[BAKU EURASIAN UNIVERSITY]

It was discussed and approved at
the meeting of Scientific Council at
Baku Eurasian University on 01.05.2026

DATA PROTECTION POLICY

Compliance with the General Data Protection Regulation (GDPR)

1. Introduction and Purpose

Baku Eurasian University ("the University") collects, holds, and processes personal data relating to staff, students, applicants, alumni, research participants, visitors, and other individuals in order to carry out its teaching, research, administrative, and statutory functions.

The University recognises that the correct and lawful treatment of personal data maintains confidence in the University and provides for successful working relationships with staff, students, and other stakeholders. The protection of personal data is an integral part of the University's operations.

This Policy sets out the framework by which the University ensures full compliance with Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR"), and any applicable national legislation implementing or supplementing the GDPR (together, "Data Protection Legislation").

The purpose of this Policy is to:

- Ensure the University processes personal data lawfully, fairly, and transparently, and in a manner that respects the rights of individuals;
- Establish clear roles, responsibilities, and accountability for data protection across the University;
- Set minimum standards for the collection, storage, use, sharing, retention, and disposal of personal data;
- Protect the University and its staff and students from the risks associated with a breach of Data Protection Legislation, including regulatory sanctions, reputational damage, and loss of stakeholder trust;
- Provide a framework for responding to data subject rights requests and personal data breaches.

2. Scope

This Policy applies to all personal data processed by or on behalf of the University, regardless of the format in which it is held (electronic, paper-based, audio-visual, or other) and regardless of where the processing takes place.

This Policy applies to:

- All staff (academic, administrative, technical, and support), whether permanent, fixed-term, casual, or on a consultancy basis;
- All students, including applicants, current students, and alumni;
- Members of the University Council, Senate, Board of Governors, and other governance bodies;
- Contractors, agency workers, placement and exchange students, visiting researchers, and honorary staff;
- Third-party organisations and data processors acting on the University's behalf;
- Any individual or system that accesses, processes, or stores personal data held by the University.

This Policy does not form part of any employee's contract of employment and may be amended by the University at any time.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, or data concerning a person's sex life or sexual orientation.
Processing	Any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, dissemination, restriction, erasure, or destruction.
Data Controller	The University, which determines the purposes and means of processing personal data.
Data Processor	A third party that processes personal data on behalf of, and under the instruction of, the University.
Data Subject	An identified or identifiable living individual to whom personal data relates.
Consent	A freely given, specific, informed, and unambiguous indication of a data subject's wishes by which they signify agreement to the processing of personal data relating to them.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Term	Definition
Data Protection Officer (DPO)	The individual formally designated by the University to oversee compliance with Data Protection Legislation and act as the primary point of contact with supervisory authorities and data subjects.
Supervisory Authority	The independent public authority responsible for monitoring the application of Data Protection Legislation within the relevant jurisdiction.
Third Country	A country outside the European Economic Area (EEA) that has not been deemed to provide an adequate level of data protection.

4. Data Protection Principles

In accordance with Article 5 of the GDPR, the University commits to ensuring that personal data is:

Principle	Requirement
Lawfulness, Fairness, and Transparency	Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
Purpose Limitation	Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
Data Minimisation	Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
Accuracy	Accurate and, where necessary, kept up to date; every reasonable step is taken to ensure inaccurate personal data is erased or rectified without delay.
Storage Limitation	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.
Integrity and Confidentiality	Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
Accountability	The University is responsible for, and must be able to demonstrate compliance with, the above principles.

5. Lawful Basis for Processing

The University will only process personal data where at least one lawful basis under Article 6 of the GDPR applies. These lawful bases are:

- Consent: the data subject has given clear, freely given consent for a specific purpose;

- Contract: processing is necessary for the performance of a contract with the data subject, or to enter into a contract;
- Legal Obligation: processing is necessary for the University to comply with a legal obligation;
- Vital Interests: processing is necessary to protect someone's life;
- Public Task: processing is necessary for the University to perform a task in the public interest or for its official functions, including teaching, research, and administration;
- Legitimate Interests: processing is necessary for the legitimate interests of the University or a third party, unless outweighed by the interests or fundamental rights of the data subject.

