



DATA PROTECTION & PRIVACY POLICY

Policy Title	Data Protection & Privacy Policy
Policy Owner	Office of the Rector / IT Governance
Approved By	University Senate
Version	1.0
Date Approved	May 2025
Next Review Date	May 2027
Applicable Legislation	Law of the Republic of Uzbekistan 'On Personal Data' No. ZRU-547 (2019); Law 'On Informatization' No. ZRU-611 (2021)
GreenMetric Indicator	GD.3 — Existence of University Data Protection Policy

1. Introduction

Central Asian University (CAU) is committed to protecting the privacy and personal data of all individuals who interact with the University — including students, academic and administrative staff, researchers, alumni, partners, and visitors. This Policy establishes the University's framework for the responsible collection, processing, storage, and security of personal data in accordance with applicable Uzbek legislation and international best-practice standards.

This Policy applies to all personal data processed in any format — electronic, paper, or otherwise — across all University campuses, units, and digital systems. Compliance may be demonstrated through alignment with the Law of the Republic of Uzbekistan 'On Personal Data' (No. ZRU-547, 2019) and equivalent institutional practices informed by internationally recognised data-protection principles.

2. Purpose and Scope

2.1 Purpose

This Policy:

- Affirms CAU's commitment to protecting the privacy rights of all data subjects;
- Establishes clear responsibilities for everyone who handles personal data on behalf of the University;
- Ensures compliance with Uzbek data-protection legislation and alignment with internationally recognised principles, including those of the EU General Data Protection Regulation (GDPR) where applicable;
- Supports CAU's submission to the UI GreenMetric World University Rankings under the Governance and Digitalization category (Indicator GD.3).

2.2 Scope

This Policy applies to:

- All employees, faculty, and administrative staff of CAU;
- All students enrolled in programmes offered by CAU;
- Contractors, vendors, and third-party service providers who process personal data on behalf of CAU;
- Visiting researchers, placement students, and volunteers;
- Members of governing and advisory bodies acting in their official capacities.

It covers all personal data held or transmitted in any medium, including but not limited to university information systems, learning management platforms, HR databases, financial records, CCTV systems, and communication tools.

3. Legal and Regulatory Framework

CAU processes personal data in accordance with the following legal instruments:

- Law of the Republic of Uzbekistan 'On Personal Data' (No. ZRU-547, 2019) — the primary national legislation governing collection, processing, storage, and protection of personal data in Uzbekistan;
 - Law 'On Informatization' (No. ZRU-611, 2021) — regulating information systems and digital governance;
 - Resolution of the Cabinet of Ministers No. 200 (2021) — technical requirements for personal data information systems;
 - CAU Charter and internal governance regulations.
-

Where Uzbek national legislation does not provide specific guidance, CAU draws on internationally recognised principles — in particular those of the EU GDPR — as supplementary best-practice reference points, provided this does not conflict with Uzbek law. This approach ensures that compliance is demonstrated through alignment with equivalent national data-protection regulations and institutional practices.

4. Key Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable individual, including names, identification numbers, location data, biometric data, and any combination of data enabling identification.
Sensitive Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, health data, biometric or genetic data, or data concerning a person's private life.
Data Subject	A living individual to whom personal data relates.
Data Controller	CAU, as the entity that determines the purposes and means of processing personal data.
Data Processor	Any internal unit or external party that processes personal data on behalf of CAU under a formal agreement.
Processing	Any operation performed on personal data, including collection, recording, storage, retrieval, use, disclosure, deletion, or destruction.
Consent	Freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of their personal data.

5. Data Protection Principles

CAU is committed to processing personal data in accordance with the following core principles, which reflect both Uzbek legislative requirements and internationally recognised standards:

Principle	Requirement
Lawfulness, Fairness & Transparency	Personal data shall be collected and processed on a lawful basis, in a manner that is fair and transparent to the data subject.
Purpose Limitation	Data shall be collected for specified, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes.
Data Minimisation	Only data that is adequate, relevant, and limited to what is necessary for the stated purpose shall be collected and retained.
Accuracy	Personal data shall be kept accurate and, where necessary, up to date. Inaccurate data shall be corrected or deleted without undue delay.
Storage Limitation	Personal data shall not be retained longer than necessary for the purposes for which it was collected, in accordance with CAU's Records Retention Schedule.
Integrity & Confidentiality	Appropriate technical and organisational measures shall be applied to protect personal data against unauthorised access, loss, destruction, or disclosure.
Accountability	CAU shall be responsible for, and able to demonstrate, compliance with all of the above principles.

