Personal Data Protection Policy at LEPL Ilia State University

This policy was developed to ensure that personal data protection at Ilia State University complies with Georgian legislation and European Union regulations. This policy incorporates the essential principles and approaches for the effective protection of individuals' personal data.

Chapter I. General Provisions

Article 1. Legal Basis and Purpose

1. The "Personal Data Protection Policy" of Ilia State University, a Legal Entity of Public Law (hereinafter referred to as the "University"), has been developed by the Law of Georgia on Personal Data Protection (hereinafter the "Law"), the General Data Protection Regulation (GDPR), and the University's Statute and Bylaws.
2. The purpose of this policy is:
   a) To ensure the protection of the rights and freedoms - including the inviolability of personal life - of the University's administrative, academic, support, and invited personnel, students, as well as third parties acting on behalf of the University, in the course of personal data processing and disclosure;
   b) To develop a personal data protection strategy within the University, incorporating fundamental principles and mechanisms of data protection;
3. The principles of personal data processing within the University are as follows:
   a) Lawfulness, fairness, and transparency: personal data shall be processed lawfully, fairly, and transparently.
   b) Legitimate purpose: personal data shall be processed for specified, explicit, and legitimate purposes, using means that are proportionate and necessary. Personal data shall not be processed unless there is a legitimate purpose.
   c) Data minimization: the collected data must be adequate, relevant, and limited to what is necessary.
   d) Accuracy: the data must be accurate and up to date.
   e) Storage limitation: personal data must be stored in a form and for a period that allows the identification of data subjects for no longer than is necessary.
   f) Integrity and confidentiality: personal data must be processed in a manner that ensures security and confidentiality.
   g) Accountability and responsibility: the University is responsible for the processing of personal data and is accountable to the data subject(s) for any case or incident.

Article 2. Definitions of Terms

1. The terms used in this policy are defined in accordance with Article 3 of the Law of Georgia on Personal Data Protection.

Article 3. Data Processing

1. The University processes data using automated, semi-automated, and manual methods.
2. The University processes the personal data of students, academic, administrative, and support staff, as well as other individuals, as defined by law, contracts, and the University's Bylaws.

3. Within its authority, the University issues orders and, for this purpose, processes personal data related to the granting, suspension, termination, or restoration of student status, as well as the allocation of social benefits, scholarships, and other actions provided for by law. The University may publish an order for public disclosure if required by law or if it involves more than 50 individuals.
4. The University, based on the interests of students and staff, processes special categories of personal data - such as data concerning health - solely based on the data subject's request and with their explicit consent. The format and procedure for obtaining the data subject's consent are set out in the relevant documentation.
5. The University is entitled to process data to prevent and detect plagiarism.
6. The University is authorized to process personal data in the context of conducting disciplinary measures.
7. The University handles the personal data of minors based on the consent of their legal representative.
8. The University processes the personal data of its academic and support staff, as well as applicants in pre-contractual relationships, based on human resource management and recruitment policies and the corresponding activities.
9. The University ensures continuous monitoring of the personal data protection process.
10. The University ensures that employees and students are informed about the processing of personal data through contracts, this policy, and other informational measures.

Chapter II. Personal Data Processing and Protection Standards

Article 4. Legal Grounds for Personal Data Processing

1. Personal data processing is permitted if:
   a) The data subject has given consent;
   b) Data processing is provided for by law;
   c) Data processing is necessary for the University to fulfill its obligations imposed by law;
   d) Data processing is necessary to protect the vital interests of the data subject;
   e) Data processing is necessary to protect the legitimate interests of the data controller (the University) or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject;
   f) Data is publicly accessible according to law or has been made accessible by the data subject;
   g) Data processing is essential for the protection of important public interests, as provided for by law;
   h) Data processing is mandatory to consider and respond to the data subject's request for the provision of a service;
2. For personal data processing to be based on the data subject's consent, such consent must:
   a. Be freely given;
   b. Be expressed prior to the processing of personal data;
   c. Be given after the data subject has received information regarding the processing of their personal data;
   d. Be expressed with a specific, clearly defined, and lawful purpose for data processing;

e. The means of expression shall be clear and capable of demonstrating the data subject's will.

