Approved by the resolution of the Academic Council of the
University of THU No. 07 of 02 May 2025

Personal Data Processing Policy

1. General information about the document

The Personal Data Processing Policy (hereinafter referred to as the Policy) aims to ensure transparency in the processing of personal data by the Tbilisi Humanitarian University (hereinafter referred to as the University). The Policy allows any person, including the data subject and/or potential data subject, to receive information about the processing of personal data by the institution in a simple and understandable language.

Personal data (hereinafter referred to as data) is any information relating to an identified or identifiable natural person. A natural person is identifiable when he or she can be identified, directly or indirectly, including by name, surname, identification number, geolocation data, electronic communication identifiers, physical, physiological, mental, psychological, genetic, economic, cultural or social characteristics.

Personal data is processed in accordance with Georgian legislation, in particular, the Law of Georgia on Personal Data Protection and other regulatory acts. The rights of the data subject are protected both under Georgian legislation and in accordance with the European General Data Protection Regulation (GDPR).

Personal data processing is carried out in accordance with the following principles provided for by Georgian and international legislation, in particular, the GDPR:

- Principle of fairness;
- Transparency;
- Purpose limitation principle;
- Data minimization principle;
- Time minimization principle;
- Data accuracy principle;
- Security principle.

The Policy ensures the implementation of subparagraph “a” of paragraph 1 of Article 4 of the Law of Georgia “On Personal Data Protection”, according to which

data must be processed lawfully, fairly, transparently for the data subject and without violating his or her dignity.

The terms used in the Policy have the meaning defined in the Law of Georgia "On Personal Data Protection".

The Policy is available on the University's website and all data subjects have the opportunity to familiarize themselves with it.

2. General information about the activities of LLC Premium Safety

LLC Premium Safety is a consulting company that ensures compliance of partner companies with the law in various areas. One of the areas of its activity is the provision of personal data officer services, officer assignment, implementation of full documentation, and bringing the activities of the client company into compliance with the law.

3. General information about the person responsible for data processing

LLC Tbilisi Humanitarian University is a higher educational institution that processes the data of students, employees and other third parties, including minors, in order to perform its functions. The data processed about the subjects include personal data of students and employees, information about the student's assessment and activity during his/her studies at the university.

The protection of personal data is the right of all members of society, therefore data processing is a clearly regulated process and the university ensures the protection of the personal data of all members, for which it has developed a personal data processing rule and has appointed a personal data protection officer.

4. General information about the person authorized to process data

4.1. The University has persons authorized to process data who process data only for the legitimate purposes of the University.

4.2. Relevant agreements have been signed between the University and the authorized persons, which, among other things, include the regulation of personal data protection issues and the authorized person(s) are obliged to ensure the confidentiality of the data processed by them within the framework of the service.

4.3. The University monitors the technical and organizational measures and data processing by the authorized persons in the performance of their functions and duties.

4.4. Upon request, the University ensures the provision of information about the authorized person(s) to the data subject(s) in accordance with the procedure established by the Law of Georgia on Personal Data Protection.

5. Rules for the processing of personal data by LLC Tbilisi Humanitarian University

5.1. Preamble

The University's Personal Data Processing Rules have been developed on the basis of the Law of Georgia on Personal Data Protection and other regulatory acts. The University's Personal Data Processing Rules are used by the institution in the process of processing data of subjects and apply to any form of data processing by the institution.

5.2. Person responsible for data processing:

LLC Tbilisi Humanitarian University - registered in accordance with the legislation of Georgia as a legal entity of public law

Identification code: 2060046045

Address: Tbilisi, Isani district, 31 Beri Gabriel Salosi avenue. Telephone number: (+995 32) 255 24 24

E-mail: thu-posta@thu.edu.ge

5.3 Personal Data

Protection Officer: Ltd "Premium Safety"

Identification code: 405656320

Address: Tbilisi, Vake district, Kipshidze street N2, building 2b, 73

Telephone number: (+995) 577 17 64 61 E-mail: zura.gujabidze@geosafety.ge

5.4 "Personal Data Processing Policy"

Article 1. General Provisions

1. This Rule regulates issues related to the processing of personal data by the University.

2. This document applies to any person employed by the University and acting on behalf of the University, as well as to interns (if any) and is mandatory for implementation.