6. Lawful Basis for Processing

CAU shall establish a lawful basis before processing any personal data. Lawful bases include:

- Consent: the data subject has freely given, specific, and informed consent;
- Contractual necessity: processing is required to fulfil a contract with the data subject (e.g., student enrolment, employment contract);
- Legal obligation: processing is required by Uzbek law or regulatory authority;
- Legitimate interests: processing is necessary for CAU's legitimate educational, research, or institutional purposes, where these interests are not overridden by the rights of the data subject;
- Vital interests: processing is necessary to protect the life of the data subject or another person;
- Public task: processing is required for the performance of a task carried out in the public interest or in exercise of official authority.

CAU shall document the lawful basis for each category of processing activity in its Register of Processing Activities (RPA).

7. Rights of Data Subjects

In accordance with Article 8 of the Law 'On Personal Data' (No. ZRU-547, 2019), all data subjects have the right to:

- Be informed about whether their personal data is being processed and for what purpose;
 - Access a copy of their personal data held by CAU;
 - Request correction of inaccurate or incomplete personal data;
-

-
- Request deletion of personal data where there is no longer a lawful basis for processing;
 - Withdraw consent at any time where consent is the lawful basis for processing;
 - Object to processing on grounds relating to their particular situation;
 - Lodge a complaint with the authorised state body for personal data protection in Uzbekistan.

Requests shall be submitted to the CAU Data Protection Officer (DPO) and responded to within 30 calendar days. CAU reserves the right to extend this period by a further 30 days where requests are complex or numerous, with notification to the data subject.

8. Data Security

8.1 Technical Measures

CAU shall implement the following technical safeguards:

- Role-based access controls and multi-factor authentication for all university information systems;
- Encryption of personal data at rest and in transit;
- Regular vulnerability assessments and penetration testing of university digital infrastructure;
- Automated system logging and audit trails;
- Secure backup and disaster-recovery procedures in compliance with Cabinet of Ministers Resolution No. 200 (2021).

8.2 Organisational Measures

CAU shall maintain the following organisational safeguards:

- Annual mandatory data-protection training for all staff and relevant student groups;
- Data Protection Impact Assessments (DPIAs) for high-risk processing activities;
- Formal data-processing agreements with all third-party processors;
- A clearly defined process for reporting, investigating, and notifying data security incidents.

8.3 Data Breach Response

In the event of a data security breach, CAU shall:

- Contain the breach and assess its scope within 24 hours of discovery;
- Notify the relevant state authority within 72 hours where the breach is likely to result in risk to the rights and freedoms of data subjects;
- Inform affected data subjects without undue delay where there is a high risk to their rights;
- Document all breaches in the University's Breach Register, including corrective actions taken.

9. Roles and Responsibilities

9.1 University Rector

Holds overall accountability for compliance with this Policy and ensures adequate resources are allocated for data protection.

9.2 Data Protection Officer (DPO)

The DPO is responsible for:

- Advising the University on data-protection obligations and best practice;
- Monitoring compliance with this Policy and applicable legislation;
- Serving as the primary point of contact for data subjects and regulatory authorities;
- Maintaining the Register of Processing Activities (RPA);
- Conducting and overseeing DPIAs;
- Coordinating the University's response to data-subject rights requests and security incidents.

9.3 Heads of Department / Dean's Offices

Responsible for implementing this Policy within their respective units, nominating Data Protection Coordinators, and ensuring staff complete required training.

9.4 All Staff and Students

All members of the University community are required to:

- Familiarise themselves with and comply with this Policy;
- Handle personal data only as necessary for their legitimate duties;
- Report any actual or suspected data security incidents to the DPO immediately;
- Participate in mandatory data-protection training.

