Approved by
"APRICOT CAPITAL"
closed joint stock company
Executive Director's decision
No. AC NQ 20/11/2024-1of November 20, 2024

Vachik Gevorgyan

"APRICOT CAPITAL"
CLOSED JOINT STOCK COMPANY

PERSONAL DATA PROTECTION POLICY

YEREVAN 2024

The purpose of this policy is to ensure the legality of the Company's activities in personal data protection, establish procedures that safeguard personal data, manage the risk of violations, and maximize the protection of individuals' personal data.

1. THE SCOPE OF THIS POLICY REGULATION

1.1. This policy defines the grounds and limits for the processing, use, transfer, and storage of personal data of Clients and representatives of partner organizations by Apricot Capital Closed Joint Stock Company (hereinafter referred to as the "Company").

1.2. For the purposes of this policy, the applicable legislation includes the laws of the Republic of Armenia, particularly the Constitution of the Republic of Armenia, the Law "On Protection of Personal Data", the Law "On Combating Money Laundering and Financing of Terrorism", the Law "On the Securities Market", as well as other relevant laws, by-laws, and international agreements ratified by the Republic of Armenia.

1.3. The regulations of other internal legal acts of the Company related to personal data protection are applicable, unless specifically addressed by this Policy. These internal legal acts include, but are not limited to, the Regulations on the Storage of Service Information, the Information Security Policy, the Procedure for Accounting Information Resources, and the Emergency Action Plan. In case of any conflict with other internal legal acts related to personal data, this Policy shall prevail.

2. Key Concepts Used in Policy

2.1. ***Data Subject:*** An identifiable natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
For the purposes of this Policy, a Data Subject is any natural person whose right to the protection of personal data is or may be affected in the course of the Company's activities, including but not limited to:

- Clients, including representatives of legal entity Clients, who use the investment services and/or non-core services provided by the Company, or who have applied to the Company to use such services;
- Suppliers;
- Representatives of other partner organizations of the Company, as a result of cooperation arising from its activities.

2.2. ***Personal Data Processor:*** "APRICOT CAPITAL" Closed Joint Stock Company.

2.3. ***Cookie:*** A small file stored on a user's device by a website to collect and store information for purposes such as user identification, personalization, analytics, advertising, and other functions.

2.4. Concepts not defined in this policy shall be used in accordance with the meanings provided in the **RA Law "On Personal Data Protection"** and **the RA Law "On Securities Market".**

3. Principles of Personal Data Protection

3.1. **Lawfulness:** The Company collects and processes personal data in accordance with applicable law. The Company only collects personal data that is necessary and relevant to its legitimate purposes.

3.2. **Proportionality:** Data processing is carried out for legitimate purposes and to the extent that it is appropriate, necessary, and proportionate to achieve those purposes.
The Company retains personal data only for as long as it is necessary for its normal activities. Once the data are no longer necessary to fulfill the legitimate purposes of the Company, they are destroyed, except when retention is required by applicable regulatory legal acts. In particular, but not limited to, **the Law "On Combating Money Laundering and Terrorism Financing"**, which mandates the retention of relevant information for reporting purposes in the fight against money laundering and terrorist financing, the Company is required to retain such information, regardless of whether the transaction or business relationship continues or ends.

3.3. **Reliability:** The company takes measures to ensure that the data processed is complete, accurate, clear, and as up-to-date as possible.

3.4. **Minimal Involvement of Data Subjects:** Personal data is processed in accordance with the principle of minimal involvement of Data Subjects, meaning that, whenever possible, the data collector obtains the data independently, without unnecessarily involving the Data Subject.

4. Basis, Procedure, and Volume of Data Collection and Processing

4.1. The Company processes personal data to achieve specific objectives related to its activities, such as opening a brokerage account for the Client, ensuring the proper provision of services, fulfilling contractual obligations with the Data Subject, complying with legal obligations, meeting supervisory requirements, detecting fraud, and other related purposes. Furthermore, the data is processed in the minimum volume necessary and stored only for the period required to achieve a legitimate goal. After that, it is archived for the period specified by the legislation of the Republic of Armenia and eventually destroyed.

4.2. The Company exercises due diligence in the collection and processing of special categories of personal data, considering their sensitive nature and the potential for significant interference with individuals' rights.