Where Special Category Data is processed, an additional condition under Article 9 GDPR must also be satisfied (for example, explicit consent, employment/social security obligations, substantial public interest, or processing for archiving, research, or statistical purposes subject to appropriate safeguards).

Schools, Departments, and Professional Services are responsible for identifying and documenting the applicable lawful basis (and, where relevant, the Article 9 condition) for each processing activity within their Record of Processing Activities (ROPA), with support from the Data Protection Office.

6. Roles and Responsibilities

Compliance with Data Protection Legislation is the responsibility of every individual who processes personal data on behalf of the University. Specific responsibilities are set out below.

6.1 University Council / Board of Governors

Holds ultimate responsibility for ensuring the University meets its legal obligations under Data Protection Legislation and for approving this Policy.

6.2 Data Protection Officer (DPO)

- Monitoring compliance with this Policy and Data Protection Legislation;
- Acting as the principal point of contact for data subjects and the relevant Supervisory Authority;
- Advising on, and monitoring the performance of, Data Protection Impact Assessments (DPIAs);
- Maintaining the University's Record of Processing Activities (ROPA);
- Investigating and coordinating the response to personal data breaches;
- Providing advice and training on data protection matters to staff and students;
- Reporting to the most senior level of management on data protection performance.

6.3 Heads of School / Department and Senior Managers

- Ensuring that data protection requirements are embedded within their area's policies, procedures, and working practices;
- Identifying and recording processing activities carried out within their area for the ROPA;
- Ensuring staff within their area complete mandatory data protection training;
- Escalating data protection risks, queries, and suspected breaches to the Data Protection Office without delay.

6.4 All Staff, Researchers, and Contractors

- Processing personal data only for legitimate University purposes and in accordance with this Policy;
- Completing mandatory data protection training and keeping their knowledge up to date;
- Keeping personal data secure and reporting any actual or suspected personal data breach immediately to the Data Protection Office;
- Only accessing personal data that they are authorised to access and that is necessary for their role;
- Referring any data subject rights request received to the Data Protection Office without delay.

6.5 Students

- Complying with this Policy and any related guidance when handling personal data of other students, staff, or third parties (for example, during group work, placements, or research projects);
- Exercising their own data subject rights through the procedures set out in this Policy.

6.6 IT Services

- Implementing and maintaining appropriate technical security measures to protect personal data;
- Supporting the secure configuration of University systems, including access controls, encryption, and backups;
- Supporting the investigation of personal data breaches involving IT systems.

7. Rights of Data Subjects

The University will uphold the rights of data subjects under Data Protection Legislation. These rights are:

Right	Description
Right to be Informed	To be told how their personal data is used, through privacy notices.
Right of Access	To request a copy of the personal data the University holds about them (a “Subject Access Request”).
Right to Rectification	To request that inaccurate or incomplete personal data be corrected.
Right to Erasure	To request deletion of personal data, in certain circumstances (the “right to be forgotten”).
Right to Restrict Processing	To request that the University limit the way it uses their personal data, in certain circumstances.
Right to Data Portability	To request their personal data be provided in a structured, commonly used, machine-readable format, and transmitted to another controller, where applicable.
Right to Object	To object to processing based on legitimate interests, public task, or for direct marketing purposes.

Right	Description
Rights Related to Automated Decision-Making and Profiling	To not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects, subject to limited exceptions.

Requests to exercise any of these rights should be submitted to the Data Protection Office. The University will respond within one calendar month of receipt of a valid request, extendable by a further two months for complex or numerous requests, in accordance with Article 12 GDPR. The University does not normally charge a fee for handling such requests.

8. Categories of Personal Data and Processing Activities

The University processes personal data in connection with a range of activities, including but not limited to those set out below. A full inventory of processing activities is maintained in the University's Record of Processing Activities (ROPA).

