Georgian American University

Policy for the Processing of Personal Data №1

Contents

1. General Information About the Document

This Personal Data Processing Policy (hereinafter referred to as "the Policy") aims to ensure the transparency of personal data processing activities conducted by Georgian American University LLC (hereinafter referred to as "the University"). The Policy enables any individual, including data subjects and/or potential data subjects, to receive clear and accessible information about how the University processes personal data.

Personal Data (hereinafter referred to as "Data") refers to any information related to an identified or identifiable natural person. A natural person is identifiable if their identity can be determined directly or indirectly, including through their name, surname, identification number, geolocation data, electronic communication identifiers, or physical, physiological, psychological, genetic, economic, cultural, or social characteristics.

Personal data is processed in compliance with Georgian legislation, specifically the Georgian Law on Personal Data Protection, and other regulatory acts.

The rights of data subjects are protected under both Georgian law and the European General Data Protection Regulation (GDPR).

Personal data processing is conducted in accordance with the principles outlined in Georgian and international legislation, particularly GDPR, including:

- **Fairness Principle**
- **Transparency**
- **Purpose Limitation Principle**
- **Data Minimization Principle**
- **Retention Minimization Principle**
- **Accuracy Principle**
- **Security Principle**

The Policy ensures compliance with Article 4, Paragraph 1(a) of the Georgian Law on Personal Data Protection, which stipulates that data must be processed lawfully, fairly, transparently, and in a manner that respects the dignity of the data subject.

The terms used in this Policy have the meanings assigned to them under the Georgian Law on Personal Data Protection.

The Policy is available on the University's website (www.gau.edu.ge), ensuring access for all data subjects.

2. General Information About LLC "Safety Corp."

LLC "Safety Corp." is a consulting company that ensures the compliance of partner companies with legal requirements in various areas. One of its areas of activity includes providing services related to personal data, such as the appointment of a data protection officer, the implementation of comprehensive documentation, and aligning the operations of client companies with legal standards.

3. General Information About the Data Controller

Georgian American University LLC is a higher education institution that processes the personal data of students, academic staff, invited lecturers, contractors, and other employees, including minors, to fulfill its functions. To effectively carry out its duties and responsibilities, the University requires the processing of personal data belonging to data subjects. This process begins with the registration of applicants at the University and continues throughout the entire educational process and the validity period of relevant agreements in the case of employees or other individuals.

The processed data includes personal information about students, lecturers, and other employees, as well as information about the academic performance and activities of students during their studies at the University.

To ensure the provision of higher education, the University operates within a unified system that includes the Ministry of Education, Science, Culture, and Sport of Georgia and public legal entities under its jurisdiction. These entities define the forms and purposes of data processing within their authority. Accordingly, data is processed both through electronic platforms and paper-based systems.

The protection of personal data is a right for all members of the University community. Consequently, data processing is a clearly regulated process, and the University ensures the protection of personal data for all members. To this end, it has developed a personal data processing policy and designated a Data Protection Officer.

4. General Information About the Authorized Data Processor

LLC "Self.GE" is an outsourcing company specializing in human resource management. It provides the University with access to a digital tool, GAU.SELF.GE, which the University uses to manage human resource processes digitally.

LLC "Self.GE" itself does not act as a data controller, as the data it processes serves the purposes of its client organizations, and the specific means of data processing are determined according to the client organization’s instructions.

Therefore, within the context of data processing, LLC "Self.GE" acts as an authorized data processor that processes data on behalf of or for the benefit of the data controller. A corresponding agreement (written contract) is concluded between LLC "Self.GE" as the authorized data processor and the data controller. This agreement defines the bases and purposes of data processing, the categories of data to be processed, the duration of data processing, and the rights and obligations of both the data controller and the authorized data processor. The agreement also covers the matters outlined in Article 36, Paragraphs 2-3 of the Georgian Law on Personal Data Protection.

As an authorized data processor, LLC "Self.GE" is only responsible for ensuring the security of the data it processes and only for the duration of the data processing period.

