International Balkan University (IBU)
Data Protection Policy

The Data Protection Policy outlines the university's commitment to safeguarding personal and sensitive information and ensures compliance with applicable data protection laws and regulations. This policy establishes guidelines for collecting, processing, storing, and sharing personal data to protect individuals' privacy and rights.

This policy applies to all employees, faculty, staff, students, contractors, and any third parties who have access to or handle personal data at the university. It covers all types of personal data, including but not limited to student records, employee data, research data, and any other identifiable information.

1. Definitions

- **Personal Data**: Any information that can be used to identify an individual, either directly or indirectly, such as names, identification numbers, location data, online identifiers, or factors specific to the individual's identity (e.g., physical, physiological, genetic, mental, economic, cultural, or social identity).
- **Sensitive Data**: A subset of personal data that includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, and data concerning a person's sex life or sexual orientation.
- **Data Controller**: The university determines the purposes and means of processing personal data.
- **Data Processor**: Any person or organization that processes data on behalf of the Data Controller (e.g., third-party service providers).
- **Processing**: Any operation performed on personal data, such as collection, recording, organization, storage, retrieval, consultation, use, disclosure, or deletion.

2. Data Protection Principles

The university adheres to the following fundamental principles when processing personal data:

- **Lawfulness**, **Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and transparently. Individuals must be informed about how their data will be used and for what purpose.
- **Purpose Limitation**: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization**: Only the data necessary for the intended purpose should be collected and processed. Unnecessary data collection should be avoided.
- **Accuracy**: Personal data must be accurate and kept up to date. Inaccurate data must be corrected or deleted without delay.
- **Storage Limitation**: Personal data should only be kept for as long as necessary.

Retention periods must be defined based on legal, academic, and administrative requirements.

- **Integrity and Confidentiality**: Personal data must be processed securely to protect against unauthorized access, accidental loss, destruction, or damage.
- **Accountability**: The university is responsible for ensuring compliance with data protection principles and must be able to demonstrate compliance.

3. **Lawful Basis for Processing**

   The university processes personal data based on one or more of the following lawful grounds:

   - **Consent**: The individual has given explicit and informed consent to process their data.
   - **Contractual Necessity**: Processing is necessary to perform a contract with the individual (e.g., student enrollment, employment contracts).
   - **Legal Obligation**: Processing is necessary to comply with a legal obligation (e.g., reporting to government authorities).
   - **Vital Interests**: Processing is necessary to protect the vital interests of an individual (e.g., in emergencies or life-threatening situations).
   - **Public Task**: Processing is necessary for performing a task in the public interest or exercising official authority.
   - **Legitimate Interests**: Processing is necessary for the legitimate interests of the university or a third party, provided the individual's rights and freedoms do not override those interests.

4. **Individual Rights**

   Individuals whose data is processed by the university have the following rights:

   - **Right to Access**: Individuals can request access to their data and obtain information about how it is processed.
   - **Right to Rectification**: Individuals can request that inaccurate or incomplete data be corrected or updated.
   - **Right to Erasure**: Also known as the "right to be forgotten," individuals can request that their data be deleted in certain circumstances, such as when it is no longer necessary for the purpose it was collected.
   - **Right to Restrict Processing**: Individuals can request that the processing of their data be restricted in certain situations, such as during the investigation of a data accuracy issue.
   - **Right to Data Portability**: Individuals can request to receive their data in a structured, commonly used, and machine-readable format, and they have the right to transfer that data to another controller.
   - **Right to Object**: Individuals can object to processing their data based on legitimate interests, public tasks, or direct marketing purposes.
   - **Right Not to Be Subject to Automated Decision-Making**: Individuals have the right not to be subject to decisions based solely on automated processing,

including profiling, which produces legal effects or significantly affects them.

5. **Data Security**
    - **Access Control**: Access to personal data is restricted to authorized personnel who need access to perform their duties. Access is granted based on role-based access control (RBAC) and the principle of least privilege.
    - **Encryption**: Personal data must be encrypted at rest and in transit to protect it from unauthorized access or disclosure.
    - **Physical Security**: Measures must be in place to protect physical locations where personal data is stored (e.g., server rooms and filing cabinets).
    - **Incident Response**: In case of a data breach or security incident, the university will follow its incident response protocol to mitigate the impact and notify affected individuals and regulatory authorities as required.
6. **Data Sharing and Transfer**
    - **Third-Party Processors**: The university may engage third-party processors to perform certain functions (e.g., cloud storage, payroll services). Third parties must comply with the university's data protection requirements and enter into data processing agreements that outline their responsibilities.
    - **International Data Transfers**: If personal data is transferred outside the country, it must be protected under applicable protection laws (e.g., GDPR). The university will ensure that adequate safeguards, such as standard contractual clauses, are in place for international data transfers.
7. **Data Retention and Disposal**
    - **Retention Periods**: Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected under legal, academic, and administrative requirements. Retention schedules will be defined for each type of data.
    - **Secure Disposal**: When personal data is no longer needed, it must be securely disposed of to prevent unauthorized access. This includes shredding physical documents and securely deleting digital files.
8. **Training and Awareness**
    - **Employee Training**: All university employees and contractors who handle personal data must undergo regular data protection training to understand their responsibilities and the importance of safeguarding personal information.
    - **Awareness Campaigns**: The university will conduct awareness campaigns to inform students and staff about data protection best practices and their rights under data protection laws.
9. **Compliance and Accountability**
    - **Data Protection Officer (DPO):** The university will appoint a DPO responsible for overseeing compliance with data protection laws, providing advice and guidance, and acting as a point of contact for individuals and regulatory authorities.
    - **Audits and Monitoring**: The university will conduct regular audits and

monitoring activities to ensure compliance with this policy and data protection laws.

- **Record Keeping**: The university will maintain records of data processing activities as required by law and ensure that these records are accurate and up to date.

10. Policy Review and Updates

- The IT department will review this policy regularly and update it as necessary to reflect changes in technology, legal requirements, or university operations. Users will be notified of any significant changes to the policy.