EUROPEAN RESEARCH
UNIVERSITY

Data Protection Policy

1. Introduction

1.1 Policy Purpose

The fundamental objective of this section is to articulate the overarching purpose of the data protection policy established by the European Research University (ERUNI). It serves as a foundational statement that outlines the core principles and procedures governing the protection of personal data within the institution's purview.

At its essence, the policy aims to ensure the comprehensive protection of personal data collected and processed by the ERUNI. By delineating clear principles and procedures, it establishes a framework that promotes transparency, accountability, and respect for individuals' privacy rights.

Through this policy, the ERUNI endeavours to:

- Establish a set of guiding principles that underscore the importance of safeguarding personal data in all its operations and activities.
- Define clear procedures and protocols for the collection, processing, storage, and disposal of personal data to mitigate risks and ensure compliance with legal obligations.
- Enhance transparency by providing clear and accessible information to data subjects regarding the purposes and methods of data processing, as well as their rights and options for recourse.
- Foster a culture of accountability and responsibility among university staff, students, and affiliated entities, emphasizing the importance of upholding data protection standards in their respective roles and activities.

- Demonstrate the university's commitment to respecting and protecting the privacy rights of individuals whose data it processes, thereby building trust and confidence in its data handling practices.

1.2 Scope

This section delineates the extent and applicability of the data protection policy within the operational domain of the ERUNI. It defines the parameters within which the policy governs the processing of personal data and identifies the individuals and entities subject to its provisions.

The scope of this policy encompasses:

- **All Personal Data Processing:** The policy applies to every instance of personal data processing conducted within the ERUNI's operations. This includes data processing activities undertaken by university departments, research units, administrative bodies, and any other entities acting on behalf of the university.

- **All Individuals and Entities:** The policy extends its jurisdiction to cover all individuals and entities associated with the ERUNI. This includes but is not limited to:

    - Employees: All staff members, including permanent, temporary, and contracted personnel, regardless of their role or position within the university hierarchy.

    - Students: All enrolled students, whether undergraduate, graduate, doctoral, or postdoctoral, and regardless of their academic discipline or program of study.

    - Data Processors: Any external entities or third-party service providers engaged by the university to process personal data on its behalf, including cloud service providers, software vendors, and research collaborators.

    - Other Affiliated Entities: Any other organizations, institutions, or entities that collaborate with or act on behalf of the ERUNI in data processing activities, such as partner universities, research consortia, or funding agencies.

1.3 Legal Framework

- The ERUNI's data protection policy operates within the framework established by applicable European and national legislation concerning the safeguarding of personal data. This includes but is not limited to regulations, directives, and statutes that govern the collection, processing, storage, and transfer of personal data.

- At the core of this legal framework is the General Data Protection Regulation (GDPR), which serves as the cornerstone of data protection legislation within the European Union. Enacted to strengthen individuals' rights and enhance control over their personal data, the GDPR sets forth stringent requirements for organizations, including universities, regarding the lawful processing of personal data. Key provisions of the GDPR include principles such as lawfulness, fairness, and transparency in data processing; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

- In addition to the GDPR, the ERUNI also adheres to other relevant legislation at the national level within the countries where it operates. These may include specific data protection laws, guidelines issued by supervisory authorities, and sector-specific regulations.

- By aligning its data protection policy with the GDPR and other pertinent legal frameworks, the ERUNI demonstrates its commitment to upholding the highest standards of data protection and privacy for individuals whose data it processes. Compliance with these laws ensures that personal data is handled ethically, responsibly, and in accordance with the rights and expectations of data subjects. Furthermore, it mitigates the risk of non-compliance penalties and fosters trust and confidence among stakeholders in the university's data handling practices.

2. Principles of Data Protection

2.1 Legitimacy of Processing

The principle of legitimacy of processing underscores the ethical and legal foundation upon which personal data is handled by the ERUNI. It emphasizes that all processing activities involving personal data must be conducted in accordance with applicable data protection laws, regulations, and principles. This includes, but is not limited to, the GDPR and any other relevant national or international laws.

