Georgian American University, LLC

Policy for the Processing of Personal Data   1

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 "HR Digital Corporation" is an outsourcing company specializing in human resource management. It provides the University with access to a digital tool, DHR, which the University uses to manage human resource processes digitally.

LLC "HR Digital Corporation" 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 "HR Digital Corporation" 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 "HR Digital Corporation" 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 "HR Digital Corporation" 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.

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 –

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 (er)5eTf1 0 0 ,er

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

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.

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.

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**

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

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

2. Additionally, data may be transferred to:
   a)

8.

- 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. **Purpose of Direct Marketing:**

   -

- o The University records the time and fact of consent and its withdrawal, retaining this information for one year after marketing activities cease.

10. **Updating Contact Information:**

Data subjects must notify the University of phone number changes to ensure accurate records for marketing purposes.

Article 16: Data Protection Officer

1. **Role of the Officer:**

   - o The University appoints a Data Protection Officer responsible for ensuring compliance with personal data protection legislation.

   - o 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.