POLICY

on the Processing and Protection of Personal Data and Rules for Using the Information Resource of the Finopolis Forum of Innovative Financial Technologies (October 8–10, 2025)

1. GENERAL PROVISIONS

1.1. This Policy on the Processing and Protection of Personal Data (hereinafter referred to as the "Policy") for the Finopolis Forum of Innovative Financial Technologies (October 8–10, 2025) defines the principles, purposes, conditions, terms, and methods of processing personal data (hereinafter referred to as "PD"), the categories of PD subjects, the actions performed with PD, the rights of PD subjects, measures to monitor compliance with Russian legislation on PD processing, and PD protection measures.

1.2. This Policy applies to Limited Liability Company "EFFECTIVE COMMUNICATIONS" (INN 7716792536, OGRN 5147746475058, address: 101000, Moscow, Potapovsky per., bldg. 5, str. 2) (hereinafter referred to as the "Organization") for:

Organizing PD processing in compliance with applicable laws;
Developing measures to promptly detect unauthorized access (UAA) to PD and implementing actions to prevent UAA;
Monitoring the established level of PD security.
1.3. This Policy is drafted in Russian. The English version is available at https://finopolis.ru/en/.

1.4. The General Director is responsible for compliance with Russian laws and the Organization’s internal regulations regarding PD.

1.5. This Policy is mandatory for all employees involved in PD processing and security.

2. KEY TERMS AND DEFINITIONS

2.1. The following terms are used in this Policy:

- Information – data (messages, records) regardless of their form;
- Documented information – information recorded on a tangible medium with details allowing its identification;
- Personal Data (PD) – any information relating to an identified or identifiable individual (PD subject);
- Confidentiality of PD – a requirement preventing unauthorized disclosure of PD without the subject’s consent or legal grounds;
- Operator – LLC "EFFECTIVE COMMUNICATIONS" (INN 7716792536, OGRN 5147746475058, address: 101000, Moscow, Potapovsky per., bldg. 5, str. 2), which

organizes and/or processes PD, determines processing purposes, and actions performed with PD;

- PD Processing – any action (automated or manual) involving PD, including collection, recording, systematization, storage, updating, retrieval, use, transfer, blocking, deletion, or destruction;
- Automated PD Processing – processing using computer technology;
- PD Dissemination – disclosure of PD to an indefinite group of persons;
- PD Provision – disclosure of PD to a specific person or group;
- PD Blocking – temporary suspension of processing (unless necessary for clarification);
- PD Destruction – actions making PD recovery impossible;
- PD Information System – a set of PD databases and related technologies;
- Cross-Border PD Transfer – transfer of PD to foreign states.

3. PROCESSING OF PERSONAL DATA

3.1. Principles of PD Processing

3.1.1 PD processing is limited to lawful, predefined purposes (§3.2).
3.1.2 Incompatible databases shall not be merged.
3.1.3 Only relevant and non-excessive PD shall be processed.
3.1.4 Accuracy and relevance of PD shall be maintained.
3.1.5 Storage duration shall not exceed legal or contractual requirements.
3.1.6 PD shall be destroyed after processing purposes are fulfilled.
3.1.7 PD shall not be disclosed without consent, unless required by law.

3.2. Purposes of PD Processing

- 3.2.1 Processing of personal data during the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025) is carried out for the following purposes:

- Ensuring compliance with legislative and regulatory acts of the Russian Federation;
- Preparation, execution, and termination of contracts with counterparties;
- Production of participant badges for the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025);
- Implementation of access control and security measures at the venue, as well as for business and cultural program events, receptions, exhibitions, and business meetings during the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025);
- Informing potential participants about the dates and location of the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025);
- Distribution of informational messages.3.3. Categories of PD Subjects

3.3 List of Personal Data Subjects

3.3.1 During the organization of the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025), the following categories of personal data subjects are processed:

- Participants of the Finopolis Forum of Innovative Financial Technologies, October 8-10, 2025;

- Speakers of the Finopolis Forum of Innovative Financial Technologies, October 8-10, 2025.

3.4 List of Processed Personal Data

3.4.1 The list of processed personal data is determined in accordance with the processing purposes specified in this Policy and includes the following information:

- Last name, first name, and patronymic (if applicable);
- Contact details (mobile phone number, email address);
- Current employment information (employer and job position);
- Photograph;
- Cookie files.

3.5 Personal Data Processing Period

3.5.1 Personal data is processed until the specified processing purposes are achieved, unless the processing period is established by federal law or an agreement where the personal data subject is a party, beneficiary, or guarantor.

