

## PRIVACY POLICY OF LANDMARK CAPITAL CJSC

### 1. Purpose and Scope

- 1.1. This Privacy Policy ("Policy") describes the principles, purposes and procedures governing the collection, Processing, storage and protection of Personal Data by Landmark Capital CJSC ("Company", "we", "us" or "our").
- 1.2. This Policy applies to all Personal Data collected via the Company website, mobile application or through any other means in the course of providing regulated financial and investment services.

### 2. Definitions

- 2.1. The terms and definitions set forth by these Rules shall have the following meaning:

Personal Data	Any information relating to an identified or identifiable natural person ("Data Subject"), including representatives, shareholders, ultimate beneficial owners (UBOs) or officers of a legal-entity client, where such person can be directly or indirectly identified by reference to an identifier (such as name, ID number, location data, online identifier) or to one or more factors specific to the person's identity.
Processing	Any operation or set of operations performed on Personal Data, whether by automated or manual means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure or destruction.
Data Subject	Any natural person whose Personal Data are processed by the Company, including: <ul style="list-style-type: none"><li>• Individual Clients;</li><li>• Representatives, directors, employees, shareholders and beneficial owners of legal-entity clients;</li><li>• Applicants, service users and visitors of the Company's website or mobile application.</li></ul>
Client	Any natural or legal person that has concluded or has expressed an intention to conclude, an agreement with the Company for the provision of financial, investment or related services. Where the Client is a legal entity, the Company may process Personal Data of its representatives or related natural persons for KYC, contractual and compliance purposes.
Data Controller	Landmark Capital CJSC, registered and operating under the laws of the Republic of Armenia, determining the purposes and means of Processing Personal Data in the context of its regulated financial and investment activities.
Data Processor	Any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Data Controller in accordance with a written data processing agreement ensuring confidentiality and compliance with applicable data-protection laws.

Third Party	Any person or organization other than the Data Subject, the Data Controller, the Data Processor or those authorized to process data under the direct authority of the Company or its Processors.
Consent	A clear, informed and voluntary agreement from the Client, expressed through a positive action, that allows the Company to collect and use their Personal Data for specific purposes.
Profiling	Any form of automated Processing of Personal Data to evaluate personal aspects of a Data Subject, particularly to analyze or predict their behavior, preferences, financial reliability or risk profile.
Personal Data Breach	A breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Supervisory Authority	The Personal Data Protection Agency under the Ministry of Justice of the Republic of Armenia or any other competent data-protection authority having jurisdiction over Company's processing activities.
KYC (Know Your Customer) Data	Identification and verification information collected under the Law of the Republic of Armenia on Combating Money Laundering and Terrorism Financing, including data on beneficial owners, representatives and ultimate controllers of legal-entity clients.
AML/CFT	The legal and regulatory framework governing Anti-Money Laundering and Counter-Financing of Terrorism, including all obligations imposed by the Central Bank of Armenia, the Financial Monitoring Center and relevant international standards (e.g., FATF).
Cookies and Tracking Technologies	Small text files or equivalent technologies (e.g., software development kits, pixels) stored on a user's device that collect information about usage, authentication, preferences and system performance.
Anonymization / Pseudonymization	The process of altering Personal Data so that the individual can no longer be identified directly or indirectly (Anonymization) or can only be identified using additional, separately stored information (Pseudonymization).
Information Security Officer	An officer who in addition to overseeing information security operations also oversee compliance with this Policy, provide guidance on data protection obligations and act as a contact point for Data Subjects and supervisory authorities (in line with Article 37 GDPR). For the purposes of the GDPR, the Information Security Officer also acts as the Company's Data Protection Officer.
Website and Mobile Application	The Company's official digital platforms through which Clients may access financial and investment services, communicate with the Company and manage accounts or transactions, including associated APIs and secure interfaces.
Applicable Law	Collectively, the laws of the Republic of Armenia, regulations of the Central Bank of Armenia, GDPR, UK Data Protection Act 2018 and OECD Privacy Guidelines, as applicable to Company's cross-border and regulated operations.