5. General Information About Co-Processors

LLC "Fitpass Georgia," LLC "Euroins Insurance Company," and JSC "Bank of Georgia" provide the University with relevant services. Specifically:

- LLC "Fitpass" offers corporate services, allowing University employees to engage in over 40 sports activities at more than 150 locations daily with a single monthly subscription fee. The University ensures that data subjects provide consent for the transfer and processing of personal data through an electronic questionnaire.
- LLC "Euroins Insurance Company" provides appropriate insurance services to University employees.
- JSC "Bank of Georgia" collaborates with the University to issue payroll cards.

These organizations act as co-processors of data because the data processing activities they carry out serve their own organizational purposes, and the specific means of data processing are determined by their instructions.

Consequently, in the context of data processing, the aforementioned companies function as co-processors, processing data for their own organizations and under their own authority. A corresponding agreement (written contract) is concluded between the co-processors and the data controller. This agreement defines the bases and purposes of data processing, the categories of data to be processed, the duration of data processing, and the rights and obligations of both the co-processors and the data controller. The agreement also covers matters outlined in Article 36, Paragraphs 2-3 of the Georgian Law on Personal Data Protection.

As co-processors, LLC "Fitpass Georgia," LLC "Euroins Insurance Company," and JSC "Bank of Georgia" are only responsible for the security of the data they process and only for the duration of the data processing period.

6. Data Processing Policy of Georgian American University

6.1. Preamble

The Data Processing Policy of Georgian American International University (hereinafter referred to as "the University") is developed based on the Georgian Law on Personal Data Protection and other regulatory acts. This Data Processing Policy (hereinafter referred to as "the Policy") applies to the processing of data by the University in relation to its administration, academic staff, invited lecturers, and students. It extends to the processing of data in any form carried out by the University.

6.2. Data Controller

- **Organization**: Georgian American University LLC
- **Identification Code**: 206169304
- **Address**: 10 Merab Aleksidze Street, Tbilisi, Georgia
- **Phone Number**: (+995 32) 220 65 20
- **Email**: tamarrobakidze@gau.edu.ge; info@gau.edu.ge

6.3. Authorized Data Processor

- **Organization**: LLC "Self.GE"
- **Identification Code**: 405373714
- **Address**: A. Politkovskaya st., N 3, building 27, bldg. 43, Vake district, Tbilis, Georgia
- **Phone Number**: +995 322 84 54 44
- **Email**: info@self.ge

6.4. Co-Processors

1. LLC "Fitpass Georgia"

- **Identification Code**: 406271895
- **Address**: 6 Gare Kakheti Street, Building 24, Isani-Samgori District, Tbilisi, Georgia
- **Phone Number**: +995 32 212 1240

- **Email**: info@fitpass.ge

2. LLC "Euroins Insurance Company"

- **Identification Code**: 406271895
- **Address**: 6 Gare Kakheti Street, Building 24, Isani-Samgori District, Tbilisi, Georgia
- **Phone Number**: +995 (32) 220 33 33
- **Email**: info@euroins.ge

3. JSC "Bank of Georgia"

- **Identification Code**: 204378869
- **Address**: 29a Gagarin Street, Vake-Saburtalo District, Tbilisi, Georgia
- **Phone Number**: +995 32 244 4444
- **Email**: customerservice@bog.ge

6.5. Data Protection Officer

- **Organization**: LLC "Safety Corp."
- **Identification Code**: 427743212
- **Address**: 37m Chavchavadze Avenue, Axis Towers, 5th Floor (Terminal), Tbilisi, Georgia
- **Phone Number**: (+995) 593 453 030
- **Email**: tamuna.tkeshelashvili@geosafety.ge

6.6. "Personal Data Processing Policy"

Article 1: General Provisions

1. This Policy regulates issues related to the processing of personal data by the University.
2. This document applies to all individuals employed by or acting on behalf of the University, including interns, and is mandatory for compliance.
3. This Policy must be used in conjunction with and in alignment with the Georgian Law on Personal Data Protection.