3.6 Conditions for Personal Data Processing

3.6.1 Personal data is processed with the consent of the personal data subject.
3.6.2 Consent signed with a simple electronic signature is recognized as an electronic document equivalent to consent signed with the subject's handwritten signature.
3.6.3 Consent is considered signed with a simple electronic signature and fully identical to a paper-based document when the verification code received via SMS or email is provided, provided that the code was sent to the phone number or email address specified by the personal data subject. The simple electronic signature has the same legal validity as the subject's handwritten signature from the moment of code submission.
3.6.4 Verification of the electronic document signing by the personal data subject is established by matching the following information: Last name, first name, patronymic (if applicable), the verification code used for signing, the Operator's receipt of information about the date and time the code was sent to the phone number or email address specified by the subject, and the phone number or email address specified by the subject.
3.6.5 The personal data subject bears all risks of adverse consequences resulting from transferring their SIM card (enabling use of their specified phone number) or email account access to third parties, including risks associated with fraudulent or unlawful actions by third parties who gain access to such information.
3.6.6 The Organization may engage third parties to process personal data with the subject's consent, unless otherwise prohibited by federal law, under a data processing agreement (hereinafter referred to as the "Operator's Instruction"). The processor must comply with the processing principles and purposes set forth in this Policy and Federal Law "On Personal Data". The Operator's Instruction must specify: (1) the processing activities to be performed, (2) the processing purposes, (3) confidentiality and security obligations, and (4) protection requirements in accordance with Article 19 of the Federal Law "On Personal Data".3.7. Methods of PD Processing

3.7 Methods of Personal Data Processing

3.7.1 Personal data is processed through both automated and non-automated (mixed) processing methods.
3.7.2 Cross-border transfer of personal data is not performed.

3.8 List of Operations Performed with Personal Data

3.8.1 Processing of personal data includes collection, systematization, accumulation, storage, updating (correction, modification), use, transfer (disclosure, access provision), blocking, deletion, destruction of personal data, and error correction.

3.9 Rights of Personal Data Subjects

3.9.1 Personal data subjects have the right to obtain information concerning the processing of their personal data, including:

- Confirmation of personal data processing by the operator;
- Legal grounds and purposes of personal data processing;
- Processing purposes and methods employed by the operator;
- Name and location of the operator, information about persons (except the operator's employees) who have access to personal data or to whom personal data may be disclosed under an agreement with the operator or pursuant to federal law;
- Personal data being processed that relates to the respective data subject, and its source, unless otherwise provided by federal law;
- Processing periods, including storage periods;
- Procedure for exercising rights granted by the Federal Law "On Personal Data";
- Name or full name and address of the entity processing personal data on behalf of the operator, if such processing is or will be assigned;
- Other information stipulated by the Federal Law "On Personal Data" or other federal laws.

3.9.2 The data subject's right to access their personal data may be restricted in accordance with federal laws, particularly when such access violates the rights and legitimate interests of third parties.

3.10 Personal Data Processing Procedure

3.10.1 Sources of personal data:

The personal data subject;
The legal representative of the personal data subject.

3.10.2 The Organization is prohibited from collecting and processing personal data concerning a subject's race, ethnicity, political views, religious or philosophical beliefs, or intimate life.

3.10.3 When using forms available on the website of the " Finopolis Forum of Innovative Financial Technologies" (October 8-10, 2025) at https://finopolis.ru/ru to collect personal data:

The personal data subject must be provided unobstructed access to review this Personal Data Processing and Protection Policy and the Rules for Using the Information Resource of the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025);
Personal data is only processed after obtaining the subject's consent by checking the appropriate box in the registration form on the Forum's website.
3.10.4 The Organization collects personal data directly from the subject or their representative only after obtaining consent, unless otherwise provided by Russian law.

3.10.5 Personal data may only be processed for the purposes specified in Section 3.2 of this Policy.

3.10.6 Personal data is processed and stored in the information system of the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025).

3.10.7 Users of the personal data information system are prohibited from recording or storing personal data on external (removable) media.

3.10.8 When making decisions affecting a data subject's interests, the Organization may not rely solely on automated processing of personal data.

3.10.9 When transferring personal data, the Organization must:

Not disclose personal data to third parties without consent, except when necessary to prevent threats to life and health or as required by federal laws;
Notify recipients that the data may only be used for the specified purposes and require confirmation of compliance.
3.10.10 If unlawful processing is detected, the Organization must rectify violations. If rectification is impossible, the Organization must destroy the personal data within 3 (three) business days of detection.

3.10.11 The Organization must notify the data subject about rectification or destruction of personal data, and if the request came from an authorized data protection authority, notify that authority as well.

3.10.12 Personal data is destroyed when:

- The processing purposes have been achieved;
- The data subject withdraws consent for processing.

3.11 Updating, Correction, Deletion, and Destruction of Personal Data; Responses to Data Subject Access Requests

3.11.1 If inaccuracies in personal data or unlawful processing are confirmed, the Operator shall update the personal data and cease processing.