3. This Rule shall be applied in conjunction with and in accordance with the Law of Georgia "On Personal Data Protection".

Article 2. Definition of Terms

1. For the purposes of this Rule, the terms used in this Rule have the meaning provided for in the Law of Georgia "On Personal Data Protection":

a) Personal data (hereinafter referred to as data) – any information relating to an identified or identifiable natural person. An individual is identifiable when he or she can be identified, directly or indirectly, including by name, surname, identification number, geolocation data, electronic communication identification data, physical, physiological, mental, psychological, genetic, economic, cultural or social characteristic;

b) Special category data – data relating to a natural person's racial or ethnic origin, political opinions, religious, philosophical or other beliefs, trade union membership, health, sex life, status of the accused, convicted, acquitted or victim in criminal proceedings, conviction, conviction, diversion, recognition as a victim of human trafficking or crime in accordance with the Law of Georgia on Prevention of Violence against Women and/or Domestic Violence, Protection and Assistance to Victims of Violence, imprisonment and execution of a sentence, as well as biometric and genetic data processed for the purpose of uniquely identifying a natural person;

c) health-related data – information about the physical or mental health of the data subject, as well as information about the provision of medical services to him, if it provides information about the physical or mental health of the data subject; d) biometric data – data processed using technical means, related to the physical, physiological or behavioral characteristics of the data subject (such as, for example: facial image, voice characteristics or dactyloscopic data), which allows for his unique identification or confirmation of his identity;

f) Data processing - any operation performed on data, including their collection, retrieval, access, photography, video and/or audio monitoring, organization, grouping, interconnection, storage, alteration, retrieval, retrieval, use, blocking, erasure or destruction, as well as disclosure of data by transmission, publication, dissemination or otherwise making available;

g) Automatic data processing - data processing using information technology;

h) Non-automatic data processing - data processing without the use of information technology;

i) Semi-automatic data processing - data processing using a combination of automatic and non-automatic means;

j) File system - a structured set of data in which they are arranged and accessible according to specific criteria;

l) Data subject - any natural person about whom data are processed;

m) Consent of the data subject - the data subject's active, freely and clearly expressed consent, in writing (including electronically) or orally, to the processing of data concerning him or her for a specific purpose, after receiving relevant information;

n) Written consent of the data subject - consent, which the data subject has signed or which he or she has otherwise expressed in writing (including electronically) to the processing of data concerning him or her for a specific purpose, after receiving relevant information;

o) Person responsible for processing - a natural person, legal entity or public institution that individually or jointly with others determines the purposes and means of data processing, carries out the processing of data directly or through a person authorized to process;

p) Persons responsible for joint processing - two or more persons responsible for processing, who jointly determine the purposes and means of data processing;

q) Data processor – a natural person, legal entity or public institution that processes data for or on behalf of the data controller. A natural person in an employment relationship with the data controller is not considered a data processor;

r) Data recipient – a natural person, legal entity or public institution to which the data has been transferred, except for the Personal Data Protection Service;

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

2. Other terms contained in these Rules, unless otherwise specified, shall be interpreted in accordance with the Law of Georgia on Personal Data Protection.

Article 3. Purposes of data processing

The purposes of personal data processing by the University are:
a) implementation of educational activities;
b) implementation of official activities;
c) ensuring the smooth flow of the educational process;
d) ensuring the smooth flow of the work process;
e) registration of students;
f) maintenance of personal files of students and employees;
g) ensuring the registration and assessment of students;
h) realization of the right to education for students with special educational needs;
i) improvement of databases for the purpose of creating an electronic assessment system;
j) organization and control of document circulation;

k) issuance of documents confirming higher education;
l) ensuring the involvement of students and employees in various activities;
m) provision of information requested by the LEPL - Education Management Information System, uploading data to their database;
n) ensuring the protection of the institution's property, property, and the physical safety of employees and/or students; n) exercising other powers assigned by law.