10. Special Categories of Personal Data

Sensitive personal data — including health data, biometric data, racial or ethnic origin, religious beliefs, and political opinions — shall be processed only where:

- The data subject has given explicit written consent;
- Processing is required by law, for the establishment, exercise, or defence of legal claims;
- or
- Processing is necessary for legitimate academic research under appropriate safeguards and in accordance with a research ethics approval.

Additional controls, including restricted access, enhanced encryption, and mandatory DPIA, shall apply to all processing of sensitive personal data.

11. Third-Party Processors and Data Transfers

11.1 Third-Party Processors

CAU may engage external service providers to process personal data on its behalf (e.g., cloud-hosting providers, learning management system vendors, payroll processors). In all such cases, CAU shall:

- Ensure that a formal Data Processing Agreement (DPA) is in place before any personal data is shared;
- Conduct a due-diligence assessment of the processor's data-protection practices;
- Retain responsibility as Data Controller for the lawfulness of the processing.

11.2 Cross-Border Data Transfers

Transfer of personal data outside the Republic of Uzbekistan shall be permitted only where:

- The receiving country provides an adequate level of data protection as determined by Uzbek authorities; or
-

-
- Appropriate safeguards are in place (e.g., contractual clauses, binding corporate rules); or
 - The data subject has given explicit informed consent to the transfer.

The DPO shall be consulted before any cross-border transfer of personal data is initiated.

12. Data Retention

Personal data shall be retained only for as long as necessary to fulfil the purpose for which it was collected, or as required by applicable Uzbek law. CAU maintains a Records Retention Schedule that specifies retention periods for each category of data. Upon expiry of the retention period, data shall be securely deleted or anonymised.

13. Training and Awareness

CAU shall provide mandatory annual data-protection training to all staff and relevant student cohorts. Training records shall be maintained by the Human Resources Department. Additional targeted training shall be provided to staff in roles involving significant personal data processing (e.g., HR, Finance, IT, Registry).

14. Policy Review and Approval

This Policy shall be reviewed every two years, or earlier in response to significant changes in applicable legislation, technology, or the University's data-processing activities. Amendments require approval by the University Senate and shall be published on the CAU website at centralasian.uz/sustainability and centralasian.uz/sdg.

15. Contact Information

For questions, data-subject requests, or to report a data security incident, please contact:

Data Protection Officer Central Asian University 100070, Tashkent, Milliy Bog Street 264, Uzbekistan Email: dpo@centralasian.uz Website: centralasian.uz

Appendix A: Alignment with UI GreenMetric GD.3 Requirements

This Policy is submitted as evidence for UI GreenMetric World University Rankings, Category 7: Governance and Digitalization, Indicator GD.3 (Existence of University Data Protection Policy).

The Policy satisfies GD.3 compliance requirements as follows:

GreenMetric / GDPR Requirement	CAU Policy Reference / National Equivalent
Formal institutional data protection policy	This document — approved by University Senate, May 2025 (Section 14)
Defined lawful basis for processing	Section 6; aligned with ZRU-547 Art. 6–7
Data subject rights	Section 7; aligned with ZRU-547 Art. 8
Security measures (technical & organisational)	Section 8; aligned with Cabinet Resolution No. 200 (2021)
Data breach response procedure	Section 8.3
Designated Data Protection Officer	Section 9.2
Third-party processor controls	Section 11.1
Cross-border transfer restrictions	Section 11.2; aligned with ZRU-547 Art. 19
Retention and disposal procedures	Section 12
Training and awareness programme	Section 13
Policy review mechanism	Section 14 — biennial review by University Senate

Compliance with this Policy is demonstrated through alignment with the Law of the Republic of Uzbekistan 'On Personal Data' (ZRU-547, 2019) and equivalent institutional practices. CAU acknowledges that while the national framework differs in structure from EU GDPR, the substantive protections afforded to data subjects — including principles of purpose limitation, data minimisation, accuracy, storage limitation, security, and data subject rights — are equivalent in effect and satisfy the governance standards assessed under the GreenMetric ranking methodology.

Approved by:

Rector, Central Asian University

Date: _____