employee, and for reflecting such changes in the Ministry of Education, Science, and Youth database.

Basis for Data Processing

1. Personal data is processed on the following legal grounds:
a) The data subject has given consent for their data to be processed for one or more specific purposes;
b) The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
c) The processing is necessary for the University to fulfill legal obligations imposed by legislation;
d) The processing is provided for by law;
e) According to law, the data is publicly accessible or has been made publicly accessible by the data subject;
f) The processing is necessary to protect the vital interests of the data subject or another person;
g) The processing is necessary to protect the significant legitimate interests of the data controller or a third party, except where such interests are overridden by the data subject's rights (including in the case of minors);
h) The processing is necessary to review the data subject's application (e.g., for the provision of services).
2. The University processes special category data only under specific circumstances:
a) Health-related data is processed for the purpose of ensuring the right to education for individuals with special educational needs, and also for managing sick leave documentation. The University also processes information on students' and staff members' citizenship in accordance with the requirements of the Ministry of Education, Science, and Youth of Georgia, since such information must be mandatorily recorded in the Ministry's database. Citizenship information is additionally processed for immigration and academic recognition purposes.
Foreign embassies frequently request statistical data on foreign students by nationality. The University may also be required to provide citizenship information to the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health, and Social Affairs of Georgia.
Moreover, the National Statistics Office (GeoStat) annually requests employment figures disaggregated by citizenship. The University's Research Development and Support Office is responsible for processing citizenship-related data upon donor request. Citizenship data also enables the University to provide applicants with comprehensive information on visa procedures required for entering Georgia. In certain cases, the University signs exclusive contracts with consulting agencies for specific countries. If an applicant independently contacts the University and is a citizen of such a country, the University provides the applicant with the consulting agency's contact details and asks them to establish communication.
b) Criminal record data — specifically, data regarding convictions for crimes against sexual freedom and inviolability — as well as health data may be processed when necessary due to the nature of the employment relationship or obligations, including for making employment-related decisions.
According to Article 32, Paragraph 2 of the Law of Georgia on Higher Education, a person convicted of crimes against sexual freedom and inviolability, as defined by the Law of Georgia on Combating Crimes Against Sexual Freedom and Inviolability, or a person deprived of the right to engage in educational activities by court order based on the same law, may not be employed in a higher educational institution.
3. When personal data is processed based on data subject consent, the consent will be deemed valid only if it is: Given freely, Following the receipt of adequate information, For a defined and specific purpose, Expressed voluntarily through the data subject's active conduct.

Assessment of the Necessity, Relevance, and Proportionality of Data Processing

Students use personal ID cards issued by the University to access the university premises and the examination center for testing purposes. These cards contain the student's name, surname, photograph, and personal identification number. The purpose of this card system is to identify students entering the examination center for written exams and to prevent risks during exam registration, such as a student taking an exam for a course from

another faculty, a non-enrolled individual taking an exam, and other similar cases.
The inclusion of the personal identification number on the card is necessary because students write their individual identification numbers on their exam papers in the examination center. These numbers are used to identify each paper and ensure individual assessment.

The technical and organizational measures implemented by the University to ensure data security serve as essential, minimally intrusive, and proportionate mechanisms for achieving the data processing objectives outlined in this document.

Despite the obligations defined by law, the University ensures the protection of every data subject's rights. In particular, when video footage is requested, the University anonymizes (depersonalizes) any individuals who are not relevant to the purpose of the request.

In its data processing activities, the University adheres to the principles of data minimization and storage limitation. In accordance with these principles and internal regulatory requirements, the University defines specific retention periods for each type of information. (For detailed information, please refer to the University's Personal Data Protection Policy document.)

