

**FINHUB GLOBAL LTD.  
PERSONAL DATA COLLECTION AND PROCESSING POLICY**

Approved by  
Director

---

Astana, 2023

## **CONTENT**

1. GENERAL PROVISIONS
2. DEFINITIONS
3. DATA PROCESSING PRINCIPLES
4. PURPOSE OF DATA COLLECTION AND PROCESSING
5. RIGHTS OF PERSONAL DATA SUBJECTS
6. CLASSIFICATION OF PERSONAL DATA AND DATA SUBJECTS
7. CONSENT TO THE COLLECTION AND PROCESSING OF DATA
8. NOTIFICATION OF PERSONAL DATA SUBJECT
9. RECORD KEEPING OF PERSONAL DATA PROCESSING
10. COMMISSIONER'S NOTIFICATION PROCEDURE

## 1. GENERAL PROVISIONS

1.1. This Personal Data Collection and Processing Policy (the "PDCP Policy") has been developed by FINHUB GLOBAL LTD (the "Company") in accordance with the regulatory rules of the Astana International Financial Centre (the "AIFC"), the applicable laws of the Republic of Kazakhstan and international standards.

1.2. The purpose of this PDCP Policy is to define the principles and procedures for collecting and processing data about Clients, implementing modern protection standards and mechanisms to prevent personal data leaks.

1.3. The provisions of this PDCP Policy apply to all employees, branches, representative offices and subsidiaries of the Company.

1.4. This PDCP Policy comes into effect from the moment of its signing.

## 2. DEFINITIONS

2.1. The following definitions are used in this PDCP Policy:

“**AFSA**” means the Astana Financial Services Authority.

“**AIFC**” means the Astana International Financial Centre.

“**AIFC Rules**” means the rules contained in the Handbook of Rules and Guidance produced by the AFSA as from time to time in force (as varied by any waiver, dispensations or individual guidance granted by the AFSA and applicable to Company).

“**Commissioner**” means an individual appointed as a Commissioner and responsible for the development and implementation of personal data protection mechanisms, as well as compliance with current legislation on the collection and processing of Personal Data;

“**Personal Data (PD)**” means any information relating to a certain individual or an individual identifiable based on such information recorded on electronic, paper and (or) other tangible media;

“**Personal Data Subject (PD Subjects)**” means an individual directly or indirectly identified or identifiable based on the Personal Data;

“**Sensitive Personal Data (SPD)**” means the Personal Data revealing or concerning, directly or indirectly, racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade union membership, and health or private life.

## 3. DATA PROCESSING PRINCIPLES

3.1. When collecting and processing PD, the Company adheres to the following principles:

- 1) fairness, legality, reliability and transparency;
- 2) data minimization;
- 3) accuracy;
- 4) integrity and confidentiality;

5) accountability.

3.2. The Company collects and processes data for lawful, explicit and understandable purposes. In order to collect and process data, the Company must obtain written consent from the Client.

3.3. The Company aims to use the minimum amount of PD necessary to accomplish the tasks at hand.

3.4. PD must be accurate, complete and not misleading. If any inaccuracies or incompleteness of PD are identified, the Company must make the necessary corrections as soon as possible.

3.5. The Company must store PD in a secure place and ensure their safety and confidentiality, as well as take all necessary measures to prevent data leakage.

3.6. The company must create and maintain records of its data collection and processing operations. The company must also notify the data Commissioner of all data collection and processing operations conducted as required by the AIFC Rules.

3.7. PD is kept for no longer than is necessary for the purposes for which it was collected and must be destroyed after the purpose of PD storage has been fulfilled.

#### **4. PURPOSE OF DATA COLLECTION AND PROCESSING**

4.1. The Company collects and processes data for the following purposes:

- 1) adherence to the Terms of Business (the "Agreement");
- 2) provision of services to the Client in accordance with the provisions of the Agreement;
- 3) biometric identification of the Client when establishing remote business relationships and when providing electronic services;
- 4) proper verification of the Client by the Company in accordance with the requirements for financial monitoring entities;
- 5) internal control and accounting of services provided by the Company, as well as conducting internal audits and investigations;
- 6) ensuring compliance with applicable regulatory norms applicable to the Company and its affiliated persons;
- 7) conducting an analysis of the services provided by the Company to improve the quality of service, providing clients with information materials using any available method;
- 8) taking measures to reduce the risk of unauthorized transactions in accordance with the legislation on AML/CFT;
- 9) provision of reporting by the Company to authorized bodies of the AIFC and the Republic of Kazakhstan in accordance with the requirements of the legislation;
- 10) compliance by the Company with requirements for the collection and processing of data provided by applicable legislation;

11) implementation of judicial and non-judicial protection of the Company's rights in case of disputes related to the performance of obligations provided for in the Agreement, including disputes with third parties regarding the provision of the Company's services;

12) exchange of information in connection with the consideration of requests, complaints, and suggestions from the Client and providing responses to them;

13) possible assignment of rights under the Agreement;

14) Provision of PD to affiliated persons of the Company and third parties for the purpose of cooperation in the field of information technologies and integration of information assets for the provision of services using information technologies.