Article 2: Definitions of Terms

1. The terms used in this policy have the meanings defined in the Georgian Law on Personal Data Protection, for the purposes of this policy:

a) Personal Data (hereinafter "Data") – Any information that relates to an identified or identifiable natural person. A natural person is identifiable if their identity can be determined directly or indirectly, including through their name, surname, identification number, geolocation data, electronic communication identifiers, physical, physiological, psychological, genetic, economic, cultural, or social characteristics.

b) Special Categories of Data – Data that relates to a natural person's racial or ethnic origin, political views, religious, philosophical, or other beliefs, trade union membership, health, sexual life, status as a defendant, convict, acquitted person, or victim in a criminal process, convictions, criminal records, diversions, recognition as a victim of trafficking or crimes under the Georgian Law on Violence Against Women and Domestic Violence, imprisonment, and enforcement of penalties, as well as biometric and genetic data processed for unique identification purposes.

c) Health-Related Data – Information regarding a data subject's physical or mental health, including data on medical services provided to the data subject.

d) Biometric Data – Data processed using technical means that relate to the physical, physiological, or behavioral characteristics of a data subject (e.g., facial image, voice characteristics, or fingerprint data) for unique identification or identity verification purposes.

e) Data Processing – Any operation performed on data, including collection, retrieval, access, photographing, video monitoring, or audio monitoring, as well as organizing, grouping, interconnecting, storing, altering, recovering, querying, using, blocking, erasing, destroying, disclosing, transmitting, publishing, distributing, or otherwise making data available.

f) Automated Data Processing – Data processing carried out using information technology.

g) Non-Automated Data Processing – Data processing carried out without the use of information technology.

h) Semi-Automated Data Processing – Data processing carried out using a combination of automated and non-automated means.

i) Filing System – A structured set of data arranged and accessible according to specific criteria.

j) Data Subject – Any natural person whose data is being processed.

k) Consent of the Data Subject – A clear and freely expressed will of the data subject, made actively, in writing (including electronically), or orally, after receiving relevant information, to allow the processing of their data for a specific purpose.

l) Written Consent of the Data Subject – Consent provided by the data subject in written form (including electronically), explicitly allowing the processing of their data for a specific purpose, after receiving relevant information.

m) Data Controller – A natural person, legal entity, or public institution that determines, either individually or jointly with others, the purposes and means of data processing, directly or through an authorized processor.

n) Joint Data Controllers – Two or more data controllers who jointly determine the purposes and means of data processing.

o) Authorized Processor – A natural person, legal entity, or public institution that processes data for or on behalf of the data controller. A person employed by the data controller is not considered an authorized processor.

p) Data Recipient – A natural person, legal entity, or public institution to whom data is transferred, excluding the Personal Data Protection Service.

q) Incident – A breach of data security that results in the unlawful or accidental damage, loss, unauthorized disclosure, destruction, alteration, access, collection, or other unauthorized processing of data.

2. Other terms used in this policy, unless specifically defined otherwise, are interpreted according to the Georgian Law on Personal Data Protection.

Article 3: Purposes of Data Processing

The purposes for which the University processes personal data include:

a) Conducting higher education activities;
b) Carrying out official duties;
c) Ensuring the smooth operation of the educational process, including remote learning;
d) Ensuring the uninterrupted workflow;
e) Student registration;
f) Facilitating enrollment processes in higher education institutions, including preparing conditional and unconditional invitation letters and undergoing recognition procedures for foreign education with the National Center for Educational Quality Enhancement (NCEQE);
g) Managing personal files of students and staff;
h) Ensuring student records, evaluations, and mobility processes;
i) Realizing the right to education for students with special educational needs;
j) Recruiting qualified candidates for employment at the University;
k) Enhancing databases for electronic evaluation systems;
l) Organizing and controlling document circulation;
m) Issuing documents confirming higher education;

n) Protecting University property, assets, and ensuring the physical security of students, staff, guests, or third parties;
o) Improving the quality of services provided by the University;
p) Providing information requested by higher authorities;
q) Collecting data on student academic performance;
r) Facilitating student and staff participation in various activities;
s) Providing requested information to the Educational Management Information System (EMIS) and uploading data to their platform;
t) Managing enrollment, status restoration, suspension, or termination processes for students in higher education institutions;
u) Preparing contracts and coordinating with financial and legal departments as well as donor organizations for research development and support purposes;
v) Enabling the Ombudsman's office to fulfill its duties;
w) Administering labor relations for recruitment purposes;
x) Conducting reporting processes as required by donors;
y) Facilitating and conducting visa-related processes;
z) Carrying out other responsibilities mandated by law.