Article 4. Grounds for data processing

1. Personal data shall be processed on the following grounds:

a) the data subject has given his consent to the processing of data concerning him for one or more specific purposes;
b) the processing of data is necessary for the performance of an obligation to which the data subject has entered into a contract or for the conclusion of a contract at the request of the data subject;
c) the processing of data is necessary for the performance of a legal obligation imposed on the institution;
d) the processing of data is provided for by law;
e) in accordance with the law, the data are publicly available or the data subject has made them publicly available;
f) the processing of data is necessary to protect the vital interests of the data subject or another person;
g) the processing of data is necessary to protect the important legitimate interests of the controller or a third party, except where there is an overriding interest in the protection of the rights of the data subject (including minors);
h) Data processing is necessary to process the data subject's application (to provide a service to him/her).

2. The institution shall process special category data only if:

a) the data is processed for the purpose of realizing the right to education of persons with special educational needs;
b) the processing of data related to convictions for committing crimes against sexual freedom and inviolability and health status is necessary due to the nature of the labor obligation and relationship. Including for making a decision on employment. According to Part 2 of Article 32 of the Law of Georgia on Higher Education: A person convicted of committing crimes against sexual freedom and inviolability and/or a person who has been deprived of the right to work in an educational institution by a court on the basis of the same law may not be employed in a higher educational institution.

3. In the event that the institution processes data with the consent of the data subject, consent shall only be considered valid if it is given after receiving relevant information, voluntarily, for a specific and specific purpose of processing the data. Consent shall be given voluntarily and with

the active participation of 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 an employment contract;
b) candidates participating in a competition for vacant positions;
c) students;
d) minors1;
e) contractors/authorized representatives of contractors in contractual relations with the organization;
f) other persons covered by video surveillance.

Article 6. Rights of the data subject

1. The data subject has the right to:
a) receive information about the processing of his/her data;
b) receive information about the co-processor and/or the authorized person;
c) receive information about the purposes, grounds and categories of data processing;
d) receive information about the identity or category of data recipients to whom the data have been or will be transferred in the future;
e) receive information about the period for which the data will be stored, or if a specific period cannot be determined, about the criteria for determining the period;
f) receive any available information about the source of data collection, if the data is not collected directly from the data subject;
g) request access to the data and a copy;
h) request the immediate correction, updating, transfer of incorrect/inaccurate data processed about him or her or, taking into account the purposes of data processing, the completion of incomplete data, including by submitting additional information/documents;
i) request the termination of data processing, deletion of data or destruction of data with consent;
j) request the blocking of data.

2. In order to exercise the rights provided for in the first part of this Article, the data subject must contact the person authorized to process or the person responsible for processing, if the data are stored with him.

---

1 In exceptional cases. Namely, when a student is entering the first year and has not yet turned 18. In such a case, like all students, a minor must submit all necessary documents together with a legal representative.

3. The data subject is informed in accordance with the policy about who is storing the data and responding to the request made by the data subject within the framework of the above-mentioned rights, within the framework of the relationship between the university and a specific organization.

4. In case of a request from the data subject, the University is obliged to provide the relevant information to the data subject no later than 10 (ten) working days from the receipt of the notification of the request. This period may be extended in exceptional cases and with due justification for no more than 10 working days, of which the data subject shall be immediately notified.

5. The data subject has the right, at any time, to withdraw the consent granted by him/her without any explanation or justification. Consent may be withdrawn in the same form in which the consent was granted.

6. The rights of the data subject may be restricted in the cases and in accordance with the procedure provided for by the Law of Georgia "On Personal Data Protection".

7. In the event that the actions to be taken to exercise the rights of the data subject fall within the powers of other agencies involved in the data processing process, such as the Personal Data Protection Service, the institution is entitled to explain this to the data subject in writing.

8. The data subject enjoys all other rights of the subject provided for by the Law "On Personal Data Protection".

9. The data subject is entitled to address any issue related to the processing of personal data to the Rector of the University and/or the Personal Data Protection Officer.

10. In the event of a dispute on issues related to the protection of personal data, the data subject has the right to address the Personal Data Protection Service and/or the court in accordance with the procedure established by law.