Article 5. Processing of Special Categories of Data

1. The University shall process special categories of personal data only where the data subject has provided explicit written consent.
2. The processing of data relating to criminal convictions and health status is essential due to the nature of employment obligations and relationships, including for the purpose of making decisions regarding employment.

Article 6. Collection of Personal Data from Third Parties

1. Ilia State University may collect the data subject's personal data from third parties for the following purposes: to provide services to the data subject, in cases defined by Georgian legislation, to fulfil obligations imposed on the University by Georgian law, and to fulfil obligations undertaken by the University under contracts concluded with third parties, including organizations operating as legal entities under public law and partner organizations.
2. A third party refers to a natural and/or legal person, or an organization operating with the status of a legal entity under public law.

Article 7. Use of Email Address and Telephone Number

1. For the purpose of effective and rapid communication, the University processes the email addresses and telephone numbers of employed individuals, administrative staff, academic and visiting personnel, students, and alumni.

Article 8. Protection of Personal Data

1. The University ensures the protection of electronic data processing device(s) against unauthorized access and intentional damage. In addition, the University takes measures to ensure that data is protected against unlawful disclosure, alteration, any other form of unlawful use, and accidental or unlawful loss.
2. The University undertakes to implement appropriate technical and organizational measures, where necessary, to ensure a level of security appropriate to the risk, including:
   a. Pseudonymization and encryption of personal data.
   b. Measures that ensure the ongoing confidentiality, integrity, restricted access, and resilience of processing systems.
   c. Measures to ensure access to and the restoration of personal data in the event of a physical or technical incident.
   d. Regular testing, assessment, and updating of security measures to ensure their effectiveness.
3. The University ensures the protection of data stored in physical form against access by unauthorized or external persons.
4. Each employee of Ilia State University is provided, where necessary, with a personal computer that is protected by a designated user account and password, access to which is restricted to the specific employee to whom the computer is assigned. Employees are

prohibited from disclosing their user credentials, including username and password, through any means.

5. The University ensures that its databases are administered in a manner that allows, when necessary, for information to be provided individually to each student; academic, administrative, support, and visiting staff member; and any other relevant individuals associated with the University.
6. Any person employed at the University who becomes aware of a violation related to the processing of personal data is obliged to immediately report it to the University's Data Protection Officer.
7. The University considers the unlawful processing of personal data to be an administrative offense and ensures that the relevant authorities are informed accordingly.

Chapter III. Rights and Obligations of Data Subjects and Individuals Involved in the Processing of Personal Data

Article 9. Rights and Obligations of the Data Subject

1. The data subject has the right to request information from the University regarding the processing of their personal data. Within no more than 10 (ten) calendar days from the receipt of the request, the University shall provide the data subject with information on the categories of personal data being processed, the purpose and legal basis of the processing, and whether the data has been disclosed to any third party; if so, to whom it was disclosed.
2. The data subject has the right to withdraw their consent at any time, without providing any explanation or justification. In such cases, upon the data subject's request, the processing of personal data shall be terminated and/or the processed data shall be erased or destroyed within no later than 10 (ten) working days from the date of the request, unless a valid legal basis for the continued processing exists.
3. The data subject shall also have the following rights:
   a) Right to rectification: the right to request the rectification of inaccurate personal data.
   b) Right to restriction of processing: the right to restriction of processing under certain conditions defined by law.
   c) Right to data portability: the right to receive their data in a structured, commonly used format and to transfer it to another device or system.
   d) Right to object: The right to object to the processing of personal data where it is based on legitimate interests, direct marketing, or other legal grounds, and to challenge such processing through appropriate legal channels.
   e) Rights related to automated decision-making: The right not to be subject to decisions based solely on automated processing, including profiling.
   f) Other rights provided under Chapter Three of this Policy.
4. The withdrawal of consent by the data subject does not affect the lawfulness of processing or legal consequences arising from the consent prior to its withdrawal.
5. The data subject is obligated to provide the University with accurate and truthful personal data. The data subject shall bear responsibility for providing inaccurate personal data, whether intentionally or through negligence.