GDPR	General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).
Business Partner	Any external entity engaged by the Company to provide services, perform functions or execute obligations under a contractual arrangement, including technology providers, custodians, intermediaries or professional advisers.
Beneficial Owner (UBO)	A natural person who ultimately owns or controls a client, legal entity or arrangement and/or on whose behalf a transaction or activity is conducted, as defined under Armenian AML/CFT laws.

### 3. Information We Collect

- 3.1. Company collects and processes Personal Data that are necessary, relevant and proportionate for the lawful provision of its regulated financial and investment services, for compliance with statutory obligations and for the maintenance of secure and efficient business operations.
- 3.2. Personal Data are obtained from multiple lawful sources, including directly from Clients or their authorized representatives, automatically through the Company's digital platforms and from verified third-party or publicly available sources, as described below.
- 3.3. Information Provided by Clients
  - 3.3.1. When a Client establishes or intends to establish a business relationship with the Company, the following categories of information may be collected and processed:
    - Identification and Personal Details: Full name, patronymic (if applicable), date and place of birth, nationality, citizenship and residential or registered address;
    - Contact Information: Telephone number, email address and preferred language of communication;
    - Identification and Verification Data: Passport or national ID number, tax identification number, issuance authority and date and KYC and/or AML/CFT documentation;
    - Financial and Investment Information: Bank account details, source of funds and wealth, income level, employment status, investment experience, declared risk profile and investment objectives;
    - Account and Security Information: Login credentials, authentication data (e.g., passwords, PIN codes, biometric data where applicable) and user preferences relating to account security or access methods.
  - 3.3.2. The Company may also collect additional supporting documentation required to meet legal and regulatory standards, such as proof of address (utility bills, tenancy agreements), beneficial ownership declarations for legal entities or professional certificates and licenses for specific service categories.
- 3.4. Information Collected Automatically
  - 3.4.1. When Clients or users access the Company's official website, mobile application or online platforms, certain technical and behavioral information is collected automatically for operational, analytical and security purposes, including:
    - Technical Identifiers: IP address, browser type and version, device ID, operating system, screen resolution and mobile network information;
    - Usage and Interaction Data: Session timestamps, login and logout records, pages visited, links clicked and user actions within the website or mobile application;
    - Cookies, Software Development Kits and Analytics Tools: Data collected through cookies, software development kits and web analytics platforms used to ensure secure operation, remember user preferences and monitor platform performance;

- Geolocation Data: Approximate location derived from IP address or device settings, used for regional compliance, fraud prevention and service customization.
- 3.4.2. This information is processed in aggregated or pseudonymized form wherever possible and is not used to identify individual users unless required for security, fraud detection or compliance purposes.
- 3.5. Information Obtained from Third Parties
- 3.5.1. In addition to direct collection, the Company may obtain and verify Personal Data from external and lawful sources, including but not limited to:
- Financial and Payment Institutions: Correspondent banks, payment processors and custodians involved in executing transactions or settlements;
  - Regulatory and Supervisory Authorities: Governmental, tax and law enforcement bodies providing information under legal or regulatory mandates;
  - The Company may obtain certain categories of Personal Data from external KYC/AML and verification service providers, who conduct identity verification, sanctions screening, and background checks in accordance with applicable AML/CFT legislation. The Personal Data received from such third-party providers may include identification and contact details, KYC/AML information (such as sanctions and watchlist data), information on corporate roles and beneficial ownership, transaction-related data, and other information necessary to comply with regulatory obligations or to provide the requested services;
  - Public Databases and Business Registers: Sources containing information about company ownership, beneficial owners or professional affiliations;
  - Business Partners and Referrals: Entities or individuals who introduce Clients or cooperate with the Company, based on consent or a lawful contractual relationship.
- 3.5.2. All third-party data are processed strictly for legitimate and predefined purposes in accordance with the principles of lawfulness, fairness and transparency and are protected by appropriate technical and organizational safeguards.
- 3.5.3. Where the Company obtains Personal Data from sources other than the Data Subject, it shall provide the Data Subject with the information contained in this Privacy Policy at the earliest appropriate opportunity and in any event within one month, or at the time of first communication or disclosure, whichever occurs first, unless an exemption applies.
- 3.6. Accuracy and Responsibility
- 3.6.1. Clients are responsible for ensuring that all Personal Data and documents provided to the Company are accurate, complete and current.
- 3.6.2. The Company may periodically request Clients to confirm or update their information to maintain accuracy and compliance with applicable laws and internal procedures.
- 3.7. Mandatory Provision of Personal Data
- 3.7.1. In most cases, the provision of Personal Data requested by the Company is a statutory and/or contractual requirement necessary to:
- comply with AML/CFT and other regulatory obligations; and
  - enter into and perform agreements for the provision of financial and investment services.
- 3.7.2. Where a Data Subject fails or refuses to provide Personal Data required by law or contract, the Company may be unable to establish or continue a business relationship, open or maintain an account, execute transactions or provide specific services.

