



Gate Securities (Cyprus) Ltd

ex. Sheer Markets (Cyprus) Ltd

PRIVACY POLICY

August 2026

CONTENTS

1. COMPANY INFORMATION	3
2. GENERAL PRINCIPLES.....	3
3. TERMINOLOGY	3
4. LEGAL GROUND FOR PERSONAL DATA PROCESSING	3
5. CATEGORIES OF DATA COLLECTED.....	4
6. HOW THE COMPANY USES DATA.....	5
7. DATA COLLECTED FROM MARKETING ACTIVITIES.....	6
8. AUTOMATED DECISION MAKING (PROFILLING).....	6
9. RETENTION PERIOD.....	7
10. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANASATIONS	7
11. THE SAFETY OF PERSONAL DATA.....	7
12. RIGHTS OF DATA SUBJECTS.....	8
13. RESTRICTION OF RESPONSIBILITY	10
14. REVIEWAL OF THE PRIVACY POLICY.....	10
15. QUERRIES & CONTACT INFORMATION.....	10

1. COMPANY INFORMATION

- 1.1. Gate Securities (Cyprus) LTD (hereafter “the Company” or “Gate Securities”) is a Cyprus Investment Firm (hereafter ‘CIF’) authorized and regulated by the Cyprus Securities and Exchange Commission (hereafter “CySEC”) with License Number 395/20 and operates in compliance to the Investment Services and Activities and Regulated Markets Law 87(I)/2017 and subsequent amendments.

2. GENERAL PRINCIPLES

- 2.1. The Company is committed to protecting all individuals' personal data in compliance with the Regulation (EU) 2016/679 (General Data Protection Regulation - "GDPR") and the Cyprus Law Providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data (Law 125(I)/2018). This commitment applies to all natural persons whose personal data the Company processes.
- 2.2. This Policy details your rights as a data subject regarding the collection, use, disclosure, storage, and protection of your personal data, as well as the legal grounds relied upon by the Company for such processing activities.
- 2.3. The Company acts primarily as a Data Controller in respect of client personal data, as it determines the purposes and means of the processing. Where applicable under relevant legislation, the Company is accountable for, and shall be able to demonstrate compliance with, the principles relating to the processing of personal data (accountability principle).
- 2.4. The Company may engage third-party service providers acting as Data Processors (e.g., IT service providers, administrative agents) or transfer personal data to separate Data Controllers (e.g., banking institutions, executing brokers, regulatory authorities) strictly where necessary for the performance of our contract with you, compliance with legal obligations, or the pursuit of legitimate interest, subject to binding data processing agreements and appropriate safeguards.

3. TERMINOLOGY

- 3.1. For the purposes of this policy.

Personal data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, dispersion indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Profiling: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,

Gate Securities (Cyprus) Ltd (ex. Sheer Markets (Cyprus) Ltd) is authorized and regulated by CySEC under license no.395/20
Head Office: 331, 28th October Avenue, Lido House Block 2, Unit 365, 3106, Limassol, Cyprus
Telephone: (+357) 25861400 Email: support@gate-securities.eu. Web: www.gate-securities.eu

restriction, erasure, or destruction.

4. LEGAL GROUND FOR PERSONAL DATA PROCESSING

4.1. The Company processes personal data only if and to the extent that at least one of the following legal bases applies:

- a) **Consent:** The data subject has given explicit consent to the processing of their personal data for one or more specific purposes.
- b) **Contractual Necessity:** Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.
- c) **Legal Obligation:** Processing is necessary for compliance with a legal or regulatory obligation to which the Company is subject under Applicable Laws.
- d) **Legitimate Interests:** Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject.

4.2. Specifically, the Company collects, records, and processes personal data for the following purposes and relied-upon legal grounds:

- a) **Identity Verification & Client Onboarding (Legal Obligation & Contractual Necessity):** To verify client identity, conduct Customer Due Diligence (CDD), and perform screening to comply with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations prior to establishing a business relationship.
- b) **Knowledge & Experience Assessment (Legal Obligation):** To assess clients' investment knowledge, financial background, and risk tolerance to ensure the appropriateness and suitability of financial instruments offered, as required by investment services legislation.
- c) **Record Keeping (Legal Obligation):** To maintain client records, transaction details, and communications for a statutory retention period of at least 5 years post-account termination, which may be extended up to 7 or 10 years upon request by competent regulatory authorities.
- d) **Transaction Reporting (Legal Obligation):** To report executed financial transactions to regulatory authorities or via Authorized Reporting Mechanisms (ARMs) and trade repositories, implementing data minimization and robust technical safeguards.
- e) **Marketing & Communications (Consent / Legitimate Interest):** To send relevant updates, market analysis, and educational material. Direct marketing via electronic channels relies on prior explicit consent or soft opt-in under applicable ePrivacy rules, giving clients an absolute right to object or opt out at any time.
- f) **Enquiries, Dispute Resolution & Legal Claims (Legal Obligation & Legitimate Interest):** To handle inquiries, respond to judicial processes or regulatory inquiries, and establish, exercise, or defend legal claims.
- g) **Website Analytics & Functional Cookies (Consent):** To monitor website traffic, analyze user navigation habits, and store preferences via non-essential cookies or tracking technologies, subject to explicit consent via our Cookie Policy banner

5. CATEGORIES OF DATA COLLECTED.

5.1. The table below sets out the specific categories of personal data collected and processed by the Company during client onboarding, through website usage, and during the performance of our services, in accordance with our statutory obligations and contractual agreements.

Data Category	Specific Types of Data Collected	Lawful Basis for Processing
Personal Identification Data	Full name, date and place of birth, nationality, national identification number, Tax Identification Number (TIN), gender, and photographic identification documents (e.g., passport, national ID card).	Legal Obligation (AML/KYC laws) & Contractual Necessity
Contact Information	Residential address, email address, telephone number, mobile number, and verified proof of address documentation (e.g., utility bills, bank statements).	Legal Obligation & Contractual Necessity
Financial & Professional Data	Employment status, employer details, source of wealth, source of funds, annual income, estimated net worth, trading history/activity, bank account details, and FATCA/CRS tax status.	Legal Obligation (CySEC/MiFID II/AML rules) & Contractual Necessity
Suitability & Assessment Data	Investment objectives, risk tolerance, financial knowledge, trading experience, professional qualifications, and results of the client suitability/appropriateness evaluation.	Legal Obligation (MiFID II)
Technical & Behavioral Data	IP address, browser type and version, operating system, device identifiers, site usage analytics, cookie data, and logs of electronic communications (e.g., telephone call recordings, emails, live chat logs).	Legitimate Interest, Legal Obligation (recording requirements), & Consent (Cookies)

6. HOW THE COMPANY USES DATA

6.1. All personal data held by the Company is treated as strictly confidential. Access is restricted on a strict need-to-know basis to authorized personnel and processors who require such access to execute their operational duties, fulfill contractual terms, pursue legitimate interests, or ensure compliance with legal obligations.

6.2. The Company may disclose or transfer personal data to third parties only under the following lawful circumstances:

- a) Regulatory & Government Bodies: To the Cyprus Securities and Exchange Commission (CySEC), central banks, law enforcement agencies, tax authorities, or other competent regulatory authorities having jurisdiction over the Company or Client, pursuant to statutory requirements or official orders.
- b) Judicial & Administrative Proceedings: To courts, tribunals, arbitrators, the Financial Ombudsman, or legal advisors where necessary to enforce or defend the Company's legal rights, handle disputes, or comply with court orders.
- c) Financial Institutions & Execution Venues: To payment service providers (PSPs), credit institutions, liquidity providers, and executing brokers to facilitate client fund deposits, withdrawals, order executions, and ancillary financial services.
- d) Professional Advisors & Auditors: To external auditors, legal counsel, compliance consultants, and financial advisors bound by professional secrecy or contractual

- confidentiality obligations.
- e) Third-Party Data Processors: To specialized service providers (e.g., IT hosting, CRM systems, database management, email distribution platforms, KYC/AML screening vendors) acting strictly under written Data Processing Agreements (DPAs) and on the Company's documented instructions.
 - f) Trade Repositories & Regulatory Reporting Venues: To trade repositories, Approved Reporting Mechanisms (ARMs), or competent authorities pursuant to Regulation (EU) No 648/2012 (EMIR) and Regulation (EU) No 600/2014 (MiFIR) for statutory transaction reporting purposes.