At the core of this principle lies the requirement that personal data shall only be processed for lawful purposes. This means that the ERUNI will ensure that there is a valid legal basis for each processing activity, such as the consent of the data subject, the performance of a contract, compliance with legal obligations, protection of vital interests, the pursuit of legitimate interests pursued by the ERUNI or a third party, or the performance of tasks carried out in the public interest or in the exercise of official authority vested in the ERUNI.

Furthermore, personal data will only be processed for the specific purpose for which it was collected. Any subsequent processing of personal data must be compatible with the original purpose for which it was obtained. If there is a need to process personal data for a new purpose not previously disclosed to the data subject, the ERUNI will seek additional consent or ensure that the new purpose is compatible with the original purpose under applicable laws and regulations.

By adhering to the principle of legitimacy of processing, the ERUNI demonstrates its commitment to respecting the rights and privacy of individuals while maintaining transparency and accountability in its data processing practices. This ensures that personal data is handled responsibly and ethically, fostering trust and confidence among data subjects and stakeholders.

2.2 Transparency

Transparency is a foundational principle guiding the ERUNI's approach to handling personal data. It underscores the importance of providing clear, accessible, and comprehensive information to data subjects regarding the processing of their personal data. This principle serves as a cornerstone for building trust, empowering individuals to understand and exercise control over their personal information.

The ERUNI is committed to ensuring transparency throughout all stages of the data processing lifecycle. This includes:

- **Informing Data Subjects:** Data subjects will be informed about the purposes for which their personal data is being processed. This information will be communicated clearly, using easily understandable language, at the time of data collection or as soon as reasonably practicable thereafter. The ERUNI will also provide information about any additional processing activities that may occur beyond the initial collection, ensuring that data subjects are aware of how their data will be used.

- **Rights and Options:** Data subjects will be informed about their rights regarding data protection. This includes the right to access their personal data, rectify inaccuracies, request erasure, restrict processing, and object to processing under certain circumstances. The ERUNI will also provide information about how data subjects can exercise these rights and any relevant procedures or forms that need to be followed.

- **Data Handling Practices:** The ERUNI will be transparent about its data handling practices, including the security measures in place to protect personal data from unauthorized access, disclosure, alteration, or destruction. This may include information about encryption, access controls, data retention policies, and measures taken in the event of a data breach.

- **Updates and Changes:** If there are any updates or changes to the ERUNI's data processing practices or policies, data subjects will be informed in a timely manner. This may include changes to the purposes of processing, the categories of personal data being processed, or any other relevant information that may impact data subjects' rights or expectations.

2.3 Purpose Limitation

- The principle of purpose limitation is fundamental to ensuring that personal data is used only for specific and legitimate purposes. The ERUNI adheres to this principle to safeguard individuals' privacy rights and maintain trust in its data processing activities.**Specified Purposes:** Personal data collected by the ERUNI is used only for clearly defined and lawful purposes. These purposes are communicated to data subjects at the time of data collection or as soon as practicable thereafter. The university ensures that data subjects are aware of why their data is being collected and how it will be used, thereby promoting transparency and accountability.

- **Legitimate Grounds:** The ERUNI processes personal data only on lawful grounds, as outlined in applicable data protection laws and regulations. This includes obtaining consent from data subjects where required, fulfilling contractual obligations, complying with legal obligations, protecting vital interests, pursuing legitimate interests, or performing tasks carried out in the public interest or in the exercise of official authority vested in the ERUNI.

- **Compatibility:** Personal data is not processed in a manner that is incompatible with the purposes for which it was originally collected. If the ERUNI intends to use personal data for a new purpose that is not compatible with the original purpose, it will seek additional consent from the data subject or ensure that the new purpose is permitted by law.

- **Minimization:** The ERUNI minimizes the processing of personal data to what is necessary for the specified purposes. Unnecessary or excessive data collection is avoided, and only data that is relevant and adequate for achieving the intended purposes is processed.

2.4 Data Minimization

Data minimization is a fundamental principle guiding the ERUNI's approach to personal data processing. It emphasizes the importance of limiting the collection, processing, and retention of personal data to only what is necessary for the specified purposes. By minimizing the amount of personal data held and processed, the university reduces privacy risks, enhances data security, and ensures compliance with data protection laws and regulations.

