Data Protection Policy

POLICY # EAI/2024/241032

Adopted by the Senate on December 2, 2024

Euro American Institute

AGORA BUSINESS CENTRE LEVEL 2
TRIQ IL- WIED TA' L-IMSIDA
MSIDA, MSD 9020, Malta
qa@euroamerican.edu.mt

1. Introduction

EAI is committed to protecting the privacy and security of personal data of students, faculty, staff, and stakeholders. This policy establishes guidelines for handling personal data in compliance with applicable data protection laws and best practices.

2. Scope

This policy applies to all personal data collected, processed, and stored by EAI including:

- Student records (admissions, academic performance, attendance)
- Faculty and staff records (employment details, payroll, performance)
- Research data
- IT systems and communications
- Any other personal information held by the institution

3. Principles of Data Protection

EIMT adheres to the following data protection principles:

- **Lawfulness, Fairness, and Transparency**: Data must be collected and processed fairly and transparently.
- **Purpose Limitation**: Data must be collected for specified, explicit, and legitimate purposes.
- **Data Minimization**: Only the necessary data should be collected and stored.
- **Accuracy**: Personal data should be kept accurate and up to date.
- **Storage Limitation**: Data should not be kept longer than necessary.
- **Integrity and Confidentiality**: Appropriate security measures must protect personal data.
- **Accountability**: The institution is responsible for demonstrating compliance with data protection laws.

4. Data Collection and Processing

- Data will only be collected when necessary for academic, administrative, research, or operational purposes.
- Individuals must be informed about the purpose of data collection and their rights.
- Consent will be obtained where required, especially for sensitive personal data.

5. Data Security Measures

- Access to personal data is restricted to authorized personnel only.
- Encryption, secure storage, and cybersecurity measures will be implemented to protect data.
- Regular audits and security assessments will be conducted to prevent data breaches.
- In case of a data breach, immediate action will be taken, and relevant authorities will be informed as per legal requirements.

6. Rights of Individuals

EAI recognizes and respects the following rights of individuals:

- **Right to Access**: Individuals can request access to their personal data.
- **Right to Rectification**: Corrections can be made to inaccurate or incomplete data.
- **Right to Erasure (Right to be Forgotten)**: Individuals can request deletion of their data under certain conditions.
- **Right to Restrict Processing**: Data processing can be limited under specific circumstances.
- **Right to Data Portability**: Individuals can obtain and reuse their personal data across different services.
- **Right to Object**: Individuals can object to the processing of their data.

7. Data Sharing and Third Parties

- Personal data will not be shared with third parties unless required by law or for legitimate academic and operational purposes.
- Where third-party services are used (e.g., cloud storage, academic partnerships), data protection agreements will be in place.

8. Data Retention and Disposal

- Personal data will only be retained for as long as necessary.
- A retention schedule will be maintained for different categories of data.
- Secure disposal methods (e.g., shredding, secure deletion) will be used when data is no longer required.

9. Roles and Responsibilities

- **Data Protection Officer (DPO)**: Oversees compliance with this policy and data protection laws.
- **IT and Security Teams**: Ensure technical security of data.
- **All Staff and Faculty**: Must comply with data protection procedures.
- **Students and Stakeholders**: Expected to follow responsible data practices.

10. Policy Review and Updates

This policy will be reviewed periodically to align with legal updates, technological advancements, and institutional needs.

11. Compliance and Violations

- Any violations of this policy may result in disciplinary actions.
- Legal action may be taken in case of serious data breaches or misuse.