7. DATA COLLECTED FROM MARKETING ACTIVITIES.

- 7.1. The Company may process personal data—such as contact information, trading history, and website browsing behavior—to inform existing clients and potential clients about investment products, services, market updates, and promotional offers tailored to their interests.
- 7.2. The personal data processed for marketing purposes includes information directly provided by data subjects, as well as analytical data collected or inferred during the use of our website and services. Automated profiling may be utilized to evaluate individual preferences and trading activity to deliver relevant marketing communications.
- 7.3. The Company conducts promotional and marketing communications strictly under the following lawful grounds:
 - a) Explicit Consent: Where the data subject has provided prior, freely given, specific, informed, and unambiguous opt-in consent to receive electronic marketing communications or allow marketing cookies/tracking.
 - b) Legitimate Interest ("Soft Opt-In"): Where existing clients have previously acquired similar financial services from the Company, provided they were offered a clear opportunity to object to such marketing at the time of data collection and in every subsequent communication.
- 7.4. Data subjects maintain an absolute, unconditional Right to Object at any time to the processing of their personal data for direct marketing purposes, including any profiling conducted for direct marketing. Upon receiving an objection or opt-out request (e.g., clicking "unsubscribe" in an email or adjusting account preference settings), the Company shall immediately cease processing personal data for such purposes without fee or penalty.

8. AUTOMATED DECISION MAKING (PROFILLING).

- 8.1. In accordance with applicable regulatory frameworks, the Company is required to assess prospective clients' investment knowledge, experience, financial situation, and investment objectives prior to providing investment services or opening a trading account.
- 8.2. The Company collects the necessary data to perform these assessments through an Onboarding Questionnaire completed during client registration.
- 8.3. Information submitted in the Onboarding Questionnaire is used to determine client categorization, evaluate risk tolerance, and conduct suitability and appropriateness assessments in accordance with statutory requirements governing investment services.

- 8.4. The evaluation of questionnaire responses may involve automated processing and profiling to determine whether a prospective client meets the eligibility criteria to open an account or trade specific complex financial instruments. Where automated processing results in a rejection or restriction of services, such automated decisions are authorized by law to fulfill mandatory regulatory suitability obligations.
- 8.5. Automated assessment systems are overseen and regularly audited by the Company's Compliance Department. The Company implements strict technical and organizational safeguards—including regular system testing, procedures to correct data inaccuracies, measures to prevent discriminatory effects, and the right for clients to request human intervention, express their point of view, and contest automated decisions.

9. RETENTION PERIOD

- 9.1. Personal data shall be retained only for as long as necessary to fulfill the operational purposes for which it was collected, or to comply with statutory legal, regulatory, and tax obligations. In accordance with applicable financial legislation, client records, identification documents, and transaction history are generally retained for a **minimum** period of five (5) years following the termination of the client relationship or the execution of an occasional transaction.
- 9.2. This statutory retention period may be extended up to a maximum of seven (7) or ten (10) years where explicitly requested by competent regulatory authorities (e.g., CySEC, MOKAS) or as required for the establishment, exercise, or defense of legal claims.
- 9.3. Upon the expiration of the applicable retention period, the Company shall securely erase, destroy, or anonymize the personal data, ensuring it is permanently rendered inaccessible in accordance with technical and organizational security standards.

10. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

- 10.1. Personal data collected by the Company may be transferred to, stored, and processed by third parties located in countries outside the European Economic Area ("EEA")—including foreign banking institutions, liquidity providers, group affiliates, and technical service providers.
- 10.2. Any transfer of personal data to a country or international organization outside the EEA shall be executed strictly in accordance with GDPR Chapter V requirements. The Company ensures that international transfers are covered by at least one of the following recognized transfer mechanisms:
- a) **Adequacy Decisions:** Transfers to third countries, territories, or specified sectors that the European Commission has determined ensure an adequate level of personal data protection.
 - b) **Standard Contractual Clauses (SCCs):** Transfers based on Standard Contractual Clauses adopted by the European Commission, incorporated into binding agreements with data importers, supplemented by technical, organizational, and security safeguards.
 - c) **EU-U.S. Data Privacy Framework:** Transfers to certified organizations in the United States adhering to the EU-U.S. Data Privacy Framework adequacy decision.
 - d) **Derogations for Specific Situations:** In the absence of an adequacy decision or standard safeguards, transfers are executed strictly under specific GDPR Article 49 derogations, such

as where the transfer is necessary for the performance of a contract with the client, the execution of client orders, or for the establishment, exercise, or defense of legal claims.