Article 7. 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 number, copy of ID card, photograph, date of birth, gender;

b) Contact data - legal and actual addresses, telephone, e-mail;

c) Special category data:
c.a) Certificate of conviction for committing a crime against the sexual freedom and inviolability of academic and administrative personnel, processing is necessary due to the nature of the labor obligation and relationship, including for making a decision on employment;
c.b) Employee's hospital record; d) Certified copies of diplomas;

e) Employment status;

f) Any other information provided for by the relevant service, as well as the regulatory acts of the university.

g) Work experience - position, position, salary, qualifications, remuneration;

h) Statement and/or document confirming the employee's consent to the establishment of an employment relationship;

i) Copy of identity document/passport;

j) Copy of education or relevant qualification document, certificates confirming teaching experience.

k) Student's school certificate;

l) Autobiography - Curriculum Vitae (CV);

m) 1 photograph in digital form;

n) Official details of a valid bank account;

o) Document confirming withdrawal from the pension scheme within the framework of the accumulative pension reform, if any;

p) In case of benefiting from income tax relief, a document confirming this - a certificate from the Revenue Service;

q) Syllabuses in printed and electronic form;

r) Document confirming foreign language proficiency;

s) Video images of other individuals within the video monitoring area;

t) Military registration certificate (in the case of male employees);

u) Military registration certificate (in the case of male students);

v) In case of mobility, a certificate/report card from the previous institution;

w) Information about the student's academic performance;

x) Information about the student's former university(s);

y) Legal acts determining the student's status;

z) Identification data of the deceased - for the purpose of reflecting the deceased student or termination of student status in the database of the Ministry of Education, Science and Youth.

Article 8. Sources of data receipt

The sources of personal data receipt for the University are:

a) provision of data based on the explicit, actively expressed consent of the data subject;
b) data obtained through video monitoring;
c) data obtained from the electronic portal (thu.edu.ge), in which the subject fills in his/her name, surname, telephone number, and e-mail address;
d) receipt of data from the Higher Education Management Information System;
e) obtaining information from any lawful source for the purposes specified in this Rule and/or by law.

Article 9. Data Security and Employee Obligations

1. The University shall ensure the security of data by taking appropriate, organizational and technical measures, protecting them from accidental or unlawful destruction, alteration, disclosure, retrieval, any other form of unlawful use and accidental or unlawful loss.

2. The University shall be obliged to inform the data subject in detail about what data it collects, how it uses them, to whom it transfers them and how it protects the security of the data.

3. Any person employed by the University who participates in data processing or who has access to the data shall be obliged to:

a) not to exceed the scope of the authority granted to him;
b) to protect the secrecy and confidentiality of data, including after the termination of official authority;
c) not to use data for personal, non-official purposes;
d) not to make data available to unauthorized persons, including by leaving data unattended and/or reviewing it in the presence of unauthorized persons.

4. Violation of the rules established by this document constitutes a violation of the University's internal labor regulations and may entail appropriate disciplinary action.

5. Access to data is available only to those employees and to the extent that they need the data to perform their functions and duties.

6. Access to electronic systems used by the University is possible only through an individual username and a password containing a complex combination, which is updated once every 3 months. It is prohibited to disclose/transfer the username and password to anyone.

7. Actions performed on data in electronic form are recorded/logged in the appropriate electronic journals. When processing data in non-electronic form, the relevant person(s) employed by the institution are obliged to ensure the recording of all actions related to the disclosure and/or change of data (including information about incidents).

8. The data is stored on the University's secure server, which is located in Georgia, namely, in

Tbilisi, namely, Beri Gabriel Salosi Avenue N31. It is locked with a mechanical key. The IT manager has full access to the server.

9. The University has allocated a separate specially protected space in which the data is stored in archived form. Entry to this space is subject to special authorization and is recorded.

10. Special category data is stored in the office of the Human Resources Management and Case Management Service and is accessed only by authorized persons. A security and access recording system is provided.

11. The University shall develop a data protection impact assessment document, which shall include: a description of the categories of data, the purposes, proportionality, process and grounds for their processing; an assessment of the possible threats to the fundamental rights and freedoms of a person and a description of the organizational and technical measures taken to protect the security of data.