Additional Information Related to the Scope of Data Processing

Are data of minors or other vulnerable groups being processed? How frequently is the data processed? What is the geographic scope of the data processing? Any other important information for determining the scale of data processing

The University processes the personal data of minors only in exceptional cases — specifically, when a student is admitted to the first year of study and has not yet reached the age of 18. In such cases, as with all students, the minor is required to submit all necessary documents along with their legal representative.
Additionally, the University processes information about students with special educational needs (including health-related data) in order to ensure their right to education.
The data processing activities of the University are not limited to the territory of Georgia. For example, embassies of various countries regularly request statistics about foreign students who are citizens of their respective countries. The University also shares information regarding foreign citizenship with the Ministry of Internally Displaced Persons from the Occupied Territories, Labour, Health, and Social Affairs of Georgia. Furthermore, the National Statistics Office (GeoStat) annually requests employment statistics categorized by citizenship. In addition, the Research Development and Support Office is responsible for processing citizenship-related information when requested by a donor.
Citizenship information is also used by the University to provide applicants with detailed guidance regarding visa procedures required to enter Georgia. In some cases, the University signs exclusive agreements with consulting agencies for certain countries. If an applicant independently contacts the University and is a citizen of a country with which such an exclusive agreement exists, the University provides the applicant with the contact information of the relevant consulting agency and advises them to get in touch.
Moreover, personal data may be obtained from foreign student agents who, with the consent of applicants, carry out the enrollment-related procedures on their behalf.

The University also transfers data to international organizations when necessary for academic or administrative purposes, and in the best interest of students and employees.

Purpose and Principles of Data Processing

Purposes of Data Processing

1. The purposes for which the University processes personal data include:

a) Carrying out higher education activities;
b) Performing official duties;
c) Ensuring the smooth operation of the teaching process, including remote learning;
d) Ensuring uninterrupted work processes;
e) Student registration;
f) Supporting the enrollment process at the higher education institution, including issuing conditional and unconditional offer letters and facilitating recognition of foreign education by the LEPL – National Center for Educational Quality Enhancement;
g) Managing personal files of students and all staff members;
h) Monitoring, assessing, and facilitating student mobility;
i) Realizing the right to education for students with special educational needs;
j) Recruiting qualified candidates seeking employment at the University;
k) Improving databases for the purpose of electronic assessment systems;
l) Organizing and controlling document flow;
m) Issuing official documents confirming higher education qualifications;
n) Ensuring the protection of University property and assets, as well as the physical safety of students, staff, guests, and third parties;
o) Improving the quality of services provided by the University;
p) Providing required information to supervisory or higher authorities;
q) Collecting data on students' academic performance;
r) Facilitating the participation of students and employees in various activities;
s) Submitting required information to the LEPL – Education Management Information System (EMIS) and uploading data to their system;
t) Ensuring the uninterrupted implementation of student admission, status restoration/suspension/termination processes;
u) Preparing contracts for research development and support, and forwarding them to the legal and financial offices as well as to donor organizations;
v) Supporting the duties of the Ombudsman;
w) Administering labor relations and recruitment;
x) Carrying out reporting procedures based on donor requests;
y) Managing and facilitating visa-related processes;
z) Fulfilling other responsibilities defined by law.

2. The purposes for which the University processes personal data via video surveillance include:
a) Fulfilling legal obligations;
b) Protecting security and property (including managing internal logistics or optimizing technical operations by providing the University leadership with data needed for daily operational improvement);
c) Protecting minors from harmful influence;
d) Preventing crime;
e) Detecting crime;
f) Ensuring professional supervision and quality assurance;
g) Continuously improving the quality of services offered to students present at the University;
h) Resolving legal disputes (video recordings serve to protect all parties involved — students, including minors, and University staff — and act as factual evidence for fair and accurate resolution of disputes or allegations);
i) Examination/testing purposes.

Principles of Personal Data Processing

Personal data is processed in accordance with the following principles defined by Georgian and international legislation:

- Principle of Fairness
- Principle of Transparency
- Purpose Limitation
- Data Minimization
- Storage Limitation
- Accuracy of Data
- Security Principle

Part II – Potential Threats to Fundamental Rights and Freedoms and Their Qualitative Analysis

Risk Level	Risk Category	Description and Required Measures
I	Non-Essential	A minor incident, considered a localized case with low impact, which does not affect the functioning of the University. No specific procedures are required; monitoring of task execution is necessary.
II	Essential	A serious incident that disrupts one or more University processes. It is necessary to develop risk mitigation procedures, assess priorities, and plan control measures to reduce the risk.
III	Critical	A critical incident that completely disrupts or halts the operations of the University. It is necessary to suspend work/educational processes, and immediate measures must be taken to reduce the risk

