



FINHUB GLOBAL LTD.

PERSONAL DATA COLLECTION AND PROCESSING POLICY

ПОЛИТИКА СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Version 2.0 — effective from 01 September 2026
Редакция 2.0 — действует с 01 сентября 2026 года

Astana, 2026 / Астана, 2026

Legal entity <i>Юридическое лицо</i>	FINHUB GLOBAL LTD, BIN 240540900142
AFSA Licence <i>Лицензия АФСА</i>	No. AFSA-A-LA-2024-0017 dated 11 July 2024 <i>№ AFSA-A-LA-2024-0017 от 11 июля 2024 г.</i>
Registered office <i>Юридический адрес</i>	Z05T8M, Republic of Kazakhstan, Astana, Yesil District, 1 Heydar Aliyev Street, premises 1 <i>Z05T8M, Республика Казахстан, г. Астана, район Есиль, ул. Гейдара Алиева, 1, помещение 1</i>
Version / effective date <i>Редакция / дата вступления</i>	Version 2.0 — effective from 01 September 2026 <i>Редакция 2.0 — действует с 01 сентября 2026 года</i>
Approved by <i>Утверждено</i>	Director, FINHUB GLOBAL LTD <i>Директором FINHUB GLOBAL LTD</i>

1. General Provisions

1. Общие положения

1.1. This Personal Data Collection and Processing Policy (the “Policy”) has been developed by FINHUB GLOBAL LTD (the “Company”) in accordance with the AIFC Data Protection Regulations (as amended, in force from 1 April 2025), the AIFC Data Protection Rules, other applicable acts of the Astana International Financial Centre (the “AIFC”) and guidance of the Astana Financial Services Authority (the “AFSA”), the applicable laws of the Republic of Kazakhstan, and international data protection standards.

1.1. Настоящая Политика сбора и обработки персональных данных (далее — «Политика») разработана компанией FINHUB GLOBAL LTD (далее — «Компания») в соответствии с AIFC Data Protection Regulations (в редакции, действующей с 1 апреля 2025 года), AIFC Data Protection Rules, иными применимыми актами Международного финансового центра «Астана» (далее — «МФЦА») и руководствами Комитета МФЦА по регулированию финансовых услуг (далее — «АФСА»), применимым законодательством Республики Казахстан и международными стандартами защиты данных.

1.2. The purpose of this Policy is to define the principles, roles and procedures under which the Company collects and processes Personal Data of Clients and other Data Subjects, and to implement modern protection standards and mechanisms preventing Personal Data leaks.

1.2. Целью настоящей Политики является определение принципов, ролей и процедур, в соответствии с которыми Компания собирает и обрабатывает персональные данные Клиентов и иных субъектов данных, а также внедрение современных стандартов и механизмов защиты, предотвращающих утечки персональных данных.

1.3. This Policy applies to all employees, branches, representative offices and subsidiaries of the Company, and to all processing operations carried out by the Company or on its behalf.

1.3. Действие настоящей Политики распространяется на всех работников, филиалы, представительства и дочерние организации Компании, а также на все операции обработки, осуществляемые Компанией или от её имени.

1.4. This Policy is read together with the Company's Regulations for the Provision of Brokerage Services on the Securities Market (the "Client Agreement"), the Data Protection Notice published on the Company's website, and the Company's internal information security documents. This Policy (Version 2.0) comes into effect and is applied from 1 July 2026 and supersedes the previous version.

1.4. Настоящая Политика применяется совместно с Регламентом оказания брокерских услуг на рынке ценных бумаг (далее — «Клиентское соглашение»), Уведомлением о защите данных, размещённым на веб-сайте Компании, и внутренними документами Компании по информационной безопасности. Настоящая Политика (редакция 2.0) вступает в силу и применяется с 1 июля 2026 года и заменяет предыдущую редакцию.

2. Definitions

2. Определения

2.1. In this Policy the following definitions apply:

2.1. В настоящей Политике используются следующие определения:

"AFSA" means the Astana Financial Services Authority.

«АФСА» означает Комитет МФЦА по регулированию финансовых услуг (Astana Financial Services Authority).

"AIFC" means the Astana International Financial Centre.

«МФЦА» означает Международный финансовый центр «Астана».

"AIFC Data Protection Regulations" and "AIFC Data Protection Rules" mean, respectively, the AIFC Data Protection Regulations and the AIFC Data Protection Rules, as in force from time to time.

«AIFC Data Protection Regulations» и «AIFC Data Protection Rules» означают соответственно AIFC Data Protection Regulations и AIFC Data Protection Rules в действующей на соответствующий момент редакции.

"Commissioner" means the Commissioner of Data Protection of the AIFC.

«Комиссар» означает Комиссара по защите данных МФЦА.

"Client" means a natural or legal person who has acceded to, or is applying to accede to, the Client Agreement, and includes such Client's representatives, directors and beneficial owners.

«Клиент» означает физическое или юридическое лицо, присоединившееся или намеревающееся присоединиться к Клиентскому соглашению, включая его представителей, руководителей и бенефициарных собственников.

"Data Controller" means the person who, alone or jointly, determines the purposes and means of Processing Personal Data. The Company is a Data Controller regulated by the AFSA (Category 1 under the AIFC Data Protection Rules).

«Контролёр данных» означает лицо, которое единолично или совместно определяет цели и средства обработки персональных данных. Компания является контролёром данных, регулируемым АФСА (Категория 1 согласно AIFC Data Protection Rules).

“Data Processor” means a person who Processes Personal Data on behalf of, and on the documented instructions of, a Data Controller.

«Обработчик данных» означает лицо, обрабатывающее персональные данные от имени и по документированным инструкциям контролёра данных.

“Personal Data (PD)” means any information relating to an identified or identifiable natural person, recorded on electronic, paper or other tangible media.

«Персональные данные (PD)» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу, зафиксированную на электронных, бумажных или иных материальных носителях.

“Personal Data Subject (Data Subject)” means a natural person who is directly or indirectly identified or identifiable on the basis of Personal Data.