Key aspects of data minimization include:

- **Collection Limitation:** The ERUNI collects only the personal data that is relevant, adequate, and necessary for the specified purposes. Before collecting any personal data, careful consideration is given to whether the information is essential to achieve the intended objectives. Unnecessary or excessive data collection is avoided.

- **Purpose-based Data Processing:** Personal data is processed solely for the purposes for which it was collected. The ERUNI ensures that data processing activities are closely aligned with the specified purposes and does not engage in any additional processing that is incompatible with those purposes.

- **Retention Period Limitation:** Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected. The ERUNI establishes and adheres to specific retention periods based on legal requirements, business needs, and the nature of the data. Once the retention period expires or the purposes for processing are fulfilled, personal data is securely disposed of or anonymized.

- **Data Minimization Techniques:** The ERUNI employs various techniques and measures to minimize the amount of personal data processed. This may include anonymization, pseudonymization, aggregation, and encryption, among others, to reduce the risk of identifying individuals and protect their privacy.

2.5 Data Accuracy

Ensuring the accuracy of personal data is a paramount principle for the ERUNI. This principle emphasizes the importance of maintaining the correctness and precision of personal data throughout its lifecycle, from collection to disposal. Accurate data is essential for making informed decisions, providing quality services, and upholding individuals' rights.

Key components of the data accuracy principle include:

- **Accuracy Assurance:** The ERUNI takes proactive measures to ensure that personal data is accurate and up to date. This includes implementing data validation procedures during collection, verifying the accuracy of data entries, and updating records as necessary to reflect any changes or corrections.

- **Data Quality Control:** Quality control mechanisms are established to monitor the accuracy of personal data over time. Regular audits, checks, and reviews are conducted to identify and rectify any inaccuracies, inconsistencies, or errors in the data.

- **Data Subject Participation:** Data subjects are encouraged to actively participate in maintaining the accuracy of their personal data. They are provided with mechanisms to review, correct, update, or delete their information as needed, ensuring that their records remain accurate and reflective of their current circumstances.

- **Staff Training and Awareness:** Employees and other personnel involved in handling personal data receive training and guidance on the importance of data accuracy and the procedures for maintaining accurate records. They are educated on best practices for data entry, verification, and validation to minimize errors and ensure data quality.

- **Documentation and Documentation:** The ERUNI maintains accurate documentation of personal data processing activities, including the sources of data, any changes made to the data, and the reasons for such changes. This documentation serves as a record of accountability and transparency in data management practices.

2.6 Data Retention Limitation

Data retention limitation is a crucial principle guiding the ERUNI's approach to managing personal data. This principle emphasizes the importance of retaining personal data only for the period necessary to fulfil the purposes for which it was collected. By limiting the retention of personal data, the university minimizes privacy risks, reduces storage costs, and ensures compliance with data protection laws and regulations.

Key aspects of the data retention limitation principle include:

- **Retention Period Determination:** The ERUNI establishes clear and documented retention periods for different categories of personal data based on legal requirements, business needs, and the purposes for which the data was collected. These retention periods are periodically reviewed and updated to ensure they remain appropriate and relevant.

- **Lawful Basis for Retention:** Personal data is retained only on lawful grounds and in accordance with applicable data protection laws and regulations. The ERUNI ensures that there is a valid legal basis for retaining each category of personal data, such as compliance with legal obligations, contractual requirements, or legitimate interests pursued by the university or third parties.

- **Data Minimization:** The ERUNI applies data minimization principles to retention practices, ensuring that only the minimum amount of personal data necessary for the specified purposes is retained. Unnecessary or outdated data is securely deleted or anonymized to reduce privacy risks and streamline data management processes.

- **Secure Storage and Disposal:** Personal data is stored securely during the retention period to prevent unauthorized access, disclosure, or loss. Once the retention period expires or the purposes for processing are fulfilled, personal data is securely disposed of using appropriate methods, such as shredding, permanent deletion, or anonymization, in accordance with data protection requirements.

