Community Participant Data Protection Policy

2025

1. General Provisions

1.1. This Policy defines the principles, procedures, and measures for ensuring the confidentiality and security of the personal data of Community participants.

1.2. The Community considers participants' data as valuable and inviolable information, requiring special protection at all stages — from collection and processing to storage and final deletion.

2. Principles of Data Processing

2.1. All personal data provided by participants are considered strictly confidential and are protected according to the principle of absolute privacy.

2.2. The Community does not transfer, sell, or disclose personal data to third parties, except in cases where it is explicitly required by applicable law, and only to the extent minimally necessary to fulfill such a requirement. We will use all lawful means to challenge or minimize any requests that, in our opinion, violate the principle of confidentiality.

3. Purposes of Data Processing

3.1. Personal data processing is carried out exclusively for:

- individual support of participants;
- personalized development planning;
- provision of educational and mentoring support;
- improvement and optimization of the Community's internal services.

4. Technical and Organizational Data Protection Measures

4.1. Personal data is protected by cryptographic information security means, including encryption and multi-factor authentication.

4.2. A distributed access model is applied: Community employees have access only to the data necessary to perform their duties.

4.3. Internal information security audits are conducted regularly.

5. Participants' Rights

5.1. A participant has the right to:

- receive full information about the purposes and methods of processing their data;

- independently determine the circle of persons who are granted access to their data;
- at any time refuse further processing and request the complete deletion of all data.

5.2. Data deletion is carried out within 14 calendar days from the moment the corresponding request is received. During this period, the participant can change their decision and withdraw the request.

5.3. If the participant does not notify about their intention to cancel the request after the specified period, all data is subject to irreversible deletion.

6. Transparency and Notifications

6.1. The data processing policy is made publicly available and accessible for all participants.

6.2. In the event of changes to the data processing conditions, participants are informed in advance through official communication channels.

7. Responsibility and Control

7.1. An authorized data protection officer is appointed, responsible for compliance with this Policy.

7.2. Continuous control over data processing security is carried out, including regular checks of procedural compliance.

8. Limitation of Liability

8.1. The Community is not responsible for cases of data disclosure caused by the participant themselves, including:

- voluntary dissemination of personal information;
- transfer of data to third parties;
- violation of security rules (for example, password compromise, hacking of personal devices).

9. Final Provisions

9.1. This Policy comes into force from the moment it is approved by the authorized persons of the Community.

9.2. All issues not regulated by this Policy are subject to consideration in accordance with the internal regulations of the Community and applicable law.