«Субъект персональных данных (субъект данных)» означает физическое лицо, прямо или косвенно идентифицированное или идентифицируемое на основании персональных данных.

“Sensitive Personal Data (SPD)” means 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, health, private life, and – for the avoidance of doubt – biometric data processed for the purpose of uniquely identifying a natural person.

«Чувствительные персональные данные (SPD)» означают персональные данные, раскрывающие или касающиеся, прямо или косвенно, расового или этнического происхождения, социального происхождения, политической принадлежности или взглядов, религиозных или философских убеждений, судимости, членства в профсоюзах, состояния здоровья, частной жизни, а также — во избежание сомнений — биометрические данные, обрабатываемые в целях уникальной идентификации физического лица.

“Biometric Data” means Personal Data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person (in particular, a facial image and its comparison with an identity document) which allow or confirm the unique identification of that person.

«Биометрические данные» означают персональные данные, полученные в результате специальной технической обработки физических или физиологических характеристик физического лица (в частности, изображения лица и его сопоставления с документом, удостоверяющим личность), которые позволяют или подтверждают уникальную идентификацию такого лица.

“Agent” means a person engaged by the Company under an agency (introducing) agreement to identify and introduce prospective Clients to the Company (for example, the Company’s introducing agent operating under the @wiqs.ru / @w-iqs.com domains).

«Агент» означает лицо, привлечённое Компанией по агентскому (представительскому) договору для поиска и представления потенциальных Клиентов Компании (например, представляющий агент Компании, использующий домены @wiqs.ru / @w-iqs.com).

“Broker” means a third-party investment firm to which the Company, acting as an introducer, introduces Clients (in particular, Axiom Invest Ltd., incorporated in the Republic of Bulgaria, UIC 206621222).

«Брокер» означает стороннюю инвестиционную компанию, которой Компания, действуя в качестве интродьюсера, представляет Клиентов (в частности, Axiom Invest Ltd., зарегистрированную в Республике Болгария, UIC 206621222).

“Shufti Pro Service” means the electronic identity-verification service used by the Company for Remote Identification, in respect of which Shufti Pro Limited acts as the Company’s Data Processor.

«Сервис Shufti Pro» означает сервис электронной проверки личности, используемый Компанией для Дистанционной идентификации, в отношении которого Shufti Pro Limited выступает обработчиком данных Компании.

“Remote Identification” means the electronic verification of a Data Subject’s identity and address, including biometric verification, carried out through the Shufti Pro Service.

«Дистанционная идентификация» означает электронную проверку личности и адреса субъекта данных, включая биометрическую проверку, осуществляемую с использованием Сервиса Shufti Pro.

“Processing” means any operation performed on Personal Data, including collection, recording, storage, use, disclosure, transfer, cross-border transfer, erasure or destruction.

«Обработка» означает любую операцию с персональными данными, включая сбор, запись, хранение, использование, раскрытие, передачу, трансграничную передачу, удаление или уничтожение.

3. Data Processing Principles

3. Принципы обработки данных

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

3.1. При сборе и обработке персональных данных Компания соблюдает следующие принципы:

1) fairness, lawfulness, reliability and transparency;

1) добросовестность, законность, достоверность и прозрачность;

2) data minimisation;

- 2) минимизация данных;
- 3) purpose limitation;
 - 3) ограничение целей;
- 4) accuracy;
 - 4) точность;
- 5) integrity and confidentiality; and
 - 5) целостность и конфиденциальность; и
- 6) accountability.
 - 6) подотчётность.

3.2. The Company collects and processes Personal Data for lawful, explicit and legitimate purposes and on a valid lawful basis established under Section 7 of this Policy. Where consent is relied upon, the Company obtains it in accordance with Section 8.

3.2. Компания собирает и обрабатывает персональные данные в законных, явно определённых и легитимных целях и при наличии действительного правового основания, установленного разделом 7 настоящей Политики. При использовании согласия Компания получает его в соответствии с разделом 8.

3.3. The Company uses the minimum amount of Personal Data necessary to accomplish the relevant purpose and, where feasible, uses pseudonymised or aggregated data.

3.3. Компания использует минимальный объём персональных данных, необходимый для достижения соответствующей цели, и по возможности использует псевдонимизированные или агрегированные данные.

3.4. Personal Data must be accurate, complete and not misleading. If any inaccuracy or incompleteness is identified, the Company makes the necessary corrections without undue delay.

3.4. Персональные данные должны быть точными, полными и не вводящими в заблуждение. При выявлении неточности или неполноты Компания вносит необходимые исправления без неоправданной задержки.

3.5. The Company stores Personal Data securely and ensures its safety and confidentiality, and takes all necessary technical and organisational measures to prevent data leakage.

3.5. Компания хранит персональные данные безопасно, обеспечивает их сохранность и конфиденциальность и принимает все необходимые технические и организационные меры для предотвращения утечки данных.

3.6. The Company creates and maintains records of its Processing operations and notifies the Commissioner of Processing operations where required by the AIFC Data Protection Regulations and Rules.

3.6. Компания создаёт и ведёт записи об операциях обработки и уведомляет Комиссара об операциях обработки в случаях, предусмотренных AIFC Data Protection Regulations и Rules.

3.7. Personal Data is kept no longer than necessary for the purposes for which it was collected and is destroyed after the retention period established in Section 19 has expired.

3.7. Персональные данные хранятся не дольше, чем это необходимо для целей, для которых они были собраны, и уничтожаются по истечении срока хранения, установленного разделом 19.

4. Roles of the Company in Personal Data Processing

4. Роли Компании при обработке персональных данных

4.1. Depending on the processing operation, the Company acts in one of the following roles:

4.1. В зависимости от операции обработки Компания выступает в одной из следующих ролей:

(a) Data Controller of its Clients' data. In the course of accepting Clients for servicing and providing brokerage and custody-arranging services, the Company determines the purposes and means of Processing and acts as an independent Data Controller regulated by the AFSA.

(a) Контролёр данных своих Клиентов. При приёме Клиентов на обслуживание и оказании брокерских услуг и услуг по организации учёта активов Компания определяет цели и средства обработки и выступает самостоятельным контролёром данных, регулируемым АФСА.