Article 10. Rights and Obligations of the Student

1. Before entering into a contract for educational services with the University, students are informed about the categories of personal data processed by the University.
2. Students (or their legal representatives, where applicable) are obliged to:
    a. Comply with this Policy when representing the University or participating in various activities on behalf of the University.
    b. Comply with this Policy while on university premises as students of the University.
    c. Notify the University of any changes to their personal data.
3. Violation of the *Personal Data Protection Policy at LEPL Ilia State University* constitutes grounds for initiating disciplinary proceedings against the student.
4. The processing of personal data during the procedure for awarding scholarships under the program 'State Scholarships for Students' (hereinafter - the 'Scholarship') is necessary for awarding the Scholarship to a specific group of individuals (students), in order to provide additional support for the exercise of their right to education.
5. The processing of personal data concerning a minor student who has reached the age of 16 may be carried out on the basis of their consent, except where otherwise provided by law - including cases in which the consent of both the minor (between the ages of 16 and 18) and their parent or legal representative is required.

5.1. When obtaining consent for the processing of a minor's personal data, the following circumstances must be taken into account:

    a. The purposes of processing personal data relating to minors must be clearly and specifically described, using language appropriate to their age.
    b. Consent must be clear, understandable, and easily accessible.
    c. The age and level of development of the minor/child must be taken into account.
    d. It is not permitted to use lengthy privacy policies that are difficult to understand or overloaded with legal terminology.
    e. The University is obliged to ensure that consent is given on the basis of information that enables the data subject to easily identify the person or entity responsible for data processing and understand what they are consenting to.
    f. The University is obliged to clearly describe the purpose of data collection for which consent is being requested.
    g. The University is obliged to develop a simple document to be used by minors/children and their parents or legal representatives. It is also essential that parents or legal representatives provide minors/children with complete information regarding the processing of their personal data.

6. The processing of special categories of personal data concerning a minor is permitted only on the basis of written consent from their parent or other legal representative, except in cases expressly provided for by law.

Article 11. Rights and Obligations of University Personnel

1. All University employees are required to adhere to the provisions of this Policy.
2. The University ensures that staff are informed, during the pre-contractual stage, about the types and scope of personal data the University will process about them.
3. Persons employed by the University are responsible for ensuring that documents and files containing personal data are not left unattended and must take all necessary measures to prevent the unauthorized disclosure of personal data.

4. University personnel are obliged not to disclose or transfer to third parties any personal data obtained in the course of performing their official duties. Persons employed by the University remain bound by the obligation to protect personal data even after their employment with the University has ended.
5. If individuals are no longer employed by the University and violate this Policy, they shall be held liable in accordance with applicable legislation.
6. Violation of the established regulations on personal data processing constitutes grounds for initiating disciplinary proceedings against university employees.

Chapter IV. Video and Audio Monitoring

Article 12. Conducting Video Surveillance on University Premises and Grounds

1. Video surveillance is conducted on university premises for the purposes of ensuring the safety of individuals, protecting University property, and monitoring examinations.
2. Video surveillance on university premises is conducted on a continuous basis, 24 hours a day, 7 days a week.
3. Video surveillance equipment is installed on university premises and is marked with appropriate informational signage. The coverage area of video surveillance equipment installed on university premises includes corridors, examination areas, parking facilities, and the University's internal and external courtyards.
4. Video recordings obtained from video surveillance equipment installed on university premises are retained for no longer than 40 (forty) days. Except in cases where, in accordance with the procedure established by law, a request from a competent authority requires the retention of the recording for a period longer than that specified in this paragraph.
5. Access to video recordings is permitted only to authorized personnel, such as the Head of the University's Security Office and designated staff responsible for video surveillance. Video recordings are accessed only for legitimate purposes, such as: ensuring security within the University, investigating potential incidents, fulfilling legal obligations, and/or other relevant legal grounds.
6. Video recordings may be accessed only by the Head of the Security Office or with their explicit authorization, in compliance with the principles of purpose limitation and necessity.
7. The video surveillance system and video recordings are protected against unauthorized access and use through appropriate technical measures. The person responsible for processing must ensure that each instance of access to video recordings is logged, including the time of access and the name of the user, in a manner that allows for the identification of the individual who accessed the recordings.
8. In the event that the person(s) authorized to access the video surveillance system are on official assignment, on leave, or no longer employed, the authority to access personal data is transferred to a designated substitute person(s), who assume the same rights and responsibilities.
9. For the purposes of special investigative measures and criminal investigations, the University may, upon request, transfer video recordings to the competent authorities only

on the basis of a court order or, in cases of urgent necessity, on the basis of a reasoned decision issued by a prosecutor.