Type of Data Processing:	
❖ The data controller makes a fully automated decision, including based on profiling, that has legal, financial, or other significant effects on the data subject.	+
❖ The data controller processes a large volume of special category data of data subjects (no less than 3% of the population of Georgia, as calculated based on the latest census results).	+
❖ The data controller conducts systematic and large-scale monitoring of data subjects' behavior in public spaces.	+
❖ Systematic and large-scale monitoring of data subjects' behavior or condition (including physical/health-related) through a specific electronic system/technology, or such monitoring being conducted in relation to employees;	+
❖ Introduction of new technology or its innovative use.	+
❖ Comparison or merging of databases originating from two or more separate data processing activities, intended for different purposes and/or managed by different data controllers;	
❖ The data processing may result in discrimination against the data subject;	+
❖ The data subjects are vulnerable individuals, including employees of the data controller, patients of medical institutions, minors, persons with disabilities, and others.	+
❖ The University processes special category data, which, in the context of educational and administrative activities, may create a risk of data disclosure. Such risks may arise due to negligent actions by University employees, violations of organizational rules for storing physical documents, and/or incorrect legal assessment of the grounds for transferring information to third parties.	+
❖ Destruction of archival material and various documentation.	+

❖ Internet, software, or hardware malfunctions.	+
❖ Cybercrime	+

Possible Outcomes of Data Processing		Risk Level
❖ Identity theft or forgery (so-called identity fraud)	The University actively processes personal data such as identity documents, their numbers, financial information, and other related details, which makes them a target for hackers and phishing schemes.	II
❖ Financial loss	Cases of direct financial harm to individuals are relatively rare, but still possible due to cyberattacks, which may target, among other things, bank accounts.	II
❖ Damage to the data subject's reputation, with a harmful impact on academic or professional opportunities	The misuse of personal or academic data may harm the reputation of students or staff; however, this often requires deliberate or targeted actions.	II
❖ Breach of confidentiality of personal data protected by professional secrecy	Special category information, including health-related data, may become easily accessible in cases of unauthorized access.	II
❖ Unlawful disclosure of pseudonymized personal data	Although pseudonymization is an additional mechanism for data protection, the security of such data may still be at risk of re-identification — especially through extensive data analytics or careless data processing.	II
❖ Other types of significant social and/or economic harm	Harm such as stigmatization or discrimination may result from the disclosure of data; however, such outcomes typically require the presence of intentional and deliberate misuse of rights.	II
❖ Deterioration of health condition	It is unlikely, unless the breach involves special category medical or psychological data.	I
❖ Restricted access to critical (life-sustaining) infrastructure	The University rarely faces infrastructure malfunction issues; however, system disruptions may temporarily interfere with the learning process.	I
❖ Legal actions and disputes initiated by affected individuals or regulatory authorities	It is likely to occur in cases involving serious breaches and special category data; however, the probability of a dispute initiated by the regulator is low due to the University's proper compliance with legally established requirements.	I

❖ System functionality disruptions due to data recovery attempts	Depends on the proper existence of backup and incident response protocols.	II
❖ Unauthorized access, which may occur through cyberattacks (hacking), phishing, or weak password protection systems	Due to the volume of personal data (including special category and financial information) processed by the University.	II
❖ Data loss, which may occur due to hardware malfunction, employee negligence, or intentional actions	Likely in cases of insufficient backups or intentional cyberattacks.	II
❖ Unlawful disclosure of data, involving the exposure of sensitive information to unauthorized parties — potentially caused by data leaks, system vulnerabilities, or theft of devices	he University actively processes sensitive data, which makes it a target for unauthorized access.	II
❖ Data modification, meaning unauthorized or accidental alteration of data — which may involve tampering with student grades, research results, or financial records	Because insider access or a specific system vulnerability is required.	I
❖ Disproportionately long data retention and improper destruction, which may occur by storing data beyond the legally established retention period or by keeping unshredded physical files	Because it occurs when there is no comprehensive data processing policy in place.	II
❖ Failure to comply with legal requirements due to deficiencies in internal documentation, including the absence of informed consent forms and necessary notices	Because this risk is driven by a lack of awareness and insufficient staff training regarding existing regulations.	II
❖ The destruction of archival materials and various documentation may result in delays in tax/audit inspection processes, disruptions in administrative workflows, and the absence of contracts and memorandums with students, academic and administrative staff, suppliers, and partners until they are renewed.	Since electronic copies, archival materials, and other documentation are stored in specially designated secure spaces, a record is kept of destroyed documents, and priorities are set for their phased restoration. Additionally, documentation is restored using electronic copies by the relevant department, and the process of re-signing contracts and memorandums is ensured.	I