(b) Introducer (independent Controller) in relation to the Broker. Where the Company introduces a Client to a third-party Broker (Axiom Invest Ltd.), the Company and the Broker act as separate (independent) Data Controllers and do not constitute joint controllers; Personal Data is transferred only where an appropriate lawful basis exists.

(b) Интродьюсер (независимый контролёр) в отношениях с Брокером. При представлении Клиента стороннему Брокеру (Axiom Invest Ltd.) Компания и Брокер выступают как отдельные (независимые) контролёры данных и не образуют совместных контролёров; персональные данные передаются только при наличии надлежащего правового основания.

(c) Principal in relation to Agents. Where a prospective Client is introduced to the Company by an Agent (for example, Wells), the Agent and the Company each act as separate (independent) Data Controllers in respect of the Personal Data they hold; the transfer of data between them takes place only on a valid lawful basis and subject to data-protection provisions in the agency agreement.

(c) Принципал в отношениях с Агентами. Если потенциальный Клиент представлен Компании Агентом (например, Wells), Агент и Компания выступают как отдельные (независимые) контролёры данных в отношении имеющихся у них персональных данных; передача данных между ними осуществляется только при наличии действительного правового основания и с соблюдением положений о защите данных в агентском договоре.

4.2. Each party acting as an independent Controller is separately responsible for its own compliance with the data-protection regime applicable to it. The Company remains responsible for identification and due diligence carried out on its behalf, including where the Shufti Pro Service is used as a technological means.

4.2. Каждая сторона, выступающая как независимый контролёр, самостоятельно отвечает за собственное соблюдение применимого к ней режима защиты данных. Компания сохраняет ответственность за идентификацию и надлежащую проверку, проводимые от её имени, в том числе при использовании Сервиса Shufti Pro в качестве технологического средства.

4.3. The allocation of roles and lawful bases is summarised in the table below.

4.3. Распределение ролей и правовых оснований обобщено в таблице ниже.

Data flow <i>Поток данных</i>	Company's role / counterparty <i>Роль Компании / контрагент</i>	Relationship <i>Отношения</i>	Principal lawful basis <i>Основное правовое основание</i>
Client → Company <i>Клиент → Компания</i>	Data Controller <i>Контролёр данных</i>	Direct servicing <i>Прямое обслуживание</i>	Contract; legal obligation (AML/CFT); consent <i>Договор; правовая обязанность (ПОД/ФТ); согласие</i>
Agent (Wells) ↔ Company <i>Агент (Wells) ↔ Компания</i>	Both independent Controllers <i>Оба — независимые контролёры</i>	Client introduction <i>Привлечение клиентов</i>	Consent; legitimate interests <i>Согласие; законные интересы</i>
Company → Axiom (Bulgaria) <i>Компания → Аxiom (Болгария)</i>	Both independent Controllers <i>Оба — независимые контролёры</i>	Introducing, cross-border <i>Интродьюсинг, трансгранично</i>	Consent; contract; legal basis (Agreement s.11.3) <i>Согласие; договор; правовое основание (Договор, п. 11.3)</i>
Company → Shufti Pro <i>Компания → Shufti Pro</i>	Company = Controller; Shufti Pro = Processor <i>Компания — контролёр; Shufti Pro — обработчик</i>	Remote identification, biometrics, cross-border <i>Дистанционная идентификация, биометрия, трансгранично</i>	Explicit consent; legal obligation (AML/CFT) <i>Явное согласие; правовая обязанность (ПОД/ФТ)</i>

5. Purpose of Data Collection and Processing

5. Цели сбора и обработки данных

5.1. The Company collects and processes Personal Data for the following purposes:

5.1. Компания собирает и обрабатывает персональные данные в следующих целях:

- 1) accession to, and performance of, the Client Agreement and provision of the requested products and services;

1) присоединение к Клиентскому соглашению и его исполнение, а также предоставление запрошенных продуктов и услуг;

- 2) identification and Remote Identification of the Client, including biometric verification, through the Shufti Pro Service;
2) идентификация и Дистанционная идентификация Клиента, включая биометрическую проверку, через Сервис Shufti Pro;
- 3) proper client due diligence, ongoing monitoring, and screening against sanctions and politically exposed person (PEP) lists;
3) надлежащая проверка клиента, постоянный мониторинг и проверка по санкционным спискам и спискам публичных должностных лиц (PEP);
- 4) introduction of the Client to a third-party Broker where the Company acts as introducer, and the receipt of Client data from Agents who introduce Clients to the Company;
4) представление Клиента стороннему Брокеру, когда Компания действует в качестве интродьюсера, и получение данных Клиента от Агентов, представляющих Клиентов Компании;
- 5) internal control, accounting, audit and investigations in relation to services provided by the Company;
5) внутренний контроль, учёт, аудит и расследования в отношении оказываемых Компанией услуг;
- 6) compliance with applicable regulatory requirements, including AML/CFT obligations, and reporting to the authorised bodies of the AIFC and the Republic of Kazakhstan;
6) соблюдение применимых регуляторных требований, включая обязательства в области ПОД/ФТ, и представление отчётности уполномоченным органам МФЦА и Республики Казахстан;
- 7) analysis and improvement of the quality of service and, subject to consent and applicable law, provision of information materials;
7) анализ и повышение качества обслуживания и, при наличии согласия и с соблюдением применимого права, предоставление информационных материалов;
- 8) judicial and non-judicial protection of the Company's rights, and the exchange of information in connection with requests, complaints and suggestions; and
8) судебная и внесудебная защита прав Компании, а также обмен информацией в связи с запросами, жалобами и предложениями; и
- 9) possible assignment of rights under the Client Agreement, and cooperation with affiliates and third parties in the field of information technologies.
9) возможная уступка прав по Клиентскому соглашению и сотрудничество с аффилированными лицами и третьими лицами в сфере информационных технологий.

6. Categories of Personal Data and Data Subjects

6. Категории персональных данных и субъектов данных

6.1. The Company distinguishes between Personal Data (PD) and Sensitive Personal Data (SPD). Biometric Data processed for Remote Identification is treated as SPD and is subject to the enhanced conditions in Sections 7 and 10.