- **Documentation and Accountability:** The ERUNI maintains accurate records and documentation of its data retention practices, including the rationale for retention decisions, the applicable retention periods, and the procedures for secure disposal. This documentation ensures accountability and transparency in data management practices and facilitates compliance with regulatory requirements.

2.7 Integrity and Security of Data

Ensuring the integrity and security of data is a paramount principle for the ERUNI. This principle underscores the university's commitment to protecting personal data from unauthorized access, alteration, disclosure, or destruction throughout its lifecycle. By maintaining the integrity and security of data, the university safeguards individuals' privacy rights, prevents data breaches, and fosters trust in its data handling practices.

Key components of the integrity and security of data principle include:

- **Data Security Measures:** The ERUNI implements robust technical, organizational, and administrative measures to protect personal data against unauthorized access, disclosure, alteration, or destruction. These measures include access controls, encryption, firewalls, intrusion detection systems, and regular security audits and assessments.

- **Confidentiality:** Personal data is treated as confidential and is accessible only to authorized personnel who have a legitimate need to access the data for specified purposes. Confidentiality agreements, data access controls, and role-based access restrictions are implemented to ensure that personal data is accessed and processed only by authorized individuals.

- **Data Integrity Checks:** The ERUNI employs measures to maintain the accuracy and completeness of personal data, including data validation checks, data integrity controls, and audit trails. These measures help detect and prevent unauthorized alterations or tampering with personal data, ensuring its reliability and trustworthiness.

- **Data Transfer Security:** When transferring personal data to third parties or across borders, the ERUNI ensures that appropriate safeguards are in place to protect the confidentiality, integrity, and security of the data. This may include implementing encryption, data minimization techniques, and contractual agreements with data processors to ensure compliance with data protection requirements.

- **Incident Response and Reporting:** The ERUNI maintains incident response procedures to promptly identify, assess, and respond to data security incidents or breaches. Data breaches are reported to the relevant supervisory authorities and affected data subjects in accordance with legal requirements, and remedial actions are taken to mitigate the impact of the breach and prevent future occurrences.

- **Employee Training and Awareness:** Employees and other personnel involved in handling personal data receive regular training and awareness programs on data security best practices, policies, and procedures. This helps ensure that staff members are equipped with the knowledge and skills necessary to protect personal data effectively and mitigate security risks.

2.8 Data Subject Rights

Respecting and upholding the rights of data subjects is a cornerstone principle for the ERUNI. This principle emphasizes the importance of empowering individuals to exercise control over their personal data and ensuring that their privacy rights are upheld in accordance with applicable data protection laws and regulations. By recognizing and respecting data subject rights, the ERUNI enhances transparency, accountability, and trust in its data processing activities.

Key aspects of the data subject rights principle include:

- **Right to Access:** Data subjects have the right to access their personal data held by the ERUNI and obtain information about how their data is being processed, including the purposes of processing, the categories of data being processed, and the recipients or categories of recipients to whom the data has been disclosed.

- **Right to Rectification:** Data subjects have the right to request the rectification of inaccurate or incomplete personal data held by the ERUNI. The ERUNI promptly addresses such requests and ensures that inaccurate or outdated data is corrected or updated as necessary.

- **Right to Erasure (Right to be Forgotten):** Data subjects have the right to request the erasure of their personal data under certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or when the data subject withdraws consent and there is no other legal basis for processing the data.

- **Right to Restriction of Processing:** Data subjects have the right to request the restriction of processing of their personal data under certain circumstances, such as when the accuracy of the data is contested, the processing is unlawful, or the data subject has objected to the processing pending verification of legitimate grounds.

- **Right to Data Portability:** Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and have the right to transmit that data to another controller without hindrance from the ERUNI, where technically feasible.

- **Right to Object:** Data subjects have the right to object to the processing of their personal data based on legitimate interests pursued by the ERUNI or third parties. The ERUNI ceases processing personal data unless it can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject.

- **Rights in Automated Decision Making and Profiling:** Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless there is a lawful basis for such processing and appropriate safeguards are in place to protect the rights and freedoms of the data subject.