❖ Internet, software, or hardware issues may lead to minor disruptions in specific or overall academic/work processes. In the case of prolonged outages, these disruptions may result in a temporary suspension of teaching or work activities. However, the University's core operations can generally continue uninterrupted unless there is damage to a large volume of equipment.	There is an alternative line available, as well as official partnerships with Microsoft, Google, and others, which reduces software-related risks. Firewall protection, antivirus applications, LAN restrictions, and regular data backups are in place. Equipment is checked periodically, and outdated hardware is replaced with new devices. In addition, a backup stock of computer equipment is maintained. In the event of a serious issue, IT support is provided to resolve the malfunction, and, if necessary, contact is made with official vendors. These processes are managed and overseen by the University's Information Technology Department.	I
❖ Cybercrime carries the risk of data loss, which may lead to potential disruptions in academic or work processes.	Since important information is stored on secure external servers, backup copies of the data are created and stored periodically (once a week). In the event of a serious issue, IT support is provided to resolve the malfunction, and, if necessary, contact is made with official vendors. These processes involve the Information Technology Department and the Legal Department	II

Threat Assessment and Response

Description of Security Measures and Organizational-Technical Measures Defined to Protect the Rights and Freedoms of the Data Subject

1. The University ensures data security through appropriate measures, protecting it from accidental or unlawful destruction, alteration, disclosure, acquisition, any other form of unlawful use, or accidental or unlawful loss.
2. Access to data is granted only to those employees and only to the extent necessary for the performance of their duties.
3. The personal data of University staff and students is stored both in physical and electronic formats, including on computers, drives, the electronic learning management system, and memory cards.
4. The University uses Microsoft and Google cloud systems for storing and transferring electronic information.
5. Data from the electronic learning management system is stored on Microsoft Azure cloud. Data is also stored in Google Sheets. On Google Drive, the University stores ID copies, signed contracts, and documents, which are also stored physically in binders in a designated secure room within the University.
6. Data processed by GeoLab LLC is stored on the organization's Google Drive, accessible only to managers directly involved in the processes.
7. Each corporate email at the University has its own drive, and each user can upload materials. In the case of shared drives, staff themselves decide with whom to share files, and all sharing activities are logged. The shared materials are accessible only to University staff using their corporate email accounts.
8. Data is stored on University-owned computers. The learning portal can be accessed on non-server devices via University or corporate email to ensure uninterrupted educational and work processes.
9. The University stores special category data separately using both electronic and physical filing systems. Access to these files is granted only to the University Ombudsman.
10. In the case of foreign student admissions, data access is limited to staff working in relevant positions. Monitoring is provided by the system administrator.
11. The University uses an electronic learning management system that includes username and password authentication mechanisms for security. Authorization levels and user roles are defined programmatically. The system is integrated with the Google platform, so students access the portal using a personal email address created by the University. Academic and administrative staff are added by the system administrator, and access is granted either with individual credentials or University-created email. Usernames and passwords must not be shared with third parties.
12. Actions performed on electronic data are logged in the relevant system. For physical data, employees are required to log any actions related to disclosure or modification, including incident records.
13. Electronic data is placed in shared files, with access granted only to University employees as required for work duties, and only via corporate email.
14. The University uses its website – www.gau.edu.ge – for informational purposes only. No external users can upload data. The site hosts University event photos, documents (charter, policies), and academic/administrative staff contact info. For the publication of identifying or biometric data, the University ensures explicit consent is obtained via signed consent forms.
15. The University receives data from GeoLab's website (https://geolab.edu.ge). GeoLab provides administrative and financial departments with student data, including documentation for discount eligibility. Individuals register for courses on the site and provide: course preference, full name, email, ID number, phone number, city, address, birthplace, date of birth, workplace/education, social media links, and IP address.
16. The University uses a COOKIES system with the following:
 a) october_session – assigns a unique session ID to the user;
 b) _ga – installed by Google Analytics to count visitors, sessions, and usage anonymously;