6.1. Компания разграничивает персональные данные (PD) и чувствительные персональные данные (SPD). Биометрические данные, обрабатываемые для Дистанционной идентификации, рассматриваются как SPD и подпадают под усиленные условия, предусмотренные разделами 7 и 10.

6.2. The categories of Personal Data processed include: identification data (name, date and place of birth, nationality, identity-document details); contact data; residential-address data; financial, account and transactional data; classification and suitability data; source-of-funds and source-of-wealth data; sanctions/PEP-screening data; and Biometric Data obtained during Remote Identification.

6.2. К обрабатываемым категориям персональных данных относятся: идентификационные данные (имя, дата и место рождения, гражданство, реквизиты документа, удостоверяющего личность); контактные данные; данные об адресе проживания; финансовые, счётные и транзакционные данные; данные о классификации и пригодности; данные об источнике средств и источнике благосостояния; данные санкционного/PEP-скрининга; и биометрические данные, полученные при Дистанционной идентификации.

6.3. The Company distinguishes the following categories of Data Subjects:

6.3. Компания различает следующие категории субъектов данных:

- 1) users of the Company's website;
1) пользователи веб-сайта Компании;
- 2) natural persons who wish to accede to the Client Agreement;
2) физические лица, желающие присоединиться к Клиентскому соглашению;
- 3) Clients and their representatives, directors and beneficial owners;
3) Клиенты и их представители, руководители и бенефициарные собственники;
- 4) employees of the Company and their close relatives;
4) работники Компании и их близкие родственники;
- 5) natural persons with whom the Company has concluded a civil-law contract;
5) физические лица, с которыми Компания заключила гражданско-правовой договор;
- 6) natural persons who are part of the Company's management;
6) физические лица, входящие в состав руководства Компании;
- 7) natural persons introduced by, or to, Agents and the Broker;
7) физические лица, представленные Агентами или Брокеру либо представленные ими;
- 8) natural persons whose Personal Data is publicly available where processing does not violate their data-protection rights; and

8) физические лица, чьи персональные данные общедоступны, если их обработка не нарушает их прав на защиту данных; и

9) other natural persons who have given consent to the collection and processing of their Personal Data.

9) иные физические лица, давшие согласие на сбор и обработку своих персональных данных.

7. Lawful Basis for Processing

7. Правовое основание обработки

7.1. The Company processes Personal Data only where at least one of the following lawful bases applies: (a) the Data Subject's consent; (b) performance of a contract with the Data Subject or steps taken at the Data Subject's request prior to entering into a contract; (c) compliance with a legal obligation of the Company, including AML/CFT obligations; (d) protection of the vital interests of a natural person; (e) performance of a task carried out in the public interest; or (f) the legitimate interests of the Company or a third party, except where overridden by the interests or fundamental rights of the Data Subject.

7.1. Компания обрабатывает персональные данные только при наличии хотя бы одного из следующих правовых оснований: (a) согласие субъекта данных; (b) исполнение договора с субъектом данных или совершение действий по его запросу до заключения договора; (c) соблюдение правовой обязанности Компании, включая обязательства в области ПОД/ФТ; (d) защита жизненно важных интересов физического лица; (e) выполнение задачи в общественных интересах; или (f) законные интересы Компании или третьего лица, за исключением случаев, когда они преобладают интересами или основными правами субъекта данных.

7.2. Sensitive Personal Data, including Biometric Data, is processed only where an enhanced condition applies, in particular: the Data Subject's explicit consent; processing necessary for compliance with the Company's obligations in the field of AML/CFT and financial-services regulation; or processing necessary for reasons of substantial public interest. Biometric Data used for Remote Identification is processed on the basis of the Data Subject's explicit consent together with the Company's legal obligation to carry out client identification.

7.2. Чувствительные персональные данные, включая биометрические, обрабатываются только при наличии усиленного условия, в частности: явного согласия субъекта данных; обработки, необходимой для соблюдения обязанностей Компании в области ПОД/ФТ и регулирования финансовых услуг; или обработки, необходимой по причинам существенного общественного интереса. Биометрические данные, используемые для Дистанционной идентификации, обрабатываются на основании явного согласия субъекта данных совместно с правовой обязанностью Компании проводить идентификацию клиента.

7.3. Explicit consent is required for the Processing of Sensitive Personal Data (including Biometric Data), for solely automated decision-making that produces legal or similarly significant effects,

and for cross-border transfers to jurisdictions that do not provide an adequate level of protection, unless another lawful basis applies.

7.3. Явное согласие требуется для обработки чувствительных персональных данных (включая биометрические), для принятия решений исключительно на основе автоматизированной обработки, влекущих правовые или аналогичные существенные последствия, а также для трансграничной передачи в юрисдикции, не обеспечивающие адекватный уровень защиты, если не применяется иное правовое основание.

8. Consent

8. Согласие

8.1. Where the Company relies on consent, such consent is a freely given, specific, informed and unambiguous indication of the Data Subject's wishes, given by a clear affirmative action. Pre-ticked boxes, silence or inactivity do not constitute consent.

8.1. Если Компания опирается на согласие, такое согласие является свободно данным, конкретным, информированным и недвусмысленным волеизъявлением субъекта данных, выраженным чётким утвердительным действием. Предварительно отмеченные поля, молчание или бездействие согласием не являются.

8.2. Where processing has multiple purposes or involves distinct categories of recipients, consent is sought separately (granularly) for each. In particular, the Company obtains separate consent for:

8.2. Если обработка имеет несколько целей или охватывает различные категории получателей, согласие запрашивается отдельно (гранулированно) по каждой из них. В частности, Компания получает отдельное согласие на:

- 1) the collection and Processing of Personal Data on any media;
1) сбор и обработку персональных данных на любых носителях;
- 2) the disclosure of Personal Data to Agents of the Company;
2) раскрытие персональных данных Агентам Компании;
- 3) the disclosure and cross-border transfer of Personal Data to the Broker (Axiom Invest Ltd., Bulgaria) where the Company acts as introducer;
3) раскрытие и трансграничную передачу персональных данных Брокеру (Axiom Invest Ltd., Болгария), когда Компания действует в качестве интродьюсера;
- 4) the Processing of Biometric Data and its cross-border transfer to the operator of the Shufti Pro Service for the purpose of Remote Identification; and
4) обработку биометрических данных и их трансграничную передачу оператору Сервиса Shufti Pro в целях Дистанционной идентификации; и
- 5) automated sanctions and PEP screening.
5) автоматизированный санкционный и PEP-скрининг.