4.3. In the context of providing investment services, personal data such as passport details, place of residence and registration, email address, phone number, registration data with the relevant tax authority, bank account number, securities account number, and data on affiliated persons may be requested from individual Clients, as well as from representatives of legal entity Clients. Additionally, any conversation with the Company related to the provision of services may be recorded and will remain the property of the Company.

4.4. The personal data specified in clause 4.3 of this Policy, along with other legitimate purposes, are collected to achieve the following objectives outlined by legislation:

- Conducting **risk-based due diligence** on the Client
- Classifying the Client as **professional or non-professional**,
- Classifying a professional Client as a **qualified Client,**
- Ensuring compliance with the requirements of the RA Law on **"Combating Money Laundering and Financing of Terrorism"**,
- Ensuring the proper execution of the Client's order.

4.5. To achieve the aforementioned goals, the following data are also collected:

- **Information on the Client's financial situation** (e.g., sources and amount of regular income, total assets, and liquid assets),
- **Information on investment objectives** (e.g., risk preferences and scope, purpose of the investment),
  Information on the Client's knowledge and experience in investment activities (e.g., familiarity with investment services, securities transactions, and securities with which the Client has been involved).

4.6. The data specified in clause 4.5 of this policy are considered personal data to the extent that they enable the identification of an individual.

4.7. Personal data may be collected verbally, in writing, electronically, or through other means.

4.8. The personal data provided by the Client is assumed to be accurate. The Company relies on this data unless it is aware, or should be aware, that the information is outdated, inaccurate, or incomplete.

4.9. When creating an account on the Company's website or application, the Client is asked to provide the data specified in paragraphs 4.3 and 4.5. Additionally, a series of actions are taken to identify the Client, including the collection of biometric data, which also serves the purpose of ensuring proper service delivery.

4.10. The Company's website may also use cookies. To prevent the unwanted collection of personal data, users are given the option to adjust their cookie settings according to their preferences.

4.11. The web server of the Company's website may automatically collect user data, such as IP address, the referring website, access date, duration, and other related information.

4.12. By using the Company's investment services and applying for their provision, the Client gives consent to the Company to process their personal data in accordance with this policy.

4.13. If the Client provides the Company with personal data of third parties, the Company assumes that the Client has obtained the third party's consent for the Company to process their data. The Client is responsible for any consequences resulting from the failure to obtain such consent and agrees to compensate the Company for any losses incurred due to this failure.

4.14. The Client may refuse to provide data; however, in such cases, the Company may be unable to provide services to the Client or perform certain actions required for service delivery. If the Client refuses to provide data or provides incomplete information, the Company will inform the Client of the potential consequences.

4.15. To ensure the performance of contracts between the Company and its suppliers, personal data may be requested from suppliers. The processing of such data is carried out in accordance with this Policy, the contract with the supplier, and applicable legislation.

4.16. In the course of its normal operations, service provision, Client orders, and other lawful activities, the Company may request personal data from its partners. The Company is entitled to transfer its partners' personal data to Clients as necessary for Clients to exercise their rights under applicable law.

4.17. The Company does not collect personally identifiable data without consent, except for data processed in accordance with this Policy, or when required by regulatory legal acts or requested by public authorities.

5. Transfer of Personal Data to Third Parties

5.1. In cases not specified in Section 4 of this Policy, the Company is entitled to transfer the personal data of individuals to third parties if:
a) The Data Subject has given consent to transfer the data to third parties, or
b) The need to transfer the data to third parties arises from the requirements of regulatory legal acts or public authorities, which need such data to exercise their powers established by law.

5.2. By becoming a Client and using investment services, the Client agrees and gives consent that the information provided in accordance with clauses 4.3 and 4.5, as well as any other personal data submitted for the purpose of providing investment services, may be transferred by the Company to third parties. This transfer may occur if necessary for the proper provision of services, including, but not limited to, intermediary financial organizations, financial institutions serving the other party in the Client's transaction, and individuals or organizations providing legal, accounting, advisory, or representative services to the Company or performing work on its behalf.

5.3. To ensure the proper provision of services, the Company utilizes the services and tools of intermediary financial and other organizations. Personal data of Clients may be transferred to these organizations as part of service delivery. Additionally, personal data of third parties may be transferred to the Company's partners if necessary for the proper provision of services or for other legitimate purposes.