#### 4. Purposes and Legal Bases of Processing

- 4.1. Company processes Personal Data only for specified, explicit and lawful purposes, and on the basis of at least one of the legal grounds set out in Article 6 of the GDPR and the Law of the Republic of Armenia on Personal Data Protection.
- 4.2. Personal Data are not processed for purposes that are incompatible with those originally identified. Any new or additional Processing shall be subject to prior notification to the Data Subject and, where required, to their explicit consent.
- 4.3. The primary purposes and corresponding legal bases for the Processing of Personal Data are summarized below:

Purpose of Processing	Description	Legal Basis
Account Registration and Service Provision	To establish, manage and maintain Client accounts; provide access to financial and investment services; execute contractual obligations; and facilitate Client communications.	Performance of a Contract
Client Identification and Verification (KYC/AML)	To verify Client identity, beneficial ownership and source of funds; conduct due diligence and screening as required under AML/CFT legislation and CBA regulations.	Legal Obligation
Regulatory and Reporting Compliance	To comply with reporting, recordkeeping, audit and inspection requirements imposed by the Central Bank of Armenia (CBA), tax authorities and other competent bodies.	Legal Obligation
Transaction Execution and Customer Support	To process financial transactions, execute Client orders, confirm settlements and provide assistance through official communication channels.	Performance of a Contract
Fraud Prevention, Risk Management and IT Security	To prevent unauthorized access, monitor system performance, detect fraud or suspicious activity and protect the integrity of Client accounts and Company systems. These activities reflect the Company's legitimate interest in ensuring the security and proper functioning of its services.	Legitimate Interests; Legal Obligation
Service Improvement and Analytics	To evaluate, improve and optimize the Company's platforms, products and internal processes through aggregated analytics and feedback, in line with the Company's legitimate interest in improving and developing its services.	Legitimate Interests; Consent
Marketing and Communication	To send service updates, research materials or promotional information relevant to the Client's interests and preferences.	Consent; Legitimate Interests
Legal Claims and Dispute Resolution	To establish, exercise or defend legal claims; handle disputes, complaints or investigations; and ensure the protection of the Company's rights and property, which constitutes a legitimate interest of the Company.	Legitimate Interests; Legal Obligation

- 4.3.1. In limited cases, and only where required for AML/CFT, fraud prevention, sanctions screening or other regulatory purposes, the Company may process special categories of Personal Data (such as data revealing political opinions in the context of identifying politically exposed persons) and Personal Data relating to criminal convictions and offences. Such Processing is carried out based on one or more of the grounds set out in Articles 9(2) and 10 GDPR, including, in particular, Processing necessary:
- for reasons of substantial public interest on the basis of Union or Member State law (e.g. AML/CFT legislation and related regulatory requirements); or
  - for the establishment, exercise or defence of legal claims.
- 4.4. The Company may also process Personal Data for secondary or compatible purposes, such as internal auditing, statistical analysis and record-keeping, provided that such Processing is consistent with the original lawful basis and does not infringe the rights and freedoms of the Data Subject.
- 4.5. Where Processing is based on Consent, the Data Subject has the right to withdraw consent at any time, without affecting the lawfulness of Processing carried out prior to such withdrawal.
- 4.6. The Company does not make decisions based solely on automated processing, including profiling, which produce legal effects concerning the Data Subject or similarly significantly affect them, within the meaning of Article 22 GDPR. Where the Company intends in the future to implement such automated decision-making, it shall provide the Data Subjects with specific prior notice and information about the logic involved, as well as the significance and envisaged consequences of such processing.