8.3. The Data Subject has the right to withdraw consent at any time. Withdrawal does not affect the lawfulness of Processing carried out before withdrawal, and does not affect Processing that is

required for the Company's compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

8.3. Субъект данных вправе отозвать согласие в любое время. Отзыв не затрагивает законность обработки, осуществлённой до отзыва, и не затрагивает обработку, необходимую для соблюдения Компанией правовой обязанности либо для установления, осуществления или защиты правовых требований.

8.4. The consent language set out in the Application for Accession (for natural persons and for legal persons) and in the Client Agreement is aligned with this Section. Where a Client is introduced by an Agent or to the Broker, the relevant consent is obtained before the corresponding transfer takes place.

8.4. Формулировки согласия, содержащиеся в Заявлении о присоединении (для физических и юридических лиц) и в Клиентском соглашении, приведены в соответствии с настоящим разделом. Если Клиент представлен Агентом или Брокеру, соответствующее согласие получается до осуществления соответствующей передачи.

9. Recipients of Personal Data and Disclosure

9. Получатели персональных данных и раскрытие

9.1. The Company may disclose Personal Data only to the following categories of recipients and only where a lawful basis and, where required, consent exist:

9.1. Компания вправе раскрывать персональные данные только следующим категориям получателей и только при наличии правового основания и, где требуется, согласия:

- 1) affiliates of the Company and persons providing services to, or acting as processors for, the Company;
 - 1) аффилированным лицам Компании и лицам, оказывающим услуги Компании или выступающим её обработчиками;*
- 2) Agents who introduce Clients to the Company (independent Controllers);
 - 2) Агентам, представляющим Клиентов Компании (независимым контролёрам);*
- 3) the Broker to which the Company introduces Clients (independent Controller), including where located outside the AIFC;
 - 3) Брокеру, которому Компания представляет Клиентов (независимому контролёру), в том числе находящемуся за пределами МФЦА;*
- 4) the operator of the Shufti Pro Service, acting as the Company's Data Processor;
 - 4) оператору Сервиса Shufti Pro, выступающему обработчиком данных Компании;*
- 5) competent regulatory, supervisory, law-enforcement and tax authorities of the AIFC and the Republic of Kazakhstan; and
 - 5) компетентным регулирующим, надзорным, правоохрнительным и налоговым органам МФЦА и Республики Казахстан; и*

6) trading-venue operators, depositories, custodians, credit-reference and fraud-prevention agencies, and the Company's professional advisers, auditors and lawyers, where necessary for the provision of services or compliance.

б) операторам торговых площадок, депозитариям, кастодианам, бюро кредитных историй и организациям по предотвращению мошенничества, а также профессиональным консультантам, аудиторам и юристам Компании, когда это необходимо для оказания услуг или соблюдения требований.

9.2. The Company treats all information about Clients as private and confidential, including after the termination of the relationship, and ensures that its affiliates, Agents and processors do not disclose such information otherwise than as permitted by law or this Policy. Where the Company discloses Personal Data to a third party, it informs that party of the confidential nature of the information.

9.2. Компания обращается со всеми сведениями о Клиентах как с частными и конфиденциальными, в том числе после прекращения отношений, и обеспечивает, чтобы её аффилированные лица, Агенты и обработчики не раскрывали такие сведения иначе как разрешено законом или настоящей Политикой. При раскрытии персональных данных третьему лицу Компания информирует его о конфиденциальном характере сведений.

9.3. Where the Company discloses Personal Data to an Agent or to the Broker, each acting as an independent Controller, the receiving party is responsible for informing the relevant Data Subjects and for complying with the data-protection regime applicable to it; the parties provide each other with reasonable assistance in giving effect to Data Subjects' rights, in responding to security incidents, and in carrying out data-protection impact assessments.

9.3. При раскрытии Компанией персональных данных Агенту или Брокеру, каждый из которых выступает независимым контролёром, получающая сторона отвечает за информирование соответствующих субъектов данных и за соблюдение применимого к ней режима защиты данных; стороны оказывают друг другу разумное содействие в реализации прав субъектов данных, в реагировании на инциденты безопасности и в проведении оценок воздействия на защиту данных.

10. Remote Identification and Use of the Shufti Pro Service

10. Дистанционная идентификация и использование Сервиса Shufti Pro

10.1. The Company carries out Remote Identification of Data Subjects using the Shufti Pro Service. In doing so, the Company obtains a photographic image of the identity document (including its machine-readable zone), a real-time visual image of the Data Subject's face, and an image of a document confirming the residential address, and performs verification of authenticity, biometric matching and liveness confirmation, address verification, and sanctions/PEP screening.

10.1. Компания осуществляет Дистанционную идентификацию субъектов данных с использованием Сервиса Shufti Pro. При этом Компания получает фотографическое изображение документа, удостоверяющего личность (включая его машиночитываемую зону), визуальное изображение лица субъекта данных в режиме реального времени и

изображение документа, подтверждающего адрес проживания, и проводит проверку подлинности, биометрическое сопоставление и подтверждение присутствия живого лица, проверку адреса, а также санкционный/PEP-скрининг.

10.2. In relation to the Shufti Pro Service, the Company acts as Data Controller and Shufti Pro Limited acts as Data Processor, processing Personal Data (including Biometric Data) solely on the documented instructions of the Company and solely for the purposes of identification and due diligence. Responsibility for identification and its results remains with the Company; the use of the Shufti Pro Service is a technological means of performing checks and does not constitute a delegation of the Company's obligations to a third party.