Article 10. Data retention periods

1. The University shall retain only those data that are necessary to achieve the specific, lawful purpose of data processing.

2. Special categories of data shall be retained by both automated and non-automated means for the period necessary to achieve the legitimate purpose of the processing of personal data on the basis provided for by the controller and the data subjects.

3. Data shall be retained in accordance with the periods specified by law. If it is necessary to determine the periods and rules for data retention, the University shall take into account the principles of personal data processing.

4. The following deadlines are established for the storage of data in physical form at the University:
a) Personal files of employees are stored for a period of 75 years;
b) Personal files of students are stored for a period of 75 years;
c) Working time registration forms are stored for a period of 1 year.
d) Information about candidates participating in the competition announced for filling vacant positions is stored for a period of 1 year.
e) Minutes of the meeting of the collegiate body - for a period of 5 years.

5. Documentation in physical form (current documents, active personal files) is stored in the Human Resources Management Service. Access to documents and/or information stored in them is possible only by receiving the specified documentation from the Head of the Human Resources Management Service and registering it accordingly.

---

[2] In addition to those listed in the above article, when determining the deadlines, the University is guided by the "Order No. 72 of the Minister of Justice of Georgia "On Approval of the List of Typical Administrative Documents Created in the Process of Institutions' Activities (with Indication of Their Storage Deadlines)" dated March 31, 2010, Tbilisi.

6. Documentation in physical form (personal files, minutes of the meeting of collegiate bodies) that is not in active use is archived and stored in a specially designated room. The room is locked with a key, which is kept by the Head of the Human Resources Management Service. Access to archived documents is possible with the permission of the Director, provided that there is an appropriate written basis.

7. After the expiration of the storage period, documents in physical form are destroyed, about which a corresponding act is drawn up.

Article 11. Access to data

1. Employees have access only to the data and to the extent necessary to perform their duties. In the event of the employee's vacation or other reason, the latter's access to information is determined by the assigned duty.
2. (QMS.EQE.GE) has access to:
a) The Head of the Human Resources Management Service
5. The Human Resources Management Service has the right to access the personal files (material documents) of employees and/or the case materials contained in the personal file.
6. The secretaries of the relevant faculty have the right to access the personal files (material documents) of students and/or the case materials contained in the personal file.
7. The document circulation system and the information contained therein:
a) The Rector and the Head of the Human Resources Management Service have the right to full access - for the purpose of distributing incoming correspondence and ensuring appropriate response;
b) Other employees have the right to limited access - for the purpose of reviewing the correspondence distributed to them and preparing appropriate responses.

Article 12. Data transfer/disclosure

1. Data processed by the University, if there is a legal basis, may be transferred to the following third parties in accordance with the procedure and to the extent established by law:
a) Law enforcement agencies; b) Court;
c) Personal Data Protection Service;
d) Other bodies provided for by law.
2. Data may also be transferred to:
a) Ministry of Education, Science and Youth; b) Ministry of Justice;
c) Ministry of Defense;
d) Law enforcement agencies;
e) Government and/or local self-government bodies in cases specified by law;
f) International organizations, when necessary for academic, administrative purposes in the best interests of students and employees;
g) LEPL - National Center for Education Quality Development within the system of the Ministry of Education, Science and Youth of Georgia;
h) LEPL - Education Management Information System; i) LEPL - Revenue Service;
j) Other persons provided for by legislation.

3. In the cases provided for in paragraphs 1 and 2 of this Article, when disclosing information, the University shall record which data was disclosed, to whom, when and on what legal basis. This information shall be stored together with the data on the subject for the period of their storage.