Article 4: Legal Bases for Data Processing

1. Personal data processing is conducted on the following legal bases:

a) The data subject has provided consent for one or more specific purposes;
b) Data processing is necessary to fulfill contractual obligations with the data subject or to prepare for a contract at the data subject's request;
c) Data processing is necessary to comply with legal obligations imposed on the University;
d) Data processing is prescribed by law;
e) Data is publicly available by law or has been made publicly available by the data subject;
f) Data processing is necessary to protect the vital interests of the data subject or another person;
g) Data processing is necessary to safeguard the legitimate interests of the data controller or a third party unless these interests are overridden by the rights of the data subject, particularly in the case of minors;
h) Data processing is necessary to consider a request submitted by the data subject (e.g., for service provision).

2. The University processes special categories of data only under specific circumstances, such as:

a) Health-related data is processed to ensure the right to education for persons with special educational needs, implement attendance systems, and comply with requirements of the Ministry of Education, Science, and Youth. Citizenship information is processed for educational recognition, immigration purposes, and statistical reporting to embassies or government entities.

b) Criminal record data related to offenses against sexual freedom and inviolability is processed when necessary for labor relations, particularly in decisions related to employment, in compliance with Article 32, Paragraph 2 of the Georgian Law on Higher Education, which prohibits employing individuals with convictions for such offenses.

3. If the University processes data based on the subject's consent, the consent is considered valid only if it is given freely, after receiving relevant information, and for a specific purpose. Consent must be expressed voluntarily through an active action by the data subject.

Article 5: Data Subjects

The University processes the personal data of the following individuals:

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

Article 6: Rights of Data Subjects

1. A data subject is entitled to:

a) Receive information about the processing of their data;
b) Obtain information about the co-processor and/or the authorized processor of the data;
c) Learn about the purposes, bases, and categories of data processing;
d) Be informed of the identity or category of recipients to whom the data has been or will be disclosed;
e) Know the duration of data retention or, if determining a specific duration is not possible, the criteria for defining it;
f) Access any available information about the source of data collection if the data was not collected directly from the subject;
g) Review and obtain a copy of the data being processed;
h) Request the immediate correction, update, transfer, or completion of inaccurate/incomplete data processed about them, including by submitting additional details/documents;
i) Demand the cessation of data processing, deletion, or destruction of their data by withdrawing consent;
j) Request the blocking of data.

2. To exercise these rights, the data subject must contact the authorized processor or the data controller if the data is held by them.

3. Upon a data subject's request, the University is obligated to provide the relevant information within no later than **10 working days** from the receipt of the request. In exceptional cases, and with appropriate justification, this period may be extended by no more than an additional 10 working days, and the data subject must be promptly informed.

4. The data subject has the right to withdraw their consent at any time without explanation or justification. Withdrawal of consent can be carried out in the same form as it was granted.

5. Upon the data subject's request, data processing must cease, and the processed data (except for cases specified under Article 12, Paragraph 9 of the Georgian Law on Personal Data Protection) must be deleted no later than **7 working days** from the request, provided no other legal basis for processing exists.

6. The rights of the data subject may be restricted in cases and under the rules provided by the Georgian Law on Personal Data Protection.

7. If the actions required to fulfill the data subject's rights involve other entities participating in the data processing (e.g., the Ministry of Education, Science, and Youth; National Center for Educational Quality Enhancement; Education Management Information System; Revenue Service; financial or audit services; Ministry of Justice; Ministry of Defense; law enforcement; government/local authorities; banks for payroll card issuance; embassies), the University is authorized to provide the data subject with written explanations about such matters.

8. The data subject enjoys all other rights provided by the Georgian Law on Personal Data Protection.

9. For any issues related to personal data processing, the data subject has the right to contact the company director and/or the Data Protection Officer.

10. In the event of a dispute regarding personal data protection, the data subject may apply to the Personal Data Protection Service and/or the court as per the procedures established by law.