10.2. В отношении Сервиса Shufti Pro Компания выступает контролёром данных, а Shufti Pro Limited — обработчиком данных, обрабатывающим персональные данные (включая биометрические) исключительно по документированным инструкциям Компании и исключительно в целях идентификации и надлежащей проверки. Ответственность за идентификацию и её результаты сохраняется за Компанией; использование Сервиса Shufti Pro является технологическим средством проведения проверок и не является передачей обязанностей Компании третьему лицу.

10.3. The engagement of Shufti Pro Limited is governed by a written data-processing agreement that includes the safeguards required by Section 14. The Company relies on the processor's technical and organisational measures, including its certifications (such as ISO/IEC 27001 and PCI-DSS) and its use of European Union Standard Contractual Clauses for international transfers.

10.3. Привлечение Shufti Pro Limited регулируется письменным договором об обработке данных, включающим гарантии, предусмотренные разделом 14. Компания опирается на технические и организационные меры обработчика, включая его сертификации (в частности, ISO/IEC 27001 и PCI-DSS) и использование Стандартных договорных положений Европейского союза для международных передач.

10.4. By undergoing Remote Identification, the Data Subject gives explicit consent to the Processing of their Personal Data, including Biometric Data, through the Shufti Pro Service, including the cross-border transfer of such data to the operator of that service for the purposes set out above.

10.4. Проходя Дистанционную идентификацию, субъект данных даёт явное согласие на обработку своих персональных данных, включая биометрические, с использованием Сервиса Shufti Pro, в том числе на трансграничную передачу таких данных оператору указанного сервиса в вышеуказанных целях.

11. Cross-Border Transfers of Personal Data

11. Трансграничная передача персональных данных

11.1. The Company transfers Personal Data outside the AIFC only where one of the following conditions is met: (a) the recipient is located in a jurisdiction recognised as providing an adequate level of protection under the AIFC Data Protection Rules; (b) appropriate safeguards are in place, in particular Standard Contractual Clauses or equivalent contractual data-protection clauses; or (c)

the Data Subject has given explicit consent to the transfer after being informed of the possible risks.

11.1. Компания передаёт персональные данные за пределы МФЦА только при выполнении одного из следующих условий: (a) получатель находится в юрисдикции, признанной обеспечивающей адекватный уровень защиты согласно AIFC Data Protection Rules; (b) обеспечены надлежащие гарантии, в частности Стандартные договорные положения или эквивалентные договорные положения о защите данных; либо (c) субъект данных дал явное согласие на передачу после информирования о возможных рисках.

11.2. Transfers to the Broker (Axiom Invest Ltd., Republic of Bulgaria, an EU/GDPR jurisdiction) are made on the basis of the conditions in clause 11.1 and only where a lawful basis exists. Transfers to the operator of the Shufti Pro Service are made on the basis of appropriate safeguards and the Data Subject's explicit consent.

11.2. Передачи Брокеру (Axiom Invest Ltd., Республика Болгария — юрисдикция ЕС/GDPR) осуществляются на основании условий пункта 11.1 и только при наличии правового основания. Передачи оператору Сервиса Shufti Pro осуществляются на основании надлежащих гарантий и явного согласия субъекта данных.

11.3. When transferring Personal Data outside the AIFC, the Company ensures that a level of protection required in the AIFC continues to apply to that data. All cross-border transfers are recorded in the Company's data-processing register and reviewed by the person responsible for data protection, who considers the impact of the transfer on Data Subjects' rights and the appropriate safeguards before the transfer takes place.

11.3. При передаче персональных данных за пределы МФЦА Компания обеспечивает сохранение к таким данным уровня защиты, требуемого в МФЦА. Все трансграничные передачи фиксируются в реестре операций обработки Компании и проверяются лицом, ответственным за защиту данных, которое до передачи оценивает её влияние на права субъектов данных и надлежащие гарантии.

12. Rights of Personal Data Subjects

12. Права субъектов персональных данных

12.1. Subject to the conditions and exemptions of the AIFC Data Protection Regulations, the Data Subject has the right to: be informed about the Processing; access their Personal Data; obtain rectification of inaccurate or incomplete data; obtain erasure of data where applicable; restrict Processing; data portability; object to Processing, including for direct marketing; not be subject to a decision based solely on automated processing that produces legal or similarly significant effects; withdraw consent; and lodge a complaint with the Commissioner or another competent authority.

12.1. С учётом условий и изъятий, предусмотренных AIFC Data Protection Regulations, субъект данных имеет право: быть информированным об обработке; получать доступ к своим персональным данным; требовать исправления неточных или неполных данных; требовать удаления данных в применимых случаях; ограничивать обработку; на переносимость данных; возражать против обработки, в том числе для целей прямого

маркетинга; не быть объектом решения, основанного исключительно на автоматизированной обработке и влекущего правовые или аналогичные существенные последствия; отзывать согласие; и подавать жалобу Комиссару либо иному компетентному органу.

12.2. Requests to exercise these rights are addressed to the person responsible for data protection within the Company and are logged. A response is provided without undue delay and in any event within the period prescribed by the applicable rules; where a request is complex or numerous, the period may be extended and the Data Subject informed accordingly. A request is free of charge unless it is manifestly unfounded, excessive or repetitive, in which case a reasonable fee may be charged.

12.2. Запросы о реализации этих прав направляются лицу, ответственному за защиту данных в Компании, и регистрируются. Ответ предоставляется без неоправданной задержки и в любом случае в срок, установленный применимыми правилами; при сложном или многочисленном характере запроса срок может быть продлён с уведомлением субъекта данных. Запрос является бесплатным, за исключением случаев, когда он явно необоснован, чрезмерен или носит повторяющийся характер, — в таком случае может взиматься разумная плата.

12.3. Where a Client is introduced by an Agent or to the Broker, and a request concerns data held by that independent Controller, the Company forwards the request or assists the Data Subject in directing it to the relevant Controller.

12.3. Если Клиент представлен Агентом или Брокеру и запрос касается данных, находящихся у такого независимого контролёра, Компания перенаправляет запрос или содействует субъекту данных в его направлении соответствующему контролёру.

