Edition #1
Approved on 11.11.2025
by CENTRAL ASIAN CAPITAL LTD.'s
Board of Directors

CENTRAL ASIAN CAPITAL LTD.
Data Protection Policy

1. DEFINITIONS

1.1. Personal Data – any information relating to an identified or identifiable natural person.
1.2. Data Subject – a person whose personal data are processed by the Company.
1.3. Processing – any operation performed on personal data, including collection, storage, use, disclosure, or deletion.
1.4. Controller – the Company, which determines the purposes and means of processing personal data.
1.5. Processor – a third party that processes personal data on behalf of the Company.
DPO (Data Protection Officer) – a person responsible for monitoring compliance with data protection obligations within the Company.

2. PURPOSE AND SCOPE

2.1. This Data Protection Policy (Policy) sets out how Central Asian Capital Ltd. (**Company, CAC, we** or **us**) collects, uses, stores, and protects personal data of clients, employees, and other data subjects in accordance with the AIFC Data Protection Regulations and other applicable laws.
2.2. The Company is committed to ensuring that all personal data are processed lawfully, fairly, and transparently, and that the privacy rights of individuals are respected at all times.
2.3. This Policy applies to:
(a) All employees, officers, and contractors of the Company;
(b) All processing of personal data performed by or on behalf of the Company;
(c) All systems and processes where personal data are stored or transmitted.

3. PRINCIPLES OF DATA PROTECTION

3.1. We adhere to the following principles when processing personal data:
(a) Lawfulness, fairness, and transparency – data are processed lawfully and in a way that is clear to the data subject;
(b) Purpose limitation – data are collected for specific, legitimate purposes and not

further processed in a manner incompatible with those purposes;

(c) Data minimisation – only the data necessary for the stated purpose are collected;

(d) Accuracy – data must be kept accurate and up to date;

(e) Storage limitation – personal data are not retained longer than necessary;

(f) Integrity and confidentiality – data are processed securely and protected against unauthorized access, loss, or destruction;

(g) Accountability – the Company takes responsibility for ensuring compliance with all data protection principles.

4. LAWFUL BASIS FOR PROCESSING

4.1. The Company processes personal data on one or more of the following lawful bases:

(a) Consent of the data subject;

(b) Performance of a contract to which the data subject is a party;

(c) Compliance with legal or regulatory obligations (e.g., AML/KYC requirements under AIFC rules);

(d) Legitimate interests pursued by the Company, provided such interests are not overridden by the data subject's rights;

(e) Security and Fraud Prevention:

(i) To protect the integrity of user accounts, prevent unauthorized access, and ensure transaction security;

(ii) To detect, investigate, and prevent fraud, suspicious activity, or violations of applicable laws or internal rules;

(iii) To safeguard the Company's information systems and infrastructure.

(f) System Management and Service Improvement:

(i) To maintain, operate, and enhance the technical performance and usability of the website and mobile application;

(ii) To monitor and analyze user behavior and system performance for troubleshooting, analytics, and product development;

(iii) To create aggregated or anonymized statistics that help improve service quality and functionality.

(g) Record-Keeping and Internal Reporting:

(i) To maintain accurate business, accounting, and audit records;

(ii) To support internal governance, compliance, and risk-management procedures.

(h) Protection of Legitimate Interests and Legal Rights:

(i) To establish, exercise, or defend legal claims and protect the Company's property, rights, and interests;

(ii) To ensure business continuity and proper operation of the Company's services.

5. INFORMATION RECEIVED FROM THIRD PARTIES AND AUTOMATICALLY COLLECTED DATA

5.1. The Company may obtain information about the Client or User from external sources and through automatic data-collection technologies integrated into the Website and mobile application.

5.2. **Information from Third Parties**. The Company may receive information from:

(a) Payment processors, banks, and custodians;

(b) Identity-verification and KYC/AML service providers;

(c) Business partners or regulatory authorities, where required by applicable law or based on the Client's consent.

5.3. The Company guarantees the confidentiality and protection of any personal data obtained from such sources. These data shall not be disclosed to third parties, except when disclosure is:

(a) required by the AIFC legislation, or

(b) authorized by the Client's consent or request.

5.4. The Company collects, stores, and uses this information solely for the administration and technical management of its Website and mobile application, as well as for compliance, system improvement, analytical, and marketing purposes.

5.5. Automatically Collected Information

5.5.1. To enhance system performance and analyze Website usage, the Company may automatically collect certain information about Users, including but not limited to:

(a) Device and technical information (device model, browser type and version, operating system and version, IP address);

(b) Pages visited and time spent on the Website;

(c) General geographic data (country or region of access);

(d) Referring sources, such as other websites or applications from which Users visit the Website;

(e) User actions on the Website to understand and remember preferences for future visits;

(f) Anonymous demographic data, such as aggregated age-group or gender statistics, where available.

5.5.2. The above information is collected and analyzed in aggregated (statistical) form for all Users. It is non-personal and cannot, under any circumstances, be used to identify or enable the identification of any specific User.

5.5.3. The Company may utilize analytical tools and similar technologies (such as web analytics platforms) to support this automatic data collection and to improve functionality, security, and User experience.

6. USE AND DISCLOSURE OF COMBINED INFORMATION

6.1. All information obtained—whether from third parties or collected automatically—is used by the Company in accordance with applicable data-protection legislation.