Data Subject Category	Examples of Processing Activities
Applicants and Students	Admissions, enrolment, registration, examinations, assessment, academic records, disability and welfare support, accommodation, financial support, disciplinary matters, careers services, alumni relations.
Staff and Job Applicants	Recruitment and selection, contracts of employment, payroll and pensions, performance management, sickness and absence records, training records, disciplinary and grievance matters.
Research Participants	Personal data collected in the course of academic research, including, where applicable, Special Category Data such as health information, subject to ethical approval and appropriate safeguards.
Visitors and Contractors	Building access records, CCTV footage, visitor sign-in records, contractor personnel data.
Website and Online Services Users	Cookies, IP addresses, account credentials, and usage data collected through University websites, portals, and virtual learning environments.

9. Consent

Where consent is relied upon as the lawful basis for processing, the University will ensure that consent is freely given, specific, informed, and unambiguous, and is given through a clear affirmative action.

- Requests for consent must be presented separately from other matters and in plain, clear language;
- Records must be kept of what the data subject was told, when, and how they consented;
- Data subjects must be able to withdraw consent at any time, as easily as it was given;
- Consent will not be considered freely given where there is a clear imbalance of power between the University and the data subject (for example, where a student's academic standing could be

affected by a refusal to consent), and an alternative lawful basis should be considered in such circumstances.

10. Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) must be carried out prior to undertaking any processing activity that is likely to result in a high risk to the rights and freedoms of individuals, including (but not limited to):

- Systematic and extensive evaluation of personal aspects, including profiling, with significant effects on individuals;
- Large-scale processing of Special Category Data;
- Systematic monitoring of a publicly accessible area on a large scale (e.g. extensive CCTV deployment);
- Use of new technologies that involve novel forms of data collection or processing (e.g. biometric identification, AI-based decision-making);
- Large-scale processing of student, staff, or research participant data combining datasets from multiple sources.

The Data Protection Office must be consulted at the earliest planning stage of any new project, system, or process involving personal data to determine whether a DPIA is required. Where a DPIA identifies a high risk that cannot be sufficiently mitigated, the matter must be referred to the relevant Supervisory Authority for prior consultation before processing begins.

11. Privacy by Design and by Default

The University will implement appropriate technical and organisational measures to ensure data protection principles are embedded into new systems, processes, products, and services from the outset ("privacy by design"), and that, by default, only personal data necessary for each specific purpose is processed ("privacy by default").

This includes, where appropriate: data minimisation, pseudonymisation or anonymisation, restricting access on a need-to-know basis, and building in mechanisms to support data subject rights from the design stage of any new system or process.

12. Data Sharing and Third-Party Data Processors

Where the University engages a third party to process personal data on its behalf (a "Data Processor"), it will ensure that:

- A written data processing agreement is in place, containing the minimum terms required by Article 28 GDPR, prior to any data being shared;
- The Data Processor provides sufficient guarantees to implement appropriate technical and organisational measures;

- Due diligence is conducted on the Data Processor's data protection practices before the contract is entered into;
- Sub-processing is only permitted with the University's prior written authorisation;
- The Data Processor assists the University in complying with data subject rights requests and personal data breach obligations.

Where personal data is shared with another data controller (for example, a partner institution, regulatory body, or funding agency), an appropriate data sharing agreement or memorandum of understanding will be put in place, setting out the purpose, scope, and safeguards applicable to the sharing arrangement.

All proposed new data processing or data sharing arrangements must be reviewed and approved by the Data Protection Office before being implemented.

13. International Data Transfers

Personal data will only be transferred outside the European Economic Area (EEA), or to an international organisation, where an appropriate safeguard under Chapter V of the GDPR is in place, such as:

- An adequacy decision by the European Commission in respect of the recipient country;
- Standard Contractual Clauses (SCCs) approved by the European Commission;
- Binding Corporate Rules, where applicable;
- An approved code of conduct or certification mechanism;
- A derogation under Article 49 GDPR, applied only in limited and exceptional circumstances.