3. Accountability and Compliance

3.1 Accountability

Accountability is a foundational principle for the ERUNI's data protection framework. This principle emphasizes the ERUNI's commitment to taking responsibility for its data processing activities and ensuring compliance with applicable data protection laws, regulations, and policies. By embracing accountability, the ERUNI demonstrates transparency, integrity, and commitment to protecting individuals' privacy rights.

Key aspects of the accountability principle include:

- **Internal Responsibility:** The ERUNI assigns responsibility for data protection compliance to designated individuals or departments, such as a Data Protection Officer (DPO) or a dedicated data protection team. These individuals or teams are responsible for overseeing data protection efforts, implementing policies and procedures, and ensuring compliance with legal requirements.

- **Policy Development:** The ERUNI develops and maintains comprehensive data protection policies and procedures that outline its commitment to privacy, the principles governing data processing, and the responsibilities of staff, students, and other stakeholders. These policies are regularly reviewed, updated, and communicated to ensure awareness and understanding among relevant parties.

- **Risk Management:** The ERUNI conducts regular risk assessments to identify and evaluate potential risks to the security and privacy of personal data. These assessments help prioritize mitigation efforts and allocate resources effectively to address identified risks and vulnerabilities.

- **Training and Awareness:** The ERUNI provides regular training and awareness programs to staff, students, and other stakeholders on data protection policies, procedures, and best practices. This ensures that individuals understand their roles and responsibilities in safeguarding personal data and are equipped with the knowledge and skills necessary to comply with data protection requirements.

- **Documentation and Record-keeping:** The ERUNI maintains accurate records and documentation of its data processing activities, including data protection policies, procedures, risk assessments, and compliance efforts. These records serve as evidence of accountability and transparency in data management practices and facilitate compliance with regulatory requirements.

- **Compliance Monitoring and Reporting:** The ERUNI monitors compliance with data protection policies and procedures through regular audits, assessments, and reviews. Any non-compliance issues are promptly identified, investigated, and addressed, and appropriate corrective actions are taken to mitigate risks and prevent recurrence. Additionally, the university reports on its data protection efforts to relevant stakeholders, such as data subjects, regulatory authorities, and governing bodies.

3.2 Training and Awareness

Training and awareness form a crucial component of the ERUNI's data protection framework. This principle underscores the importance of educating employees, students, and other relevant stakeholders about their roles, responsibilities, and obligations concerning data protection. By investing in training and raising awareness, the university aims to cultivate a culture of privacy, security, and compliance throughout its operations.

Key aspects of the training and awareness principle include:

- **Employee Training:** The ERUNI provides comprehensive training programs to employees at all levels on data protection policies, procedures, and best practices. Training sessions cover topics such as the principles of data protection, legal requirements, handling of personal data, security measures, and incident response protocols. Employees receive regular updates and refresher courses to stay abreast of evolving data protection regulations and emerging threats.

- **Student Education:** Students are educated about data protection principles, their rights regarding personal data, and the ERUNI 's policies and procedures through orientation programs, workshops, and information sessions. Student representatives may also be involved in promoting data protection awareness and compliance initiatives within the student body.

- **Specialized Training:** Certain roles or departments may require specialized training tailored to their specific data protection responsibilities. For example, individuals involved in data processing activities, such as researchers or IT personnel, may receive specialized training on data handling practices, data security protocols, and compliance requirements relevant to their roles.

- **Awareness Campaigns:** The ERUNI conducts awareness campaigns and communication initiatives to reinforce data protection principles and promote a culture of privacy and security. These campaigns may include posters, newsletters, email reminders, and intranet resources highlighting key data protection messages, best practices, and recent developments.

- **Testing and Evaluation:** The effectiveness of training and awareness initiatives is periodically evaluated through assessments, quizzes, or surveys to measure knowledge retention and identify areas for improvement. Feedback from participants is used to refine training materials, update content, and enhance the overall effectiveness of the training program.

- **Ongoing Support:** The ERUNI offers ongoing support and guidance to employees, students, and other stakeholders through dedicated channels, such as a data protection helpdesk or resource centre. Individuals can seek assistance, ask questions, and report concerns related to data protection issues, ensuring that they receive timely and accurate responses to their inquiries.