6.2. The Company may share aggregated, anonymized, or otherwise non-identifiable data with trusted service providers or business partners for the purposes of analysis, performance monitoring, and service improvement. Such information cannot identify the Client or User.

7. Security Assurance

7.1. Emphasizing the importance of ensuring the confidentiality of information received about the Client through the web site and mobile application, the Company protects both the information provided by the Client and the information automatically obtained about the Client in several ways.

7.2. To ensure the security of information received about the Client through the web site and mobile application, the Client, when logging into their personal page in the system, confirming transactions through the system, as well as performing any actions that may contain the Client's personal data.

7.3. The Client is obliged to ensure the confidentiality of the information required to access the web site and mobile application and not to disclose in any way to third parties the usernames, passwords, codes, and other data used to access and operate the system, or to avoid any actions that may result in such data becoming known to third parties.

8. CATEGORIES OF DATA PROCESSED

8.1. We may collect and process the following types of personal data:

(a) Identification information (name, passport, ID number);

(b) Contact details (address, email, phone number);

(c) Financial information (bank details, investment portfolio, transaction records);

(d) Employment data (for staff and contractors);

(e) KYC and AML information (including source of funds, beneficial ownership);

(f) Any other data required by the AIFC regulator or contractual obligations.

9. DATA SUBJECT RIGHTS

9.1. Data subjects have the following rights under the AIFC Data Protection Regulations:

(a) Right to access – to obtain confirmation and a copy of personal data held by the Company;

(b) Right to rectification – to correct inaccurate or incomplete data;

(c) Right to erasure ("right to be forgotten") – to request deletion of personal data under certain conditions;

(d) Right to restriction of processing;

(e) Right to data portability;

(f) Right to object to certain processing activities, including direct marketing.

9.2. Requests from data subjects are handled promptly and no later than one month from receipt.

10. DATA SECURITY AND STORAGE

10.1. The Company implements appropriate technical and organisational measures to ensure data security, including:

(a) Access control and authentication procedures;
(b) Encryption of sensitive data and secure file transfer;
(c) Regular system audits and backups;
(d) Physical security measures in the office;
(e) Confidentiality agreements with all employees and contractors.

10.2. All personal data are stored in secure servers located within the AIFC or other jurisdictions providing an adequate level of protection.

11. DATA TRANSFERS

11.1. Personal data may only be transferred outside the AIFC if:

(a) The destination jurisdiction ensures adequate protection as recognized by the AIFC Commissioner of Data Protection; or
(b) Appropriate safeguards (such as standard contractual clauses) are in place; or
(c) The data subject has explicitly consented to such transfer.

12. DATA RETENTION

12.1. Personal data are retained only for as long as necessary for the purposes for which they were collected, or as required by applicable law.

12.2. Retention periods are defined in the Record Retention Schedule maintained by the Compliance Officer.

12.3. Upon expiration of retention periods, data are securely deleted or anonymised.

13. ROLES AND RESPONSIBILITIES

13.1. Board of Directors – responsible for approving this Policy and overseeing compliance with data protection laws.

13.2. Compliance Officer / DPO – ensures day-to-day implementation, conducts audits, and acts as a contact point with the AIFC Commissioner of Data Protection.

13.3. Employees – must comply with this Policy and immediately report any data breaches or incidents.

14. DATA BREACH MANAGEMENT

14.1. Any suspected or actual data breach must be reported immediately to the DPO.

14.2. The DPO will:

(a) Investigate the incident;
(b) Assess the potential impact on individuals;
(c) Notify the AIFC Commissioner of Data Protection within 72 hours if the breach is likely to result in a risk to data subjects;
(d) Document all incidents and corrective actions taken.

15. TRAINING AND AWARENESS

15.1. All employees receive data protection and cybersecurity training upon hiring and annually thereafter.

15.2. The Company promotes a culture of privacy awareness and ensures that employees understand their responsibilities regarding personal data.

16. Other Provisions

16.1. By using the web site and mobile application the Client accepts the terms set forth in this Policy and gives their consent for the collection, use, and other processing of information about the Client for the purposes and in the manner defined by this Policy.

16.2. In the presence of legal grounds provided by the legislation of the AIFC, a written request submitted by the Client to the Company regarding obtaining, processing, storing, using, or revoking previously given consent(s) for the processing of their personal data shall be reviewed and handled by the Company in accordance with the procedures and timeframes established by the AIFC Regulations and/or the Company's internal legal acts. In case of withdrawal of consent(s), the Company's provision of services to the Client may be restricted and/or terminated.

16.3. In the presence of legal grounds provided by the AIFC legislation, a written request submitted by the Client to the Company regarding the correction, destruction, and/or suspension of the processing of personal data provided to the Company shall be reviewed and handled by the Company in accordance with the procedures and timeframes established by the AIFC Regulations and/or the Company's internal legal acts.

17. MONITORING AND REVIEW

17.1. This Policy can be reviewed annually or whenever there are significant regulatory or operational changes.

17.2. Compliance with this Policy is monitored through periodic internal audits.

18. CONTACT

For questions or concerns regarding this Policy or data protection matters, please contact:
Data Protection Officer (DPO)
Central Asian Capital Ltd.

AIFC, 5 Dostyk ave, office NP-199, Astana city, Kazakhstan
Email: info@centralasiancapital.org