Article 13. Video monitoring

1. The University shall use the video monitoring system to fulfill its obligations under the law - for the purposes of protecting the safety and property of a person, as well as protecting minors from harmful influences. In addition, the University may conduct video monitoring during the examination.
2. In order to inform data subjects about data processing, appropriate warning signs shall be placed in visible places in the building.
3. The University shall ensure that employees whose work areas fall within the field of view of the video surveillance system are duly informed.
4. The video monitoring system and recordings are protected from unauthorized access and use. Access to it is protected by a username and password.
5. The video monitoring system is protected by an encryption function and is equipped with an appropriate self-destruct mechanism. A circle of persons authorized to access data obtained through video monitoring has been developed, which is represented by:
a) IT manager - full access.
6. The storage period of data obtained through video monitoring is 30 calendar days, after which the data is automatically destroyed by the system.
7. In the cases provided for in paragraphs 1 and 2 of this Article, when disclosing information, the University shall record which data was disclosed, to whom, when and on what legal basis. This information shall be stored together with the data about the subject for the duration of their storage.

Article 13. Video Monitoring

1. The University uses the video monitoring system to fulfill its obligations under the law - to protect the safety and property of a person, as well as to protect minors from harmful influences. In addition, the University may conduct video monitoring during the exam.
2. In order to inform data subjects about data processing, appropriate warning signs are placed in visible places in the building.
3. The University ensures that employees whose work space falls within the field of view of the video surveillance system are properly informed.
4. The video monitoring system and recordings are protected from unauthorized access and use. Access to it is protected by a username and password.
5. The video monitoring system is protected by an encryption function and is equipped with an appropriate self-destruct mechanism. A circle of persons authorized to access data obtained through video monitoring has been developed, which is represented by:
a) IT Manager - full access.
6. The storage period of data obtained through video monitoring is 30 calendar days, after which

the data is automatically destroyed by the system.
7. The video monitoring area includes:
a) the common area of the institution;
b) corridors;
c) "foyer"
d) the external perimeter of the institution, which includes - the external space of the institution, the entrance.
8. Video monitoring is not carried out in changing rooms, areas intended for hygiene or in such a space where the subject has a reasonable expectation of privacy and/or the implementation of video monitoring contradicts generally recognized moral norms.

Article 14. Access control to the video monitoring system

The following types of access are defined within the video surveillance system owned by the University:
a) Monitoring of video surveillance cameras in real (online) mode - a user with this access can only monitor current footage. He has limited rights to scroll and download the recording (to a computer or other media carrier);
b) The right to scroll and track the recordings of video surveillance cameras - a user with this access can both monitor the cameras in real mode, as well as scroll and track the recordings, but has limited rights to download the recording (to a computer or other media carrier);
c) Downloading video surveillance camera recordings - a user with this access can monitor cameras in real time, rewind and track recordings, download recordings to the local network and, if approved, deliver them to an authorized person;
d) Technical support rights - a user with this access has the right to create new users in the video surveillance system, cancel existing users, monitor electronically performed actions (logs) in the video surveillance system, perform various actions to eliminate errors in the event of technical problems, as well as make configuration changes.

Note: A user is any person who has access to the video surveillance system. Access to the video surveillance system is provided only through an individual user name and password.

Article 15 Personal Data Protection Officer

1. The University has a Personal Data Protection Officer who ensures compliance of personal data processing processes with personal data protection legislation.

2. The Personal Data Protection Officer is independent in his/her activities and is subordinate to the Rector of the University.

3. The Personal Data Protection Officer:
a) informing the person responsible for processing, the person authorized to process and their employees on issues related to data protection, including the adoption or amendment of regulatory legal norms, providing them with consultation and methodological assistance;
b) participating in the development of internal regulations related to data processing and a data protection impact assessment document, as well as monitoring the compliance of the person responsible for processing or the person authorized to process with the legislation of Georgia and

internal organizational documents;
c) Analysis of applications and complaints received regarding data processing and issuing relevant recommendations;
d) Receiving consultations from the Personal Data Protection Service, representing the person responsible for processing and the person authorized to process in relations with the Personal Data Protection Service, submitting information and documents at its request, and coordinating and monitoring the implementation of its tasks and recommendations;
e) Providing information about data processing processes and their rights upon request of the data subject;
f) Performing other functions by the person responsible for processing or the person authorized to process in order to raise data processing standards.

Article 16. Policy Update

In the event of changes in individual issues related to data processing, the Policy shall be subject to update as necessary.