3.3 Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) are a vital tool employed by the ERUNI to identify, assess, and mitigate risks associated with data processing activities. This principle emphasizes the importance of conducting DPIAs for projects, initiatives, or systems involving the processing of personal data, particularly those that pose potential risks to individuals' privacy rights.

Key aspects of the DPIAs principle include:

- **Identification of Processing Activities:** The ERUNI identifies all data processing activities that may impact individuals' privacy rights. This includes the collection, storage, use, sharing, and disposal of personal data within various projects, initiatives, or systems.

- **Assessment of Risks:** DPIAs systematically evaluate the potential risks and impacts of data processing activities on individuals' privacy and data protection rights. Risks may include unauthorized access, disclosure, alteration, or loss of personal data, as well as risks related to data accuracy, security, and compliance.

- **Legal and Ethical Considerations:** DPIAs consider legal and ethical considerations relevant to data protection laws, regulations, and best practices. This ensures that data processing activities comply with applicable legal requirements, respect individuals' privacy rights, and adhere to ethical standards and principles.

- **Consultation and Collaboration:** DPIAs involve consultation and collaboration with relevant stakeholders, including data subjects, project teams, legal experts, IT specialists, and data protection officers. This multi-disciplinary approach ensures that diverse perspectives are considered, and potential risks are adequately addressed.

- **Risk Mitigation Strategies:** DPIAs identify and recommend appropriate risk mitigation strategies and measures to address identified risks and vulnerabilities. This may include implementing technical, organizational, or procedural controls to minimize risks, enhance data security, and protect individuals' privacy rights.

- **Documentation and Reporting:** DPIAs are documented comprehensively, detailing the scope of the assessment, the methodology used, the findings, and the recommended actions. The results of DPIAs are reported to relevant stakeholders, such as project sponsors, decision-makers, and data protection authorities, to ensure transparency and accountability in risk management efforts.

- **Ongoing Monitoring and Review:** DPIAs are not static documents but are subject to ongoing monitoring and review throughout the lifecycle of data processing activities. Any changes to the project scope, data processing methods, or risk landscape trigger a reassessment of DPIAs to ensure that risk mitigation measures remain effective and proportionate.

In Ostrava, 1st September 2023

Assoc. Prof. Zuzana Machová, Ph.D.
rector

Annex: Security Measures for Using IT Assets

Security Measures for Using IT Assets

In accordance with the structure of version 1.2: Minimum Security Standard of the National Cyber and Information Security Agency (hereinafter referred to as the Standard), the structure derived from the structure of the Technical Part of the Standard was used for security measures.

Physical Security

Physical data security at the location (domain controller) is ensured by controlled access to the school building (access is controlled by a chip access system), which eliminates the movement of unidentified persons near servers and data storage. Outside of operating hours, the building is protected by an electronic system with a connection to a remote central security control panel.

Access Control

Access to systems is granted to users based on username and password authentication. Considering the higher risk of this approach, strict password strength requirements are applied. Password rotation is not required as it is not considered a desirable security measure.

Protection against Malicious Code

Protection against malicious code is provided on two levels: At the network perimeter entry level, the entire network is protected by a Sophos XG210 network firewall with activated content inspection. At the level of individual endpoints (PCs, tablets, smartphones, but also servers), Eset/Avast antivirus software provides protection against malicious code.

Use of Cryptographic Means

Data transfer is limited to cloud services available via HTTPS (e.g., Moodle, STAG), so encryption of transmitted data is ensured. Centralized password storage is not used, and the use of external disks for school data is restricted by organizational directive, so disk encryption is not centrally mandated.

Service Availability

Service availability is addressed based on SLA parameters for the administrator (Moodle) or based on SLA terms in contracts with external service providers (STAG).

Backup of Internal Systems

Backup of internal systems (domain controller, Moodle) is performed by administrators using standardized procedures.

Cloud Service Protection

In terms of cloud services, only the STAG system (hosted by a provider in the Czech Republic with storage location in the Czech Republic) and Office 365 are used, where compliance with regulatory requirements, including storage location, is ensured by standard service terms for customers in the EU.