## 5. Data Subject Rights

- 5.1. Under the Law of the Republic of Armenia on Personal Data Protection and the GDPR, every individual whose Personal Data are processed by Company is entitled to exercise the following rights, subject to applicable legal and regulatory limitations:
- Right of Access — The Data Subject has the right to obtain confirmation as to whether the Company processes Personal Data relating to them and, if so, to receive a copy of such data together with information on the purposes of Processing, categories of data, recipients and applicable retention periods.
  - Right to Rectification — The Data Subject may request correction or completion of inaccurate or incomplete Personal Data to ensure their accuracy and relevance.
  - Right to Erasure (“Right to be Forgotten”) — The Data Subject may request the deletion of their Personal Data where there are lawful grounds, such as withdrawal of consent, cessation of purpose or unlawful Processing. This right may be restricted where data retention is required by law or regulatory obligations (e.g., AML/CFT recordkeeping).
  - Right to Restriction of Processing — The Data Subject may request that the Company temporarily suspend Processing of their Personal Data in certain circumstances, including disputes over accuracy or legality, or where the data are needed for the establishment or defense of legal claims.
  - Right to Object — The Data Subject may object to Processing carried out on the basis of the Company’s legitimate interests or for direct marketing purposes. The Company shall cease such Processing unless it demonstrates compelling legitimate grounds or a legal obligation to continue.
  - Right to Data Portability — Where Processing is based on consent or contract and carried out by automated means, the Data Subject may request to receive their Personal Data in a structured, commonly used and machine-readable format, or to have them transmitted to another controller where technically feasible.

- Right to Withdraw Consent — Where Processing is based on consent, the Data Subject may withdraw such consent at any time, without affecting the lawfulness of Processing performed prior to withdrawal. Certain services may be limited where Processing of specific data is required for their provision.
  - Right to Lodge a Complaint — The Data Subject may submit a complaint regarding the Processing of their Personal Data to the Personal Data Protection Agency under the Ministry of Justice of the Republic of Armenia or to another competent supervisory authority within the European Economic Area, as applicable.
- 5.2. Requests to exercise any of the above rights shall be submitted in writing or electronically to the Company's Information Security Officer using the contact details provided in Section 11 of this Policy. The Company shall review and respond to each valid request within one month of receipt, which period may be extended in accordance with applicable law where requests are particularly complex or numerous.

## 6. Data Sharing and Disclosure

- 6.1. Personal Data processed by Company may be disclosed or shared only where such disclosure is necessary, lawful and proportionate for the performance of contractual, legal or regulatory obligations and always in accordance with applicable data protection legislation.
- 6.2. The Company may share Personal Data with the following categories of recipients:
- Regulatory and Supervisory Authorities — including, but not limited to, the Central Bank of Armenia (CBA), tax authorities and judicial or law-enforcement bodies, where disclosure is required to comply with statutory or regulatory obligations, inspections or lawful orders.
  - KYC/AML and Identity Verification Service Providers — for the purpose of customer due diligence, sanctions screening and ongoing monitoring in accordance with the Law on Combating Money Laundering and Terrorism Financing.
  - IT and Cloud Infrastructure Providers — responsible for secure hosting, maintenance and operation of the Company's information systems and digital platforms, subject to strict data protection and confidentiality undertakings.
  - External Auditors, Legal Advisers and Professional Consultants — engaged for audit, compliance or legal support services, bound by professional secrecy and contractual confidentiality obligations.
  - Business Partners and Third-Party Service Providers — involved in the delivery of financial or investment services, engaged under written agreements ensuring compliance with applicable data protection laws and, where required, subject to the Client's prior consent.
- 6.3. All third parties receiving Personal Data from the Company shall process such data only for the purposes for which it was disclosed and in accordance with the Company's written instructions, confidentiality clauses and applicable legislation.
- 6.4. Personal Data shall never be sold, rented or disclosed to any third party for marketing or other commercial purposes unrelated to the Company's legitimate business activities or the provision of services to Clients.
- 6.5. Where required by law or applicable cross-border data transfer rules, the Company shall ensure that appropriate contractual and technical safeguards (such as Standard Contractual Clauses or equivalent mechanisms) are in place prior to any international transfer of Personal Data.