Article 7: Data Categories

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

a) Identification data – name, surname, personal identification number, date of birth, gender.
b) Contact data – legal and actual addresses, phone number, email address.
c) Special categories – citizenship information, student/employee health data, and criminal records related to offenses against sexual freedom and inviolability.
d) Certified copies of diplomas.

e) Employment status.
f) Education.
g) Any other information required by relevant services or regulations governing University activities.
h) Personal data of hotline users, processed only with the explicit consent of the beneficiary.
i) Work experience – position, title, remuneration, qualifications, salary.
j) Statements/documents confirming the intent to establish a labor relationship.
k) Copies of identification documents/passports.
l) Copies of education or qualification certificates.
m) School transcripts for students.
n) Curriculum Vitae (CV).
o) One digital photograph.
p) Official details of active bank accounts.
q) Documents related to exiting pension schemes under the cumulative pension reform, if applicable.
r) Documents confirming eligibility for income tax benefits, such as certificates from the Revenue Service.
s) Military conscription documents for individuals aged 17 or older (except those not subject to military registration).
t) Photographs of minors and data related to registration for events and courses for submission to donors.
u) Social media links.
v) Images of individuals captured in video surveillance.
w) Military service records (for male employees/students).
x) Academic transcripts from previous institutions.
y) Contact information for students' parents or emergency contacts.
z) Academic performance data for students.
aa) Information about the student's previous university(ies).
ab) Legal acts defining student status.
ac) Identification data of deceased individuals for purposes such as issuing termination orders for student status or labor relationships and reporting to the Ministry of Education.

2. Students use University-issued cards, containing their name, surname, photograph, and personal identification number, to access the University and examination centers. The card system aims to identify students entering the examination centers and prevent risks, such as unauthorized individuals taking exams or students attempting exams for unrelated subjects. Including the personal identification number on the card is necessary for students to link their work with unique identifiers, facilitating individual evaluations.

Article 8: Sources of Data Collection

The sources of personal data collection for the University include:

a) Data provided with the explicit and actively expressed consent of the data subject (including recruitment, contractual agreements, and student registration).
b) Data obtained through video surveillance.
c) Information submitted via the University's website, including fields for name, surname, phone number, and email address.
d) Data from agents handling admission procedures for foreign students, based on the applicants' expressed will.
e) Data received from the Higher Education Management Information System (EMIS).
f) Data generated during the educational process, including personal files, the academic management electronic system ("Goni"), remote learning modules, and other resources.
g) Data collected through Google application forms.
h) Data obtained from registration forms for foreign applicants (e.g., Google form link).
i) Emails from consulting agencies sent to the admissions.gau.edu.ge email group, containing scanned versions of student passports and educational documents.
j) Data collected through registration forms on LLC Geolab's website.
k) Any legally obtained information necessary for the purposes defined by this policy or by law.

Article 9: Data Security and Employee Responsibilities

1. Data Security Measures

The University ensures data security by taking appropriate measures to protect data from accidental or unlawful destruction, alteration, disclosure, unauthorized access, or any other form of unlawful use or accidental or unlawful loss.

2. Transparency to Data Subjects

The University is obligated to inform data subjects in detail about the data collected, how it is used, who it is shared with, and how its security is maintained.

3. Responsibilities of Employees Involved in Data Processing

Employees involved in data processing or with access to data are required to:

a) Act within the limits of their granted authority.
b) Maintain the confidentiality of the data, including after the termination of their employment.
c) Avoid using the data for personal or non-work-related purposes.
d) Prevent unauthorized access to the data, including through negligence (e.g., leaving data unattended or discussing it in the presence of unauthorized persons).

Violating these provisions constitutes a breach of the University's internal regulations, employment contracts, and the standards established by the University's Research Integrity Committee. Disciplinary actions will apply accordingly. The obligation to maintain confidentiality continues even after the termination of employment.

4. Access to Data

Only employees who need the data to perform their duties have access to it, and only to the extent necessary for their functions.

5. Data Storage

Personal data of employees and students is stored in both physical and electronic formats, including computers, drives, electronic learning management systems, and memory cards.

6. Cloud Storage

The University uses Microsoft and Google cloud systems for storing and transmitting data electronically.

7. Electronic Learning Management Systems

Data in the electronic learning management system is stored on Microsoft Azure cloud systems. Additionally, data is stored on Google Sheets and Google Drive, which includes identification documents and contracts. Physical copies of these documents are also stored in designated rooms in binders.

8. Data Managed by LLC Geolab

Data processed by LLC Geolab is stored on the organization's Google Drive, accessible only to managers directly involved in the processes.

9. Corporate Email Drives

Each corporate email account has its drive, and users can upload materials. Shared files are managed by employees who decide access permissions, which are logged. Shared file access is limited to employees with corporate emails.

