

DATA PROTECTION POLICY

1. General Provisions

1.1. This Privacy Policy (hereinafter – the Policy) establishes a comprehensive legal and organizational framework for the collection, processing, storage, and protection of information relating to identified or identifiable natural persons involved in the activities of the ERASMUS+ Jean Monnet Module “European Regulation of the Cryptocurrency Market: Implementation in Ukraine” (hereinafter – ERCM).

1.2. The Policy has been developed as a guarantee of compliance with the provisions of the Grant Agreement, which require beneficiaries to strictly adhere to the norms of the EU General Data Protection Regulation (GDPR – Regulation (EU) 2016/679).

1.3. The project is implemented in Ukraine by Yaroslav Mudryi National Law University; therefore, the processing of personal data is also aligned with the requirements of the Law of Ukraine “On Personal Data Protection.” The specifics of the project, which include the implementation of certificate program modules, organization of international conferences, participant surveys, and an active information campaign in the digital environment, necessitate the processing of large volumes of data.

1.4. The University acts as the Data Controller, independently determining the purposes and means of data processing within the framework of tasks delegated by the European Education and Culture Executive Agency (hereinafter – EACEA).

2. Basic Principles of Personal Data Processing

2.1. The principle of lawfulness, fairness, and transparency implies that data collection is carried out exclusively on legitimate grounds. For participants of certificate programs and conferences, such grounds consist of their clear, informed, and voluntary consent provided by completing electronic registration forms or signing relevant documents. Participants are informed in an accessible manner about what information is collected and for what purpose.

2.2. The principle of purpose limitation ensures that personal data is collected solely for clearly defined and legitimate purposes: administration of the educational process, issuance of certificates, organization of communication, evaluation of project effectiveness, and preparation of statistical reporting. Further processing incompatible with these purposes is not permitted.

2.3. The principle of data minimization is applied: only the amount of information necessary and relevant to achieve the defined purposes is processed. The collection of excessive data is prohibited.

2.4. Data accuracy is ensured through timely updates upon user request, storage limitation, and the maintenance of integrity and confidentiality through appropriate technical and organizational security measures.

3. Categories of Data and Purposes of Processing

3.1. To ensure transparency of processing, the following categories of personal data subjects, types of data, and purposes of their use within the ERCM project are defined:

3.1.1. Participants of the certificate program / webinar attendees: processed data includes surname, name, age, gender (for statistical purposes), email address, contact phone number, place of study or employment, and test results. The purpose is to provide access to educational materials, monitor academic performance, issue certificates, and prepare reports. Processing is based on consent.

3.1.2. Conference speakers and authors of academic materials: collected data includes surname, name, academic degree, academic title, place of work, presentation topic, and contact information. Data is

used for event organization, publication of materials, and communication. Processing is based on consent and legitimate interest.

3.1.3. Members of the working group and invited experts: processed data includes passport details, identification numbers, bank details, CVs, and qualification information. This is necessary for concluding contracts, making payments, and maintaining financial reporting. Processing is based on consent.

3.1.4. Visitors of digital platforms and the project website: processed data includes IP addresses, cookies, and technical connection logs. The purpose is to ensure cybersecurity, analyze communication effectiveness, and improve user experience. Processing is based on consent.

4. Ensuring the Rights of Data Subjects

4.1. Data subjects within the ERCM project retain full control over their personal information. The University, as the controller, ensures proper conditions for the free and unhindered exercise of their rights.

4.2. Each participant has the right to contact the project coordinator with a request to confirm whether their personal data is being processed, as well as to obtain a copy of such data.

4.3. In case of inaccuracies or incompleteness of personal data, including in registration forms or certificates, the data subject has the right to request their immediate correction or completion.

4.4. The data subject has the right to request the deletion of their personal data if there is no longer a need for its processing for project purposes or if consent is withdrawn. This right may be restricted if data retention is mandatory in accordance with EU audit requirements to confirm the proper use of grant funds.

4.5. The data subject has the right to request restriction of processing of their personal data, including during the period of verification of its accuracy, and to object to processing, particularly regarding the use of contact data for informational mailings within the project.

4.6. Upon request, personal data may be provided in a structured, commonly used, and machine-readable format for further transmission to another controller.

4.7. To exercise any of these rights, the data subject must submit an electronic or written request addressed to the project coordinator, which shall be processed within no more than one month.

5. Organizational and Technical Protection Measures and Incident Management

5.1. The protection of personal data is a priority of the project's activities. Access to personal information is granted only to authorized persons whose functional duties are directly related to its processing. Such persons are obliged to maintain confidentiality.

5.2. Technical protection is ensured through the use of modern encryption tools, secure storage, multi-factor authentication, and regular backups. Data used for analytics is subject to anonymization.

5.3. In the event of a personal data breach, a response procedure is applied, including incident containment, documentation, investigation, and, where necessary, notification of competent authorities and data subjects.

6. Data Storage, Archiving, and Cross-Border Transfer

6.1. Due to the international nature of the project, cross-border transfers of personal data may occur, particularly to facilitate cooperation with foreign lecturers. Such transfers are carried out only if an adequate level of data protection is ensured in accordance with GDPR requirements or on the basis of appropriate contractual mechanisms.

6.2. The retention periods for personal data are strictly regulated by EU grant financial management rules. In accordance with Article 20 (Record-keeping) of the Grant Agreement, all primary documents confirming proper project implementation and potentially containing personal data (registration sheets, questionnaires, contracts) are stored in the University's secure archives for at least 5 years after the final payment (or 3 years for grants up to EUR 60,000) to enable post-project audits by EU institutions. After this period, and in the absence of other legal grounds for retention, personal data shall be irreversibly destroyed.