All international transfers of personal data, including those arising from international research collaborations, cloud-based services, or the use of overseas conference and travel platforms, must be approved in advance by the Data Protection Office, including a Transfer Impact Assessment (TIA) where required.

14. Data Retention and Disposal

Personal data will not be kept for longer than is necessary for the purpose(s) for which it was collected. The University maintains a Records Retention Schedule setting out retention periods for the principal categories of records held, having regard to:

- Statutory and regulatory retention requirements;
- Limitation periods for legal claims;
- Funder and contractual requirements (particularly for research data);
- Academic and administrative necessity;
- Guidance issued by relevant sector and professional bodies.

At the end of the applicable retention period, personal data will be securely and irrecoverably destroyed or permanently and irreversibly anonymised. Disposal of physical records will be by confidential, secure shredding or destruction; electronic records will be deleted in accordance with IT Services' secure disposal procedures.

15. Data Security — Technical and Organisational Measures

The University will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate:

15.1 Technical Measures

- Encryption of personal data at rest and in transit, in particular for Special Category Data and data held on portable devices;
- Role-based access controls and the principle of least privilege;
- Multi-factor authentication for access to systems holding personal data;
- Firewalls, anti-malware software, and intrusion detection and prevention systems;
- Secure configuration management and timely application of security patches;
- Regular, tested data backups with secure offsite or cloud storage;
- Pseudonymisation or anonymisation of data, where feasible, for research and statistical purposes.

15.2 Organisational Measures

- Mandatory data protection and information security training for all staff;
- Clear desk and clear screen practices, and secure storage of physical records;
- Confidentiality clauses in contracts of employment and with third-party processors;
- Restriction of access to personal data on a need-to-know basis;
- Regular review and audit of access permissions and data protection practices;
- An Acceptable Use Policy governing the use of University IT systems and devices.

16. Personal Data Breach Management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All actual or suspected personal data breaches must be reported immediately upon discovery.

16.1 Reporting

Any member of staff, student, or contractor who becomes aware of an actual or suspected personal data breach must report it to the Data Protection Office without delay, and in any event within 24 hours of discovery, using the University's Data Breach Report Form.

16.2 Assessment and Notification Timelines

Stage	Action / Timeline
Discovery of breach	Immediate internal report to the Data Protection Office

Stage	Action / Timeline
Within 72 hours of becoming aware	Notification to the relevant Supervisory Authority, where the breach is likely to result in a risk to the rights and freedoms of individuals
Without undue delay	Notification to affected data subjects, where the breach is likely to result in a high risk to their rights and freedoms

16.3 Investigation

The Data Protection Office will lead the investigation of any reported breach, in conjunction with IT Services and other relevant departments as necessary, to establish the cause, scope, and impact of the breach, and to identify remedial and preventative actions. A central log of all personal data breaches, including those not requiring notification to the Supervisory Authority, will be maintained.

17. Subject Access Request (SAR) Procedure

A Subject Access Request may be made verbally or in writing, by the data subject or an authorised third party (such as a solicitor), and should be directed to the Data Protection Office.

- The identity of the requester will be verified before any personal data is disclosed;
- The University will respond within one calendar month of receipt of the request, extendable by up to two further months for complex or numerous requests, with the data subject informed of any extension and the reasons for it within one month;
- Where the request is manifestly unfounded or excessive, the University may charge a reasonable fee or refuse to act on the request, having regard to applicable guidance;
- Information will be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

18. CCTV, Biometric Data, and Physical Security

Where the University operates CCTV systems or biometric access control systems (e.g. fingerprint or facial recognition for building access), it will ensure that:

- Signage clearly informs individuals that CCTV is in operation and provides contact details for further information;
- Access to CCTV footage and biometric data is restricted to authorised personnel only;
- Footage and biometric data are retained only for as long as necessary and in line with the Records Retention Schedule;
- A DPIA is conducted prior to the deployment of any new or extended CCTV or biometric system.