10. Local Data Storage

Data is stored on University-owned computers. The educational portal is accessible through University or corporate email on non-server devices to ensure uninterrupted academic and administrative processes.

11. Sensitive Data Handling

Sensitive data is stored separately using electronic and physical filing systems. Access to these files is restricted to the University Ombudsman.

12. Data Access for Foreign Student Admissions

Only employees involved in relevant positions have access to data during foreign student admissions, with monitoring provided by an administrator.

13. Access Control in Systems

The University uses an electronic learning management system with username and password authentication mechanisms. User authorization levels and roles are defined programmatically, and the system integrates with Google platforms. Students access the portal using University-provided email and passwords, while academic and administrative staff are added by the system administrator.

Sharing usernames and passwords with third parties is strictly prohibited.

14. Activity Logging

Actions performed on electronic data are logged in the respective systems. For non-electronic data, designated employees must record all actions, including incidents related to disclosure or modification.

15. File Sharing

Electronic data is stored in shared files accessible to employees within the scope of their duties and only via corporate email.

16. Data Security Policy

Data security is ensured per the University's information security policy. Organizational and technical measures are implemented, such as penetration testing and restricting access to users whose roles involve data processing.

17. University Website

The University website (www.gau.edu.ge) serves informational purposes and does not allow third-party data uploads. It features updates on events, photos, and documentation such as charters, internal rules, and contact information. Explicit consent is obtained from data subjects for publishing identifiable or biometric data, confirmed via signed consent forms.

18. Data from LLC Geolab Website

LLC Geolab provides the University with relevant administrative data about students for processing discounts or other educational benefits. Course applicants register on the Geolab website and provide data such as name, email, personal ID, phone number, residential address, and more. The site also stores standard information like IP addresses.

19. Use of Cookies

The University uses the following cookies:

A. **october_session**: Identifies user sessions with a unique ID.

B. **_ga**: Installed by Google Analytics to track visitors, sessions, and site usage for analytics reports. Stores data anonymously.

C. **_gid**: Installed by Google Analytics to store data on user behavior and create reports about site performance.

D. ***gat_gtag_UA****: Used by Google Analytics to store unique user IDs.

E. ***ga****: Used by Google Analytics to store and calculate page views.

F. **YSC**: Tracks embedded YouTube video views.

G. **VISITOR_INFO1_LIVE**: Measures YouTube bandwidth.

H. **VISITOR_PRIVACY_METADATA**: Stores user cookie consent status on the current domain, used by YouTube.

I. **guest_id**: Used by Twitter to identify website visitors and track their activity. If the user is logged into Twitter, it registers and collects information about advertising preferences.

20. The University's website integrates Google Analytics, which provides general information about the number of visitors, their countries of origin, their access method (direct link or social network), and the devices they use.

21. **Physical Document Storage**:

- Active employee records are stored in binders within a locked cabinet managed by the Human Resources Department.
- Scanned copies of all employee records are maintained digitally.
- Active student records are stored in physical format in the respective faculty deans' offices and are also scanned. Access to these documents is controlled and tracked.

22. **Archiving**:

- Both physical and digital formats of employee and student records are archived.
- Student Services handles the archiving of physical student records, while the HR Department archives non-active employee files.
- Archived materials are stored in a designated University storage room, accessible only to authorized personnel based on their roles.
- The IT Department manages the electronic archiving of data on secure hard drives.

23. **Sensitive Data**:

- Information such as health-related data is securely stored in personal files and electronic systems, accessible only to authorized personnel with logging of access.

24. The University prepares a **Data Protection Impact Assessment Document**, which includes:

- Description of data categories, processing purposes, proportionality, processes, and legal bases.
- Evaluation of potential risks to fundamental rights and freedoms.
- Organizational and technical measures for data security.