5.4. The Company conducts due diligence, to the extent possible, and takes appropriate measures to ensure that third parties are capable of protecting the data it transfers. Personal data may be transferred to another country if that country is included in the list officially published by the authorized personal data protection authority, or in cases required by law.

5.5. Subject to the proper execution of the actions specified in paragraph 5.3 of this Policy, the Company assumes that third parties adequately protect the data.

5.6. The Company is not responsible for the effectiveness of data protection measures taken by third parties, except when it knew, prior to transferring the data, that the third party was not ensuring adequate protection of personal data.

5.7. Under regulatory legal acts or requests from public authorities, the Company may transfer personal data without notifying the Data Subject or obtaining their consent. The Company is not responsible for the legality of such legislative provisions or requests from public authorities.

6. Ensuring the Security of Personal Data, Risk Assessment, and Monitoring

6.1. To ensure the security of personal data processing, as well as risk assessment and monitoring, the Company is obligated to take measures that ensure compliance with this Policy and other internal legal acts related to the protection of personal data.

6.2. When processing data, the Company is obligated to comply with applicable legislation. It is also required to monitor the activities of the Company and its employees to ensure the protection of personal data from unlawful destruction, accidental loss, unauthorized dissemination, alteration, copying, misuse, and other forms of unauthorized processing.

6.3. The protection of collected personal data is ensured in accordance with the Company's information security policy. Security measures for personal data must be proportionate to the risks associated with data processing.

6.4. To ensure the protection of personal data, the Company takes the following measures:

6.4.1. The Company ensures proper technical measures, including but not limited to antivirus protection, encryption, and other relevant security protocols.

6.4.2. The Company may enter into confidentiality agreements with employees, conduct regular audits of personal data flows, perform risk assessments, and implement other necessary safeguards.

6.4.3. The Company organizes organizational measures outlined in Chapter 7 of this Policy, including training programs, to ensure employee awareness and compliance with personal data protection standards.

6.5. This policy is reviewed at least every two years, taking into account developments in the data protection sector and periodic legislative changes in the field of personal data.

7. Employee Responsibilities and Employee Training

7.1. Recognizing the importance of proper employee training to achieve the goals of personal data protection, the Company takes measures to educate employees handling personal data and implements relevant training and informational programs.

7.2. The Company's internal regulations may require mandatory participation in the programs outlined in clause 7.1 for employees who handle personal data, along with additional sector-specific qualification requirements.

7.3. Employees of the Company are required to comply with the provisions of this Policy, other internal regulations, and applicable legislation.

7.4. Employees may collect and process personal data only within the scope of their job duties.

7.5. The Company's employees are prohibited from accessing data that is not necessary for the performance of their job duties.

7.6. The Company's employees are prohibited from copying, modifying, or transferring data in their possession, except when such actions are required as part of their job duties.

7.7. In the event of a violation of this Policy or other internal legal acts of the Company, employees may be subject to disciplinary action, the procedure and extent of which are determined by the agreement between the Company and the employee.

7.7. The procedure for storing work related information is regulated in detail by the Company's Regulation on Protection of Work Related Information.

8. Rights of Data Subjects and Appeal Procedure

8.1. The Data Subject has, among other rights:

8.1.1. The right to receive information about his/her personal data, the processing of the data, the grounds and purposes for processing, the data processor, its location, as well as the categories of persons to whom the personal data may be transferred.

8.1.2. The right to withdraw his/her consent, where applicable, in the manner prescribed by applicable law.

8.1.3. The right to access his/her personal data and to request the data processor to correct, block, or destroy personal data if such data is incomplete, inaccurate, outdated, unlawfully obtained, or no longer necessary for the purposes of processing. However, the destruction of personal data may not be carried out if it contradicts the provisions of applicable law.

8.1.4. In case of suspicion that personal data has been corrected, blocked, or destroyed by the processor, the Data Subject has the right to apply to the authorized body for personal data protection to clarify whether his/her personal data has been altered, blocked, or destroyed and to request relevant information.

8.1.5. The right to apply to the authorized body for personal data protection or to the courts in the event of a violation of his/her rights in the field of personal data protection.

8.2. To exercise the rights set forth in Clause 8.1 of this Policy, the Data Subject has the right to contact the Company through the following communication channels:

Email: info@apricotcapital.am
Phone numbers: +37460707111, +37498222881

Or visit the Company's office at 10 Vazgen Sargsyan Street, 2nd Floor, 110, Yerevan, Republic of Armenia.