19. Research Data and Academic Records

Research involving personal data, including human participant research, must be reviewed and approved by the relevant Research Ethics Committee prior to commencement, and must comply with this Policy and any applicable research data management requirements.

- Personal data collected for research purposes will be pseudonymised or anonymised wherever this is consistent with the research aims;
- Special Category Data processed for research purposes will only be processed where an appropriate Article 9 condition and additional safeguards (as required by national legislation) are in place;
- Researchers must complete a DPIA where research processing is likely to result in high risk, particularly where Special Category Data, vulnerable participants, or large-scale data linkage is involved;
- Personal data used for research should not be retained for longer than necessary and should be managed in accordance with funder and institutional data management plans.

20. Marketing, Recruitment, and Alumni Communications

Where the University processes personal data for marketing, student recruitment, or alumni and development communications, it will:

- Rely on an appropriate lawful basis, generally consent or legitimate interests, and apply additional consent requirements under applicable e-privacy/electronic communications legislation for electronic marketing;
- Provide a clear and simple means for individuals to opt out of, or object to, direct marketing communications at any time, free of charge;
- Maintain suppression lists to ensure individuals who have opted out are not subsequently contacted for marketing purposes.

21. Use of Cloud Services and Third-Party IT Systems

Staff and students must not use personal cloud storage accounts, unauthorised software-as-a-service tools, or personal devices to store or process University personal data unless the service or device has been approved by IT Services and, where appropriate, subject to a data processing agreement and security review. Procurement of any new IT system or service that will process personal data must involve the Data Protection Office at the earliest stage.

22. Training and Awareness

All staff, including governors and contractors with access to personal data, must complete mandatory data protection training upon induction and on a periodic basis thereafter (at least annually), as determined by the Data Protection Office. Staff in roles with significant data protection responsibilities (e.g. those handling Special Category Data or managing large datasets) will be required to undertake additional, role-specific training.

23. Monitoring, Audit, and Compliance Review

The Data Protection Office will:

- Maintain and regularly update the University's Record of Processing Activities (ROPA);
- Conduct periodic audits of data protection practices across Schools, Departments, and Professional Services;
- Report on data protection compliance, including breach statistics and SAR performance, to senior management and the University Council / Board of Governors at least annually;
- Review and update this Policy at least every 12 months, or sooner where required by changes in legislation, guidance, or University practice.

24. Breach of this Policy and Disciplinary Action

Failure to comply with this Policy may constitute a disciplinary matter and may be dealt with under the University's Staff or Student Disciplinary Procedures, as applicable. Depending on the nature and severity of the non-compliance, this may result in disciplinary action up to and including dismissal or expulsion, and may also expose the individual and/or the University to civil or criminal liability under Data Protection Legislation.

25. Complaints and Right to Lodge a Complaint

Any individual who has concerns about how the University processes their personal data may raise these with the Data Protection Office in the first instance, via [DPO CONTACT EMAIL] or [DPO CONTACT ADDRESS].

If an individual remains dissatisfied following the University's response, they have the right to lodge a complaint with the relevant national Supervisory Authority. Contact details for the Supervisory Authority will be provided by the Data Protection Office on request and are published on the University's data protection webpages.

26. Related Policies and Documents

- Information Security Policy
- Records Retention Schedule
- Acceptable Use of IT Policy
- Data Breach Response Procedure
- Privacy Notices (Staff, Student, Research Participant, Website/Cookies)
- Research Ethics Policy
- CCTV Policy
- Staff and Student Disciplinary Procedures
- Freedom of Information Policy (where applicable)

27. Policy Governance

This Policy is owned by the Data Protection Officer and approved by the University Council / Board of Governors. It will be reviewed at least annually, or earlier where required by changes in Data Protection Legislation, regulatory guidance, or organisational structure. Any amendments will be approved through the University's normal policy governance process.

Review

This policy will be periodically reviewed to ensure its effectiveness and relevance.