c) _gid – tracks how users use the website;
d) _gat_gtag_UA_* – stores user ID for Google Analytics;
e) _ga_* – tracks and counts page views;
f) YSC – tracks views of embedded YouTube videos;
g) VISITOR_INFO1_LIVE – measures bandwidth for YouTube;
h) VISITOR_PRIVACY_METADATA – saves cookie consent status for YouTube;
i) guest_id – used by Twitter to identify and track visitors, storing ad preference data.

17. Google Analytics on the website provides general information on user origin, access method (direct or from social media), and device type.

18. Physical documentation (e.g., employment files) is stored in binders in locked cabinets in the HR office. All employee documents are scanned. Student documents are also scanned and stored in faculty offices. Access is only allowed via formal request and logging.

19. Student and staff personal files are archived both physically and electronically. Student files are archived by the Student Services Office. The Chancellor's Office archives incoming/outgoing documents, while HR archives inactive personnel files. A designated secure storage room is available for archived files. Access is logged and restricted to authorized departments. IT also backs up data on hard drives.

20. Health-related special category data is stored both in personal files and electronic systems and is accessible only by authorized individuals. Access and logging systems are in place for security.

Specific measures implemented or planned by the data controller to eliminate potential threats to the fundamental rights and freedoms of individuals and/or to reduce the high likelihood of their occurrence.

The university is obliged to inform the data subject in detail about what data it collects, how it uses the data, to whom it transfers it, and how it ensures data security.

Any employee of the university who participates in data processing or has access to the data is required to:
a) Not exceed the scope of their authorized access;
b) Maintain the confidentiality and secrecy of the data, including after termination of employment;
c) Not use the data for personal or non-work-related purposes;
d) Not make the data accessible to unauthorized persons, including by leaving data unattended or discussing it in the presence of unauthorized individuals.

Violation of the rules established by this document constitutes a breach of the university's internal regulations, employment contracts, and the regulations developed by the university's Research Integrity Committee regarding medical research and project implementation, and entails corresponding disciplinary action. The obligation to protect confidential information continues even after the employee leaves the university.

Data security is ensured in accordance with the university's Information Security Policy. Appropriate organizational and technical measures are implemented on the university's website to ensure data security (including penetration testing and access restrictions limited to users whose duties directly involve data processing).

Within the university, data processing involves secure deletion protocols for digital files (using certified deletion tools), while physical documents are shredded or incinerated.

Furthermore, all data transmission activities are logged and audited. In cases of data transfer, the university ensures that informed consent is obtained from data subjects.

Additionally, personal data protection is carried out through staff training sessions, and the implementation of relevant documentation such as the Personal Data Protection Policy, Incident Response Plan, Video Surveillance Policy, and others. The university also conducts regular audits of data processing activities via the Data Protection Officer and reviews existing documentation, making changes when necessary to ensure legal compliance.

Part III – Information on the Methodology Used in the Impact Assessment Process

Methodology Used in the Impact Assessment
Legislation provides for various methods and tools to be used at different stages of the impact assessment proces: a) SWOT Analysis – A strategic planning method used to assess the position of the data controller, evaluate their capabilities, and examine the operational environment. This includes analyzing stakeholder expectations, as well as the strengths and weaknesses, opportunities, and threats of the data processing process. It helps identify the requirements faced by the data controller and the competencies of the participants involved in data processing. b) Individual and Group Discussions – Planned as needed to share or communicate any relevant information. c) Workshops/Seminars – Aimed at informing participants involved in the data processing process about potential risks.
Use of the Consultation Mechanism with the Data Protection Officer: If a threat is identified as a result of the impact assessment, the university takes all necessary measures to substantially reduce the risk and consults the Data Protection Officer to obtain prior guidance.