Article 10: Data Retention Periods

1. The University retains only the data necessary to achieve specific, lawful processing purposes.
2. Personal data is stored in the filing system for a duration sufficient to achieve legitimate purposes, as defined by the data controller and subject.
3. Special categories of data are stored using automated and non-automated means for durations necessary to achieve legitimate purposes.
4. Retention durations comply with legal requirements. When determining storage periods, the University considers personal data processing principles.
5. **Retention Periods for Physical Data**:
   a) Student personal records: **75 years**.
   b) Employee personal records: **75 years**.
   c) Bachelor's, Master's, and Doctoral theses: **75 years**.
   d) Employee timesheets: **1 year**.
   e) Student exam papers: **3 years**.
   f) Student applications: **3 years**.
   g) Decisions of academic and administrative councils: **75 years**.
   h) Meeting minutes of academic and administrative councils: **3 years**.
6. After the retention period expires, physical documents are destroyed, with an official record prepared to confirm their destruction.

Article 11: Access to Data

1. Employee Access

Employees are granted access only to the data necessary to fulfill their job responsibilities. In cases where an employee is on leave or unable to perform their duties for other reasons, their replacement is granted access to the same data as the employee they are substituting, within the limits and procedures defined in the order assigning their temporary role.

2. **Access to the University's Electronic Learning Management System**

Access to the electronic learning management system is granted to:
a) Faculty deans' office staff;
b) Academic process management staff;
c) Legal department (restricted access);
d) Financial department (restricted access);
e) Human resources management department (restricted access);
f) Records management department (restricted access);

g) Marketing and communications department (restricted access);
h) Strategic development department (restricted access).

3. **Access to Financial Accounting System**

Access to the financial accounting system is available to the financial department. With authorization from the head of the HR department, employees may also access data necessary for payroll processing.

4. **Access to Student Card System**

Access to the student card system is available to the relevant school dean, school administration, IT department, marketing department, and examination center staff.

5. **Access to Admissions Mail Group**

Access to the admissions.gau.edu.ge mail group is limited to student admissions office managers.

6. **Access to LLC Geolab Data**

Data managed by the University's study center (LLC Geolab) is stored on the University's Google Drive and is accessible to University employees.

7. **Access to Google Meet**

Access to Google Meet for remote meetings is granted to students, lecturers, and any other individuals using the University's corporate email.

8. **Access to Employee Personal Files**

The HR department has access to material documents and records in employees' personal files to manage and update the relevant information.

9. **Access to Minutes of Collegial Bodies**

The chancellery has access to the minutes of collegial bodies for registration and storage purposes.

10. **Access to the Document Management System**

a) **Full access** is granted to the chancellery and legal department for managing incoming correspondence and ensuring appropriate responses.
b) **Restricted access** is granted to the HR and financial departments for reviewing distributed correspondence and preparing appropriate responses.

Article 12: Data Disclosure/Transfer

1. Data processed by the University may be disclosed to the following third parties as per legal grounds and regulations:
   a) Law enforcement agencies;
   b) Courts;

c) Personal Data Protection Service;
d) Other legally designated authorities.

2. Additionally, data may be transferred to:
a) Ministry of Education, Science, Culture, and Sport of Georgia;
b) Ministry of Justice;
c) Ministry of Defense;
d) Law enforcement bodies;
e) Governmental or local self-government bodies as per legal requirements;
f) International organizations for academic and administrative purposes to serve the best interests of students and employees;
g) Organizers of higher education activities;
h) National Center for Educational Quality Enhancement under the Ministry of Education, Science, and Youth;
i) Education Management Information System (EMIS);
j) Revenue Service;
k) Audit firms;
l) LLC "Fitpass" (with data subjects' consent obtained via electronic questionnaires);
m) Insurance Company "Euroins" (subject consent is expressed by signing an agreement);
n) Self HR Portal for managing human resources;
o) Banks for payroll card issuance;
p) National Assessment and Examinations Center;
q) Other higher education institutions for student mobility purposes;
r) The university's contractor companies, where the university's students undertake internships and practical training for the purpose of gaining work experience, in accordance with the syllabus/syllabi of the program(s).

2[1] The University's Research Development and Support Office shares registration data and photos of attendees at events and courses organized by the University with donors as part of projects.

2[2] The Strategic Development Office conducts various studies annually, including semester surveys via self-administered questionnaires linked to the student portal. Data is grouped for analysis by nationality, level, program, course, and group. Annual surveys are conducted using Google Forms, and the University compiles reports to share with donors, schools, departments, or offices via email.

2[3] The University's Foreign Student Admission Office grants marketing material access to consulting companies, with access levels defined by management and monitored by an administrator.

3. The University engages third parties for assistance in service delivery, internal IT system management, and maintenance.