10. Video recordings are stored in encrypted digital storage systems. Physical access to storage devices is restricted to authorized personnel only. Regular audits are conducted to ensure data integrity and security.
11. Data subjects (students, staff, visitors) have the right to be informed about the video surveillance practices, to access footage related to them, and, in accordance with the law and applicable circumstances, to request the rectification or erasure of their data.
12. The Security Office, with the assistance of the Information Technology Office, ensures the deletion and destruction of data upon the expiration of the retention period specified in paragraph 4 of this Article.

Article 13. Audio Monitoring of Calls Received via the University Hotline

1. To ensure service efficiency, the University operates a dedicated hotline, where incoming calls are monitored and recorded. These audio recordings are retained for a period of one (1) month.
2. The Information Technology Office ensures the deletion and destruction of data upon the expiration of the retention period specified in paragraph 10 of this Article.

Chapter V. Processing of Personal Data by the University's Structural and Support Units

Article 14. Processing of University Employees' Personal Data by the Human Resources Management Office of Ilia State University

1. The Human Resources Management Office of Ilia State University processes and stores personal data of university employees, including personnel files, for the purpose of entering into employment contracts with staff and ensuring effective human resources management. A personnel file of a university employee includes the following personal data: first name, last name, national identification number, address, and telephone number - this information is reflected in the following documents: Identification documents, official name change decree, bank account number, qualification certificate(s), employment contract, and various administrative orders.
2. The personnel files of Ilia State University employees are stored in physical form - on paper -and electronically, in the form of Excel documents and, partially, in the enterprise resource planning (ERP) system.
3. Personal data in paper form is securely stored in the office assigned to the University's Human Resources Management Office. Access to information in paper form is restricted to employees of the Human Resources Management Office.
4. The Human Resources Management Office ensures the security of personnel files stored in paper form and protects them from unauthorized access. To ensure the security of personnel files, a staffing arrangement is in place whereby at least one employee of the Human Resources Management Office is present in the room where the files are kept at all times. After working hours, the office door is locked, and access to the key is restricted to employees of the Human Resources Management Office, security staff, and cleaning staff.

During non-working hours, the room is secured by the Security Office of Ilia State University.

5. University employees' personal data and personal information are also stored in the form of Excel documents, access to which is granted only to employees of the Human Resources Management Office with the authorization of the head of the office or, in their absence, their acting replacement. The computer equipment used to store personal data in the form of Excel documents is protected by user credentials and passwords, access to which is limited to employees of the Human Resources Management Office.
6. At Ilia State University, personnel files of employees shall be retained for a period of 5 (five) years following the termination of the employment relationship and shall thereafter be transferred to the University archive.

Article 15. Storage and Processing of Student Personal Data by the Faculties of Ilia State University

1. The University maintains an archive that is used for the processing and long-term storage of personal data. The archive contains student personnel files, which include various categories of personal data, including information that allows for identification. These data are subject to retention for a period prescribed by law - 75 (seventy-five) years - in accordance with the regulations of the National Archives of Georgia.
2. In addition, the University also holds documents subject to permanent retention, which often contain personal data and relate to academic and administrative matters, as well as legal and employment relations. The storage and processing of personal data contained in these documents are carried out strictly for clearly defined purposes, based on the fundamental principles of both the Law of Georgia on Personal Data Protection and the European Union's General Data Protection Regulation (GDPR).
3. The University is authorized to retain personal data only for the period necessary, depending on the type of document, to achieve the intended purpose or to fulfill legal obligations. Data retention does not exceed clearly defined and lawful purposes and is based on the need for archiving, public interest, preservation of academic records, or the fulfillment of legal obligations.
4. The University implements appropriate technical and organizational measures to ensure the security, confidentiality, and integrity of data, and to prevent unauthorized access, destruction, or unlawful processing.