4.2. The Company collects and processes data throughout the entire period of business relations with the Client and stores personal data on any media for 6 (six) years after the termination of relations.

## **5. RIGHTS OF PERSONAL DATA SUBJECTS**

5.1. The PD Subject has the right to:

- 1) request information from the Company about the data collected and processed.
- 2) correct, supplement, restrict and delete their data;
- 3) access their PD, including information that the Company has collected about them;
- 4) file a complaint with regulatory authorities.

## **6. CLASSIFICATION OF PERSONAL DATA AND DATA SUBJECTS**

6.1. The company distinguishes between Personal Data (PD) and Sensitive Personal Data (SPD).

6.2. The company distinguishes the following types of PD Subjects:

- 1) users of the Company's website;
- 2) individuals who wish to join the Agreement;
- 3) the Company's Client's and their representatives;
- 4) the Company's employees and their close relatives;
- 5) individuals with whom the Company has concluded a civil law contract;
- 6) individuals who are part of the Company's management;
- 7) individuals whose PD is publicly available, and their processing does not violate their right to the protection of personal data;
- 9) affiliated persons of the company;
- 10) other individuals who have given written consent to the collection and processing of PD.

## **7. CONSENT TO THE COLLECTION AND PROCESSING OF DATA**

7.1. The Company, in accordance with the requirements of applicable laws, ensures obtaining written consent for the collection and processing of PD of PD Subjects.

7.2. The Company requests consent for the following actions:

- 1) collection and processing of PD on any media;
- 2) disclosure of PD to affiliated companies, third parties, when such action is necessary in accordance with the requirements of applicable laws or for the performance of obligations under contracts with third parties. In this case, the Company undertakes to require the confidentiality of the transferred PD; and
- 3) cross-border transfer of PD, including to countries that are not listed in the jurisdiction with an adequate level of protection, established by the [Rules for the Protection of Personal Data of the AIFC dated January 22, 2018](#).

## **8. NOTIFICATION OF PERSONAL DATA SUBJECT**

8.1. Unless the Company reasonably believes that such information is already known to the PD Subject, the Company shall promptly provide the PD Subject with the following information upon the collection and processing of PD:

- 1) information identifying the Company;
- 2) purposes for which the Company is collecting and processing PD;
- 3) information necessary for fair processing of Personal Data, including:
  - Recipients of PD or categories of such recipients;
  - an indication of whether the requested information is mandatory or optional;
  - information as to whether PD will be used for marketing purposes.

8.2. Notification of the information provided in Clause 8.1 shall be made through the Company's website or any other available means.

## **9. RECORD KEEPING OF PERSONAL DATA PROCESSING**

9.1. The company keeps records of operations related to the processing of personal data that it has completed or performed on its behalf, including:

- 1) a description of operations related to the processing of personal data;
- 2) an explanation of the purposes for which personal data is collected and processed;
- 3) a list of jurisdictions to which the company transfers or will transfer personal data, as well as information on the adequacy of the level of protection in these jurisdictions.

## **10. COMMISSIONER'S NOTIFICATION PROCEDURE**

10.1. In accordance with the AIFC Rules, the Company is required to notify the Commissioner of the details of the following Personal Data processing operations that have been or will be carried out by the Company or on its behalf:

- 1) any operation involving the processing of SPD (or a set of such operations);
- 2) the details of those personal data processing operations required by the AIFC Rules;
- 3) about changes in operations.

10.2. The notification to the Commissioner must contain the information specified in paragraph 9.1.

10.3. Notification of data processing operations must be sent to the Commissioner no later than 14 (fourteen) days after the start of the operation. In the event that operations continue for more than one year from the date of notification, notification is sent every year on the date of the first notification.

10.4. Notification of changes in data processing operations must be sent to the Commissioner no later than 14 (fourteen) days after the changes.

## **11. FINAL PROVISIONS**

11.1. Responsibility for compliance with the provisions of this PDCP Policy lies with all Company employees who have access to personal data as part of their duties.

11.2. In cases where the provisions of this PDCP Policy do not regulate the issue, the provisions of other internal regulatory documents of the Company, the regulatory rules of the AIFC and the legislation of the Republic of Kazakhstan shall apply.