## 7. Data Security

- 7.1. Company shall implement and maintain comprehensive technical and organizational security measures to ensure the confidentiality, integrity and availability of Personal Data processed within its operations. These measures are designed in accordance with the requirements of the Central

- Bank of Armenia (CBA), Article 32 of the GDPR, internal legal acts of the Company's information security system and applicable international information security standards.
- 7.2. The Company's data protection framework includes, but is not limited to, the following measures:
- Encryption and Secure Communication: Use of Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols to protect data during transmission between Clients and the Company's systems;
  - Access Control and Authentication: Implementation of role-based access controls, multi-factor authentication (MFA) and user authorization procedures to restrict access strictly to authorized personnel;
  - System Monitoring and Vulnerability Testing: Continuous monitoring of networks and applications, periodic penetration testing and vulnerability assessments to detect, prevent and mitigate potential threats;
  - Physical and Environmental Security: Protection of data centers and office premises through controlled access systems, surveillance and environmental safeguards to prevent unauthorized entry, data loss or damage;
  - Data Backup and Business Continuity: Regular data backups, disaster recovery plans and redundancy mechanisms to ensure service continuity and information availability;
  - Secure Data Retention and Destruction: Safe storage of Personal Data in encrypted or access-controlled systems and secure deletion or destruction of outdated, redundant or legally expired data using industry-approved methods.
- 7.3. All employees, contractors and third parties authorized to access Personal Data are bound by confidentiality obligations and are trained in information security and data protection principles as part of the Company's compliance program.
- 7.4. The Company shall promptly investigate and respond to any data breach or security incident, take appropriate remedial actions and notify the competent authorities and affected Data Subjects when required by law.
- 7.5. Clients bear responsibility for maintaining the confidentiality of their access credentials, passwords and authentication data. The Company strongly recommends that Clients implement robust security practices, including the use of unique passwords and secure device management, when accessing the Company's digital platforms and services.

## 8. Data Retention

- 8.1. Company shall retain Personal Data only for as long as necessary to fulfill the purposes for which such data were collected and Processed or as required by the applicable laws and regulations of the Republic of Armenia, including anti-money laundering and counter-terrorism financing (AML/CFT) obligations.
- 8.2. Retention periods are determined based on:
- The nature and category of the Personal Data;
  - The purpose and legal basis of Processing;
  - Applicable statutory or regulatory requirements imposed by the Central Bank of Armenia (CBA), tax authorities or other competent bodies; and
  - The necessity to preserve information for the establishment, exercise or defense of legal claims.
- 8.3. The Company applies the following standard retention timeframes unless otherwise mandated by law or regulatory guidance:
- AML/CFT and KYC Documentation: Retained for a minimum period of five (5) years following the termination of the business relationship or completion of the transaction, in accordance with the Law on Combating Money Laundering and Terrorism Financing;

- Transactional, Accounting and Audit Records: Retained for a period of seven (7) years from the date of the transaction or record creation, as required under financial and tax regulations;
  - Contractual and Correspondence Records: Retained for as long as necessary to administer the contractual relationship and up to five (5) years after termination, unless longer retention is required for dispute resolution or legal claims;
  - Marketing and Communication Preferences: Retained until the Data Subject withdraws consent or opts out of receiving such communications;
  - Employment and Internal Governance Records: Retained in accordance with labor, accounting and compliance obligations applicable to the Company.
- 8.4. Upon the expiry of the applicable retention period, Personal Data shall be securely deleted, anonymized or irreversibly destroyed in a manner preventing further identification or recovery. Where deletion is not immediately feasible due to technical or regulatory constraints, such data shall be securely archived and access restricted until final removal is possible.
- 8.5. The Company maintains an internal Data Retention Schedule and implements regular reviews to ensure that stored information remains accurate, necessary and lawfully retained. The schedule forms part of the Company's overall data governance and compliance framework.