Article 16. Role of the University Information Technology (IT) Office in Personal Data Processing

1. The Information Technology (IT) Office of Ilia State University provides technical support for the electronic processing of personal data.
2. The IT Office must ensure the proper functioning of information systems in accordance with personal data protection standards. In addition, it must provide technical support to create an appropriate working environment for students and teachers with special needs.
3. This Policy defines the secure data storage policy, telecommunications policy, technical equipment configuration policy, visitor access and equipment usage policy, information sensitivity policy, password policy, personal identification policy, and other related policies.
4. Data are automatically backed up on a daily basis.

Article 17. Processing of Personal Data by the Quality Assurance Office

1. The Quality Assurance Office of Ilia State University processes personal data within the scope of its functional responsibilities. This activity includes access to and processing of personal data of students, graduates, academic staff, and invited lecturers for the purposes of quality monitoring and evaluation.
2. Data processing is carried out on a lawful basis, solely for specified and legitimate purposes, and in accordance with the legislation of Georgia and the applicable personal data protection regulations. All processing of personal data is based on the principles of data minimization, accuracy, and confidentiality, and is conducted in compliance with appropriate technical and organizational security measures.
3. Personal data processed by the Quality Assurance Office within the scope of university research is deleted and destroyed within 6 (six) months following the completion of the research report.

Chapter VI. Processing of Personal Data Through Electronic Systems

Article 18. Processing of Personal Data and Ensuring Information Security in Electronic Document Management Systems

1. For educational and instructional purposes, Ilia State University processes and stores student personal data in the electronic system for accounting tuition fees and tuition-derived revenues (Billing System) and in the electronic course selection and information system (Argus). The storage, processing, and other procedures involving personal data within these systems are defined by the relevant regulation.
2. At Ilia State University, correspondence containing personal data is registered and circulated through the automated document management system (e-doc). University staff have individual accounts in the system, protected by a designated username and password. The processing of personal data through this system is subject to the applicable personal data protection provisions, as established by this Policy and the relevant legislative and regulatory frameworks.
3. Ilia State University is composed of academic staff, researchers, instructors, and administrative-support personnel. University staff use their official (@iliauni.edu.ge) email accounts for work-related communication, in accordance with internal administrative procedures that help ensure efficient information exchange. - Each staff member's official email account is protected by a password accessible only to the account holder. University personnel are prohibited from disclosing their email password or leaving it unattended, including storing it on other devices (such as non-personal computers).

Chapter VII. Personal Data Breach

Article 19. Definition and Scope of a Personal Data Breach

1. A personal data breach is defined as any event that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that is transmitted, stored, or otherwise processed by the University.

2. All University employees, students, and third parties are required to immediately report any personal data breach to the Data Protection Officer.
3. A personal data breach may be reported via email, the hotline, or other available communication channels.
4. Upon receiving a personal data breach notification, the Data Protection Officer conducts an initial assessment to determine the nature and severity of the incident.

   4.1 The assessment of the incident includes the following components:
   a) Identification of the affected data subjects.
   b) Assessment of the type and volume of personal data involved.
   c) Assessment of the potential impact on data subjects.
   d) Identification of the cause of the incident.
   e) Identification of appropriate remedial measures.

   4.2 Where necessary, immediate measures shall be taken to contain the incident and mitigate potential harm to data subjects, including the following:
   a) Isolation of affected systems.
   b) Suspension of compromised accounts.
   c) Implementation of temporary security measures and other necessary actions.

   4.3 Records of personal data breaches at the University are retained for a minimum of 5 (five) years and are periodically reviewed to identify trends and improve the University's data protection practices.

   4.4 The University shall notify the competent supervisory authority of any personal data breach within 72 (seventy-two) hours.

   4.5 The notification to the supervisory authority shall include the following components:
   a) The nature of the personal data breach.
   b) The categories and approximate number of data subjects affected.
   c) The categories and approximate number of affected personal data records.
   d) The identity and contact information of the Data Protection Officer or another relevant individual.
   e) The anticipated consequences of the data breach.
   f) The measures undertaken and/or proposed to remedy the personal data breach.

   4.6 Lessons learned from personal data breaches shall be used to enhance the University's overall data protection strategy and its capacity to respond to future incidents.