3.11.2 If a Data Subject (or an authorized body) identifies inaccurate personal data and/or unlawful processing, they may submit a request stating:

"Personal data is inaccurate" and/or
"Processing of personal data is unlawful",
along with the Data Subject's last name and details of the incorrect information.
3.11.3 A Data Subject may withdraw consent either:

In person, or
By submitting a written request containing their last name, first name, patronymic (if applicable), date of birth, and place of birth.
3.11.4 Written requests from Data Subjects may be submitted via:

Email (including as an electronically signed document using a basic or enhanced qualified electronic signature) to: info@finopolis.ru;
Postal mail to:
101000, Moscow, Potapovsky Lane, Building 5, Structure 2.

4. PROTECTION OF PERSONAL DATA

4.1 Key Measures for Ensuring Personal Data Security

4.1.1 The security of personal data during processing is ensured by preventing unauthorized (including accidental) access that could lead to destruction, alteration, blocking, copying, dissemination, or other unlawful actions with personal data.

4.1.2 Security measures are determined based on the level of protection required for personal data in the information system (ISPD), taking into account potential threats to the vital interests of individuals, society, and the state.

4.1.3 The following measures are implemented to comply with the Federal Law "On Personal Data":

- Obtaining consent from data subjects for processing their personal data, unless otherwise provided by Russian law;
- Appointing a responsible officer for organizing personal data processing;
- Appointing a responsible officer for ensuring personal data security;
- Adopting internal policies and regulations on personal data processing and protection;
- Implementing legal, organizational, and technical safeguards in accordance with personal data protection requirements;
- Conducting internal audits to verify compliance with the Federal Law "On Personal Data," related regulations, organizational policies, and internal data protection rules;
- Assessing potential harm to data subjects in case of violations of the Federal Law "On Personal Data";
- Training personnel involved in data processing on Russian data protection laws, security requirements, and organizational policies;
- Implementing measures to recover personal data modified or destroyed due to unauthorized access;
- Prohibiting the transmission of personal data via open communication channels outside controlled zones without appropriate security measures.

4.2 Personal Data Protection Measures

4.2.1 Access control measures are implemented for personal data processed within the information system of the Finopolis Forum of Innovative Financial Technologies (October 8–10, 2025).

4.2.2 Access to automated workstations is secured via unique login credentials for each user. Unauthorized access prevention is enforced through dedicated security tools.

5. ORGANIZATION OF PD PROTECTION

5.1 Personal Data Protection Framework

5.1 The implementation of personal data protection measures shall adhere to the following core principles:

- Holistic approach to building the personal data protection system;
- Use of security measures that do not significantly degrade the core functionality of the personal data information system;
- Continuous monitoring of the effectiveness of personal data protection measures.

5.2 Management of Protection Measures

5.2 The Personal Data Protection Officer shall directly oversee the development, operation, and enhancement of the protection system for the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025).

5.3 Implementation Responsibilities

5.3 The Personal Data Protection Officer shall be responsible for:

- Deploying, configuring, and commissioning software and hardware protection tools;
- Developing organizational protection measures;
- Monitoring the operational status of the protection system within the personal data information system of the Finopolis Forum of Innovative Financial Technologies (October 8-10, 2025).

6. COMPLIANCE MONITORING WITH RUSSIAN FEDERATION LEGISLATION ON PERSONAL DATA PROCESSING

6.1 Monitoring compliance with the requirements of Russian Federation legislation in the field of personal data is conducted for the following purposes:

- Verifying compliance of personal data processing with these requirements;
- Verifying compliance of applied personal data protection measures with these requirements;
- Implementing measures to identify and prevent violations of these requirements;
- Detecting potential personal data leakage channels;
- Eliminating consequences of potential violations.

- Responsibility for monitoring compliance with Russian Federation legislation on personal data processing is assigned to the officer responsible for organizing personal data processing.

7. SECURITY STATUS MONITORING OF PERSONAL DATA

7.1 Monitoring the security status of personal data is performed to:

Timely identify and prevent unauthorized access to personal data;
Detect and prevent deliberate software and technical impacts on personal data;
Assess the effectiveness of protection measures.
7.2 The monitoring involves:

Verifying compliance with legal acts and regulations on personal data protection;
Evaluating the adequacy and effectiveness of implemented protection measures.
7.3 Based on monitoring results:

The effectiveness of implemented protection measures is assessed;
Protection is considered effective if measures comply with established requirements and standards;
Non-compliance with established personal data protection requirements and standards constitutes a violation;
Results of periodic monitoring analyses, identified violation causes, and remediation recommendations serve as the basis for appropriate decision-making.