4. In cases of data disclosure as outlined in points 1-23, the University informs data subjects and logs details of the disclosed data, recipients, timing, and legal basis. This log is maintained alongside the subject's data for the duration of its retention period.

5. The University uses the gau.self.ge portal, providing an electronic database for human resource management, including personal and contact information, salaries, attendance, and leave records.

Article 13: Video Monitoring

1. The University employs a video monitoring system to fulfill legal obligations related to personal and property security and to protect minors from harmful influences.
2. To inform data subjects about video monitoring, warning signs and contact information for the person responsible for data processing are displayed in visible areas.
3. Employees whose workspaces fall within the monitoring system's field of view are duly informed about this.
4. The video monitoring system and recordings are protected from unauthorized access and use. Access is granted only to the head of the security service, secured with a username and password. Each instance of access is logged, including the time and user identity, enabling the identification of the accessing individual.
5. The system uses encryption and self-destruction mechanisms. Camera monitors are located in a locked security room. Authorized access to the keys and video monitoring data is restricted to security personnel. During examination periods, exam halls are monitored by representatives of the examination service.
6. Retention of video monitoring data is limited to 30 calendar days, after which it is automatically deleted unless the recording is attached to documentation for disciplinary proceedings.

Article 14: Access Control for Video Monitoring System

1. The University's video monitoring system provides the following access levels:

a) Real-time monitoring:

- Users with this access can only view live footage without the ability to rewind or download recordings to devices.

b) Rewinding and reviewing recordings:

- Users can monitor live footage and rewind or review recordings but cannot download them.

c) Downloading recordings:

- Users can monitor live footage, rewind and review recordings, and download recordings to local networks for authorized personnel upon approval.

d) Technical support:

- Users can create and delete system users, monitor system activity logs, resolve technical issues, and make configuration changes.

Note: Access to the video monitoring system is strictly individual and controlled by usernames and passwords.

Article 15: Direct Marketing

1. The University engages in direct marketing during promotional meetings with high school seniors in regions to share information for future campaigns. Information is sent via email and SMS.

1. Students periodically receive informational messages via SMS. During their studies, the student periodically receives various types of informational messages in the form of SMS as stipulated in their contracts.

2. Applicants provide personal information for attending University events and lectures, which is used for communication and offering additional events.

3. The University conducts direct marketing through schools, training centers, social media, and its events.

4. As a University training center, LLC Geolab engages in direct marketing about vacancies, internships, and free programs via email.

5. The University ensures compliance with Georgian legislation by obtaining data subjects' consent for marketing purposes.

6. Apart from the data subject's name, surname, address, phone number, and email address, if the processing of additional data is required for direct marketing purposes, the university ensures that written consent is obtained from the data subject.

7. Before obtaining the data subject's consent and during the implementation of direct marketing, the data subject(s) will be clearly, simply, and in an understandable language informed about their right to withdraw consent at any time, as well as the mechanism/procedure for exercising this right.

8. For the purpose of direct marketing, when processing data, the university records the time and fact of the data subject's consent to data processing and its withdrawal. This information is stored for the duration of direct marketing activities and for one (1) year after the cessation of direct marketing.

9. For the purpose of direct marketing, after providing consent and registering the phone number, in case of a change in the phone number, the data subject is entitled to contact the authorized person responsible for processing using the provided contact details and inform them of the change to ensure the accurate and correct recording of data. Article

16: Data Protection Officer

1. **Role of the Officer:**

- The University appoints a Data Protection Officer responsible for ensuring compliance with personal data protection legislation.
- The officer operates independently in their duties.

2. **Responsibilities:**
   a) Monitor data processing within the University.
   b) Assess risks in data processing when necessary.
   c) Collaborate with the Personal Data Protection Service when needed.
   d) Inform and train staff on data protection issues.
   e) Address data subjects' inquiries, complaints, and requests.
   f) Provide consultations on data protection to students, lecturers, and employees.
   g) Maintain and submit catalogues of file systems to the Personal Data Protection Service.
   h) Identify, investigate, and appropriately respond to data breaches.

Article 17: Policy Updates and Additional Information

- The policy is subject to updates as necessary when specific aspects of data processing change.
- Changes to the policy are implemented by an order from the University Chancellor.