   4.7 The University shall provide regular training sessions and awareness programs for employees and students on data protection and personal data breach response procedures.

Article 20. Obligation to Report a Personal Data Breach to the Data Protection Office

1. Ilia State University is obliged to document the incident, its consequences, and the measures taken, and to notify the Data Protection Office in writing or electronically within 72 (seventy-two) hours of discovering the incident, except in cases where it is unlikely to result in significant harm or pose a substantial risk to the fundamental rights and freedoms of individuals.
2. Other actions and legal procedures related to the incident shall be carried out in accordance with Article 29 of the Law of Georgia on Personal Data Protection.

Article 21. Criteria for Assessing the Severity of Fundamental Rights and Freedoms infringement

1. An incident shall be considered as causing significant harm to fundamental rights and freedoms if it results in, or is likely to result in, any of the following outcomes:
   a) Discrimination against the data subject (including identity theft or fraud, financial loss, damage to the data subject's reputation, breach of confidentiality of personal data protected by professional secrecy, or other forms of significant social and/or economic harm);
   b) Obstruction of the data subject's ability to exercise the rights granted under the Law of Georgia on Personal Data Protection, including limitation of the exercise of those rights within the timeframes prescribed by law;
   c) Deletion or destruction of personal data in such a manner that it cannot be recovered or its recovery would require disproportionate time and effort, except in cases where, considering the purpose of processing (excluding special categories of personal data), such deletion or destruction does not cause significant harm to the data subject;
   d) Unlawful disclosure of special categories of personal data;
   e) Physical harm, including limited access to medical services that results in the rescheduling of a medical procedure or operation, with a negative impact on the patient's treatment process;
   f) Unlawful processing of personal data belonging to minors, persons with disabilities, or other data subjects in need of special social or legal protection.
2. Following the assessment of the potential severity of the impact of the incident on the rights of data subjects, LEPL Ilia State University must determine the likelihood of such impact occurring.
3. The probability of the impact occurring may be assessed as low, medium, or high.

Chapter VIII. Data Protection Officer

Article 22. Role and Responsibilities of the Data Protection Officer

1. In order to oversee matters related to personal data protection - including the adoption and amendment of relevant regulatory provisions, informing the persons responsible for and authorized to process personal data, as well as their staff, and ensuring other actions prescribed by law - the University shall appoint a Data Protection Officer.
2. The Data Protection Officer is accountable to the Rector of the University and the Head of Administration.
3. The functions of the Data Protection Officer shall be defined as follows:
   a) Informing the University and its employees on matters related to data protection, including the adoption or amendment of the University's internal regulatory legal acts, and providing consultations and methodological assistance within the scope of the DPO's authority.
   b) Participation in the development of internal regulations related to data processing and in the preparation of data protection impact assessment documentation.
   c) Monitoring the University's compliance with Georgian legislation and internal organizational documents, including data recording, identification of data processing activities, and preparation of documentation (such as policy documents and others).

d) Reviewing statements and complaints related to data processing and issuing relevant recommendations.
e) Receiving consultations from the Personal Data Protection Office, representing the University in its communications with the Personal Data Protection Office, submitting information and documents upon its request, and coordinating and monitoring the implementation of its instructions and recommendations.
f) Providing the data subject, upon request, with information regarding data processing activities and their rights.
g) Notifying the Personal Data Protection Office of any data breach incident.
h) Performing other functions aimed at improving the University's data processing standards.

4. The University undertakes to ensure the appropriate involvement of the Data Protection Officer (DPO) in decision-making processes concerning data processing, to provide the DPO with adequate resources, and to guarantee their independence in the performance of their duties.

Chapter IX. Final provisions

Article 23. Final provisions

1. This Policy sets out the rules and procedures for the processing of personal data at the University. Any matter not covered by this Policy shall be resolved in accordance with the legislation of Georgia, including the Law of Georgia on Personal Data Protection and other regulations in force at the University.
2. This Policy shall be approved by the Rector of the University.
3. The annulment of this Policy, as well as any amendments or additions thereto, shall be carried out in accordance with the relevant regulations in force at the University.
4. This Policy shall come into force on the date it is approved.