UNEC
1930

AZERBAIJAN STATE UNIVERSITY OF ECONOMICS (UNEC)

GENERAL DATA PROTECTI ON POLICY

Azerbaijan State University of Economics (UNEC)

Table of Contents

1. Purpose ... **3**
2. Scope ... **3**
3. Definitions ... **4**
4. Data Protection Principles ... **4**
4.1 Lawfulness, Fairness and Transparency ... 4
4.2 Purpose Limitation ... 4
4.3 Data Minimization ... 4
4.4 Accuracy ... 4
4.5 Storage Limitation ... 4
4.6 Integrity and Confidentiality ... 4
4.7 Accountability ... 4
5. Categories of Personal Data ... **5**
6. Lawful Basis for Processing Personal Data ... **5**
7. Rights of Data Subjects ... **6**
8. Data Security and Protection Measures ... **6**
9. Data Sharing and Third-Party Processing ... **6**
10. International Data Transfers ... **7**
11. Data Retention and Disposal ... **7**
12. Data Breach Management ... **7**
13. Governance and Responsibilities ... **7**
13.1 University Leadership ... 7
13.2 Information Technology Services ... 8
13.3 Academic and Administrative Units ... 8
13.4 Faculty, Staff and Students ... 8
14. Training and Awareness ... **8**
15. Monitoring and Compliance ... **8**
16. Policy Review ... **9**

1. Purpose

The Azerbaijan State University of Economics (UNEC) recognizes the importance of protecting personal data and ensuring the privacy rights of all individuals whose information is processed by the University.

The purpose of this Policy is to establish a comprehensive framework for the collection, processing, storage, use, sharing, retention, and protection of personal data in accordance with applicable legislation, international best practices, institutional governance requirements, and ethical standards.

This Policy supports UNEC's commitment to transparency, accountability, information security, digital transformation, and responsible data management.

2. Scope

This Policy applies to:

- Students;
- Academic staff;
- Administrative staff;
- Researchers;
- Alumni;
- Applicants;
- Contractors;
- Service providers;
- Visitors;
- External partners;
- Any individual whose personal data is processed by UNEC.

The Policy applies to all personal data processed through:

- Digital systems;
- University websites;
- Learning management systems;
- Research activities;
- Administrative processes;
- Human resource systems;

- Financial systems;
- Physical records;
- Cloud services;
- Third-party platforms utilized by UNEC.

3. Definitions

For the purpose of this Policy:

Personal Data means any information relating to an identified or identifiable individual.

Processing means any operation performed on personal data including collection, storage, organization, use, disclosure, transfer, deletion, or destruction.

Data Subject means the individual to whom the personal data relates.

Data Controller means UNEC as the institution determining the purposes and means of processing personal data.

Data Processor means any third-party processing personal data on behalf of UNEC.

4. Data Protection Principles

UNEC shall process personal data according to the following principles.

4.1 Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly, and transparently.

4.2 Purpose Limitation

Personal data shall be collected for specified, explicit, and legitimate purposes.

4.3 Data Minimization

Only personal data necessary for the intended purpose shall be collected and processed.

4.4 Accuracy

UNEC shall take reasonable steps to ensure personal data remains accurate and up to date.

4.5 Storage Limitation

Personal data shall not be retained longer than necessary.

4.6 Integrity and Confidentiality

Appropriate technical and organizational measures shall be implemented to protect personal data.

4.7 Accountability

UNEC shall demonstrate compliance with all applicable data protection obligations.

5. Categories of Personal Data

UNEC may process:

- Identification information;
- Contact details;
- Academic records;
- Employment information;
- Financial information;
- Research participation information;
- Digital activity records;
- System access logs;
- Audio and visual recordings;
- Library usage records;
- Campus access information.

Special categories of personal data shall be processed only where legally permitted and appropriately safeguarded.

6. Lawful Basis for Processing Personal Data

UNEC may process personal data where necessary for:

- Performance of educational services;
- Employment administration;
- Legal obligations;
- Public interest tasks;
- Research activities;
- Protection of vital interests;
- Legitimate institutional interests;
- Consent of the data subject where required.

7. Rights of Data Subjects

Individuals may exercise the following rights:

- Right to be informed;
- Right of access;
- Right to rectification;
- Right to erasure where applicable;
- Right to restrict processing;
- Right to data portability where applicable;
- Right to object to processing;
- Rights related to automated decision-making.

UNEC shall establish procedures to respond to such requests within reasonable timeframes.

8. Data Security and Protection Measures

UNEC shall implement appropriate safeguards including:

- Access controls;
- User authentication;
- Encryption technologies;
- Secure backups;
- Network security controls;
- Cybersecurity monitoring;
- Incident management procedures;
- Physical security measures.

Information systems shall be protected against unauthorized access, alteration, disclosure, loss, or destruction.

9. Data Sharing and Third-Party Processing

Personal data may be shared only where:

- Legally required;
- Necessary for educational or administrative purposes;

- Supported by contractual safeguards;
- Approved through institutional procedures.

Third-party service providers shall be required to maintain adequate data protection standards.

10. International Data Transfers

Where personal data is transferred internationally, UNEC shall ensure that appropriate safeguards are implemented to protect the rights and freedoms of data subjects.

11. Data Retention and Disposal

Personal data shall be retained according to applicable legal, regulatory, academic, and operational requirements.

When retention periods expire, data shall be securely deleted, anonymized, or destroyed.

12. Data Breach Management

UNEC shall maintain procedures for:

- Detection of data breaches;
- Incident reporting;
- Risk assessment;
- Containment and mitigation;
- Notifications where required;
- Corrective actions.

All personnel shall promptly report suspected or actual data breaches.

13. Governance and Responsibilities

13.1 University Leadership

University leadership shall:

- Approve and oversee this Policy;
- Support compliance initiatives;
- Allocate necessary resources.

13.2 Information Technology Services

Responsible IT units shall:

- Maintain secure infrastructure;
- Implement cybersecurity controls;
- Monitor security risks.

13.3 Academic and Administrative Units

Units shall:

- Process personal data responsibly;
- Maintain compliance with this Policy;
- Support data protection requirements.

13.4 Faculty, Staff and Students

All members of the University community shall:

- Protect personal data;
- Follow security procedures;
- Report incidents and risks.

14. Training and Awareness

UNEC shall provide regular training and awareness programs covering:

- Data protection principles;
- Information security;
- Privacy obligations;
- Cybersecurity awareness;
- Responsible data handling practices.

15. Monitoring and Compliance

UNEC shall periodically assess compliance through:

- Internal reviews;
- Risk assessments;
- Security audits;

- Policy monitoring activities.

Corrective measures shall be implemented where necessary.

16. Policy Review

This Policy shall be reviewed periodically to ensure alignment with:

- Legislative developments;
- International best practices;
- Institutional priorities;
- Technological changes;
- Information security requirements.

UNEC remains committed to protecting personal data and maintaining the highest standards of privacy, security, accountability, and responsible information governance.