13. Notification of Personal Data Subjects

13. Информирование субъектов персональных данных

13.1. Unless the Company reasonably believes the information is already known to the Data Subject, the Company provides, at the time of collection, the following information: the identity and contact details of the Company; the purposes and lawful basis of Processing; the recipients or categories of recipients of the Personal Data (including Agents, the Broker and the Shufti Pro processor); the fact and safeguards of any cross-border transfer; the retention period; the Data Subject's rights; and whether the provision of data is mandatory or optional and the consequences of failing to provide it.

13.1. Если Компания обоснованно не полагает, что информация уже известна субъекту данных, Компания предоставляет при сборе следующую информацию: наименование и контактные данные Компании; цели и правовое основание обработки; получателей или категории получателей персональных данных (включая Агентов, Брокера и обработчика Shufti Pro); факт и гарантии любой трансграничной передачи; срок хранения; права субъекта данных; а также является ли предоставление данных обязательным или добровольным и каковы последствия их непредоставления.

13.2. This information is provided through the Company's Data Protection Notice published on its website, through the Client Agreement, and through the Application for Accession, or by any other appropriate means.

13.2. Данная информация предоставляется через Уведомление о защите данных, размещённое на веб-сайте Компании, через Клиентское соглашение и Заявление о присоединении либо иным надлежащим способом.

14. Personal Data Processors and Third-Party Contracts

14. Обработчики персональных данных и договоры с третьими лицами

14.1. The Company engages a Data Processor only under a written contract that requires the processor to: act only on the Company's documented instructions; ensure the confidentiality of persons processing the data; take appropriate security measures; engage sub-processors only with the Company's prior authorisation and under equivalent obligations; assist the Company in responding to Data Subject requests, security incidents and impact assessments; and delete or return Personal Data at the end of the engagement.

14.1. Компания привлекает обработчика данных только на основании письменного договора, обязывающего обработчика: действовать исключительно по документированным инструкциям Компании; обеспечивать конфиденциальность лиц, обрабатывающих данные; принимать надлежащие меры безопасности; привлекать субобработчиков только с предварительного разрешения Компании и на эквивалентных условиях; содействовать Компании в реагировании на запросы субъектов данных, инциденты безопасности и оценки воздействия; а также удалять или возвращать персональные данные по окончании привлечения.

14.2. The Company carries out due diligence on processors and third parties commensurate with the potential impact on the security of Personal Data, and reviews third-party relationships at least annually as part of a data-protection impact assessment.

14.2. Компания проводит проверку обработчиков и третьих лиц соразмерно потенциальному влиянию на безопасность персональных данных и не реже одного раза в год пересматривает отношения с третьими лицами в рамках оценки воздействия на защиту данных.

14.3. Where the Company shares Personal Data with an independent Controller (an Agent or the Broker), the relevant agreement sets out each party's role, the lawful basis for the transfer, security-incident notification (within the time limits agreed, and in any event promptly), and mutual assistance in giving effect to Data Subjects' rights.

14.3. При передаче Компанией персональных данных независимому контролёру (Агенту или Брокеру) соответствующий договор определяет роль каждой стороны, правовое основание передачи, порядок уведомления об инцидентах безопасности (в согласованные сроки и в любом случае незамедлительно) и взаимное содействие в реализации прав субъектов данных.

15. Security Measures

15. Меры безопасности

15.1. The Company implements and maintains an Information Security Policy that establishes technical and organisational measures proportionate to the risk, including: role-based access control and the least-privilege and need-to-know principles; segregation of duties and strong authentication; change management; a vulnerability-management and patching process; firewalls and intrusion-detection/prevention and monitoring systems; encryption and pseudonymisation; separation of Personal Data and its backups from other data; secure backup and recovery; and incident-management procedures.

15.1. Компания внедряет и поддерживает Политику информационной безопасности, устанавливающую технические и организационные меры, соразмерные риску, включая: ролевое управление доступом и принципы наименьших привилегий и необходимого знания; разделение обязанностей и усиленную аутентификацию; управление изменениями; процесс управления уязвимостями и установки обновлений; межсетевые экраны, системы обнаружения/предотвращения вторжений и мониторинга; шифрование и псевдонимизацию; отделение персональных данных и их резервных копий от иных данных; безопасное резервное копирование и восстановление; и процедуры управления инцидентами.

15.2. The Company ensures physical and logical access controls over premises, systems and servers, and requires third parties (including data-centre operators and processors) to adhere to equivalent controls.

15.2. Компания обеспечивает физический и логический контроль доступа к помещениям, системам и серверам и требует от третьих лиц (включая операторов центров обработки данных и обработчиков) соблюдения эквивалентных мер контроля.

16. Record-Keeping of Processing Activities

16. Ведение записей об операциях обработки

16.1. The Company maintains a Record of Processing Activities in accordance with the record-keeping requirements of the AIFC Data Protection Regulations and Rules, including: the identity and contact details of the Company and the person responsible for data protection; the purposes of Processing; the categories of Data Subjects and Personal Data; the categories of recipients, including recipients in third countries; the jurisdictions to which data is or will be transferred and the safeguards applied; the envisaged retention periods; and a general description of the technical and organisational security measures. Where Sensitive Personal Data is processed, the Company also documents the applicable condition and lawful basis.

16.1. Компания ведёт Реестр операций обработки в соответствии с требованиями к ведению записей, предусмотренными AIFC Data Protection Regulations и Rules, включая: наименование и контактные данные Компании и лица, ответственного за защиту данных; цели обработки; категории субъектов данных и персональных данных; категории получателей, включая получателей в третьих странах; юрисдикции, в которые данные

передаются или будут переданы, и применяемые гарантии; предполагаемые сроки хранения; и общее описание технических и организационных мер безопасности. При обработке чувствительных персональных данных Компания также документирует применимое условие и правовое основание.

16.2. The records are reviewed regularly to ensure accuracy and compliance.

16.2. Записи регулярно пересматриваются для обеспечения их точности и соответствия требованиям.