### **9. Cookies and Analytics**

- 9.1. The official website and mobile application of Company use cookies, software development kits and other comparable tracking technologies to ensure secure operation, enhance functionality and improve user experience.
- 9.2. Cookies are small data files placed on a user's device or browser when accessing the Company's digital platforms. They enable essential website functionality, session management and personalized service delivery, as well as performance analytics and security monitoring.
- 9.3. The Company categorizes cookies and similar technologies as follows:
- Strictly Necessary Cookies: Required for the secure and proper functioning of the website or mobile application, including authentication, session management and transaction processing. These cookies cannot be disabled through consent tools.
  - Preference Cookies: Used to remember user settings such as language, display preferences and login options to facilitate a more personalized experience.
  - Analytical and Performance Cookies: Collect aggregated, anonymous statistics on website usage and system performance to help the Company improve its services and detect technical issues.
  - Marketing or Third-Party Cookies: Used to deliver relevant content or promotional messages and to measure the effectiveness of marketing campaigns. These are enabled only with the Data Subject's prior consent.
- 9.4. The use of non-essential cookies (including preference, analytics and marketing cookies) shall occur only after the user provides explicit Consent, in accordance with the GDPR and applicable Armenian e-communications and data protection laws. Users may withdraw or modify their cookie preferences at any time.
- 9.5. Users can manage or disable cookies through their web browser or mobile device settings. However, disabling certain cookies may affect the availability or performance of some website or application features.
- 9.6. The Company may also employ analytical tools, software development kits and third-party service providers to collect non-personally identifiable data about website or application performance, visitor behavior and service usage trends. Such data are processed in aggregated or anonymized form and cannot be used to identify individual users.

- 9.7. For more detailed information regarding the types of cookies used, their duration and management options, users are encouraged to consult the Company's Cookie Notice, available on the official website.

### **10. Updates to this Policy**

- 10.1. Company shall periodically review and, where necessary, update this Privacy Policy to ensure continued compliance with applicable laws, regulatory requirements and internal governance standards of the Company.
- 10.2. Revisions may be made in response to:
- Changes in data protection or financial-sector legislation, including amendments to the Law of the Republic of Armenia on Personal Data Protection or the GDPR;
  - Updates in regulatory guidance issued by the Central Bank of Armenia (CBA) or other competent authorities;
  - Modifications to the Company's internal processes, technologies or service offerings that affect Personal Data Processing; or
  - Identified opportunities to strengthen data protection and transparency practices.
- 10.3. The most current and effective version of this Privacy Policy shall always be made available on the Company's official website and mobile application. If you continue to use the Company's website or application after the changes come into force, you will be deemed to have accepted the terms set forth in the revised Policy.
- 10.4. In the event of substantial or material changes that may affect Clients' rights or the manner in which their Personal Data are processed, the Company shall notify Clients in advance via electronic mail, in-app notifications or other appropriate means prior to the changes taking effect.
- 10.5. The Company shall maintain version control and an internal record of all amendments, including the date of approval and the authority responsible for adoption of each revised version.

### **11. Contact Information**

#### **Data Controller:**

Landmark Capital CJSC

Registered Address: Territory 118, Vazgen Sargsyan 10, 0010 Yerevan, Republic of Armenia

Phone: +374 (60) 277-274

Email: [info@landmarkcapital.am](mailto:info@landmarkcapital.am)

Website: [www.landmarkcapital.am](http://www.landmarkcapital.am)

#### **Information Security Officer / Data Protection Officer:**

Email: [information\\_security@landmarkcapital.am](mailto:information_security@landmarkcapital.am)

Postal: Landmark Capital CJSC, DPO Office, Yerevan, Republic of Armenia

#### **Supervisory Authority (RA):**

Personal Data Protection Agency, Ministry of Justice of the Republic of Armenia

Website: [www.mojustice.am](http://www.mojustice.am)