17. Notification of the Commissioner

17. Уведомление Комиссара

17.1. The Company notifies the Commissioner of the details of Processing operations that are required to be notified under the AIFC Data Protection Regulations and Rules, including any operation involving the Processing of Sensitive Personal Data (such as Biometric Data), and of material changes to such operations.

17.1. Компания уведомляет Комиссара о деталях операций обработки, подлежащих уведомлению согласно AIFC Data Protection Regulations и Rules, включая любую операцию, связанную с обработкой чувствительных персональных данных (в частности, биометрических), а также о существенных изменениях таких операций.

17.2. Notifications are made within the time limits prescribed by the AIFC Data Protection Rules and are renewed where the Processing operation continues, in accordance with those rules.

17.2. Уведомления направляются в сроки, установленные AIFC Data Protection Rules, и возобновляются при продолжении операции обработки в соответствии с этими правилами.

18. Personal Data Breaches

18. Нарушения безопасности персональных данных

18.1. The person responsible for data protection must be notified of any Personal Data breach as soon as possible. That person records the breach, assesses its likely impact together with the relevant information owner, and, where the breach is notifiable, informs the Commissioner within the time limit prescribed by the AIFC Data Protection Regulations and Rules.

18.1. Лицо, ответственное за защиту данных, должно быть уведомлено о любом нарушении безопасности персональных данных в кратчайший возможный срок. Это лицо регистрирует нарушение, оценивает его вероятное воздействие совместно с соответствующим владельцем информации и, если нарушение подлежит уведомлению, информирует Комиссара в срок, установленный AIFC Data Protection Regulations и Rules.

18.2. Where a breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the Company informs the affected Data Subjects. Where a breach affects data shared with an independent Controller (an Agent or the Broker) or a processor, the Company notifies, and

cooperates with, the relevant party without undue delay and in any event within the time limit agreed in the relevant contract.

18.2. Если нарушение с большой вероятностью повлечёт высокий риск для прав и свобод субъектов данных, Компания информирует затронутых субъектов данных. Если нарушение затрагивает данные, переданные независимому контролёру (Агенту или Брокеру) либо обработчику, Компания уведомляет соответствующую сторону и взаимодействует с ней без неоправданной задержки и в любом случае в срок, согласованный в соответствующем договоре.

18.3. A dedicated Data Breach Policy governs the investigation, reporting and mitigation of breaches and provides guidance to employees.

18.3. Отдельная Политика реагирования на нарушения регулирует расследование, отчётность и снижение последствий нарушений и содержит руководство для работников.

19. Retention and Destruction of Personal Data

19. Хранение и уничтожение персональных данных

19.1. The Company processes Personal Data throughout the period of business relations with the Client and retains it thereafter for the period required for legal, regulatory, anti-fraud and legitimate business purposes.

19.1. Компания обрабатывает персональные данные в течение всего периода деловых отношений с Клиентом и хранит их после этого в течение срока, необходимого для правовых, регуляторных, противомошеннических и законных деловых целей.

19.2. Records relating to a Client are retained for at least 6 (six) years following the termination of the relationship with that Client, in accordance with the applicable Conduct of Business requirements, unless a longer period is required by law. Upon expiry of the applicable retention period, Personal Data is securely destroyed or irreversibly anonymised.

19.2. Записи, относящиеся к Клиенту, хранятся не менее 6 (шести) лет после прекращения отношений с этим Клиентом в соответствии с применимыми требованиями Conduct of Business, если более длительный срок не требуется законом. По истечении применимого срока хранения персональные данные безопасно уничтожаются или необратимо анонимизируются.

20. Roles and Responsibilities

20. Роли и ответственность

20.1. Responsibility for compliance with this Policy lies with all employees who have access to Personal Data in the course of their duties. Management ensures adequate resources and governance. The person responsible for data protection monitors compliance, maintains the Record of Processing Activities, conducts impact assessments, serves as the point of contact for the Commissioner and Data Subjects, and reviews cross-border transfers and third-party relationships.

Information owners establish and enforce data-control measures. Employees follow this Policy and report potential breaches.

20.1. Ответственность за соблюдение настоящей Политики несут все работники, имеющие доступ к персональным данным в рамках своих обязанностей. Руководство обеспечивает достаточные ресурсы и управление. Лицо, ответственное за защиту данных, контролирует соблюдение требований, ведёт Реестр операций обработки, проводит оценки воздействия, выступает контактным лицом для Комиссара и субъектов данных и пересматривает трансграничные передачи и отношения с третьими лицами. Владельцы информации устанавливают и обеспечивают соблюдение мер контроля данных. Работники соблюдают настоящую Политику и сообщают о возможных нарушениях.

20.2. Employees are trained on this Policy at least annually and upon induction, covering the AIFC Data Protection Regulations and Rules, AML/CFT obligations, information security, and breach recognition and escalation.

20.2. Работники проходят обучение по настоящей Политике не реже одного раза в год и при приёме на работу, охватывающее AIFC Data Protection Regulations и Rules, обязательства в области ПОД/ФТ, информационную безопасность, а также распознавание и эскалацию нарушений.

21. Final Provisions

21. Заключительные положения

21.1. Where a matter is not regulated by this Policy, the Company's other internal documents, the AIFC Data Protection Regulations and Rules, other applicable AIFC acts, and the legislation of the Republic of Kazakhstan apply.

21.1. В случаях, когда вопрос не урегулирован настоящей Политикой, применяются иные внутренние документы Компании, AIFC Data Protection Regulations и Rules, иные применимые акты МФЦА и законодательство Республики Казахстан.

21.2. This Policy is reviewed at least annually, and following any material change in the Company's Processing operations or the applicable legal framework. Amendments are approved by the Director and communicated through the Company's internal channels; the current version is published or made available as required.

21.2. Настоящая Политика пересматривается не реже одного раза в год, а также при любом существенном изменении операций обработки Компании или применимой правовой базы. Изменения утверждаются Директором и доводятся до сведения через внутренние каналы Компании; действующая редакция публикуется или предоставляется по мере необходимости.