10.3. Data subjects may contact the Company's Data Protection Officer to request a copy of the appropriate transfer safeguards or details regarding third-country mechanisms implemented by the Company.

11. THE SAFETY OF PERSONAL DATA

11.1. The Company implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, protecting personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These security controls adhere to the principles of Data Protection by Design and by Default, ensuring that only personal data necessary for each specific processing purpose is collected and accessed.

11.2. Technical and organizational security safeguards implemented by the Company include, but are not limited to:

- a) Data Encryption: Industry-standard pseudonymization and cryptographic encryption protocols for data in transit (e.g., TLS/SSL) and data at rest (e.g., AES-256).
- b) Access Control Management: Strict Role-Based Access Control (RBAC) mechanisms, multi-factor authentication (MFA), and least-privilege principles to govern access to application environments, databases, and system networks.
- c) Clean Desk & Clear Screen Policies: Strict administrative and physical controls mandating the secure disposal or shredding of physical documents containing personal data and requiring screen lock mechanisms on all workstations and mobile devices.
- d) Business Continuity & Disaster Recovery: Structured operational frameworks, off-site system backups, and failover capabilities to ensure continuous service availability and timely restoration of personal data access following physical or technical incidents.
- e) IT Risk Assessments & Vulnerability Management: Periodic penetration testing, network monitoring, and threat impact assessments to identify and mitigate operational or cybersecurity risks.
- f) Physical & Logical Access Segregation: Physical perimeter security controls at office facilities alongside network segmentation and logical access barriers separating development, production, and storage environments.
- g) Incident Management & Data Breach Notification: Standardized incident response protocols establishing clear operational responsibilities to detect, contain, and remediate security breaches, including statutory notification mechanisms.

11.3. Access to client personal data is restricted strictly to employees, agents, contractors, and third-party processors who have a legitimate business need to know. All authorized personnel process personal data strictly in accordance with documented instructions from the Company and are bound by contractual duties of confidentiality.

12. RIGHTS OF DATA SUBJECTS

12.1. **Right of Access:** Data subjects have the right to request confirmation as to whether their personal data is being processed, obtain access to such data, and receive a copy along with supplementary details regarding the processing scope.

12.2. **Right to Rectification:** Data subjects have the right to request the prompt correction of inaccurate personal data or the completion of incomplete personal data held by the Company.

12.3. **Right to Erasure ("Right to be Forgotten"):** Data subjects have the right to request the Gate Securities (Cyprus) Ltd (ex. Sheer Markets (Cyprus) Ltd) is authorized and regulated by CySEC under license no.395/20
Head Office: 331, 28th October Avenue, Lido House Block 2, Unit 365, 3106, Limassol, Cyprus
Telephone: (+357) 25861400 Email: support@gate-securities.eu Web: www.gate-securities.eu

- erasure of their personal data where the data is no longer necessary for the original collection purposes, consent has been withdrawn, or the processing lacks a legal basis.
- 12.4. Exceptions to Erasure:** Paragraph 12.3 shall not apply to the extent that retention is necessary:
- a) For compliance with a statutory legal obligation under applicable Union, CySEC, or national laws to which the Company is subject;
 - b) For the establishment, exercise, or defense of legal claims;
 - c) For reasons of public interest in the area of public health or statutory archiving obligations.
- 12.5. Right to Restriction of Processing:** Data subjects have the right to request the restriction of processing where the accuracy of the data is contested, the processing is unlawful, or the Company no longer needs the data but it is required for legal claims.
- 12.6.** Where processing has been restricted under paragraph 12.5, such personal data shall— with the exception of storage—only be processed with the data subject's explicit consent, for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person.
- 12.7. Right to Data Portability:** Data subjects have the right to receive their personal data provided to the Company in a structured, commonly used, and machine-readable format, and have the right to transmit that data to another controller without hindrance, where processing is based on consent or contract.
- 12.8. Right to Object:** Data subjects have the right to object, on grounds relating to their particular situation, at any time to processing based on the legitimate interests of the Company or a third party. The Company shall cease processing unless it demonstrates compelling legitimate grounds that override the subject's fundamental rights and freedoms.
- 12.9. Direct Marketing Objection:** Data subjects have an absolute right to object at any time to the processing of their personal data for direct marketing purposes, including profiling related to direct marketing. Upon receipt of such objection, direct marketing processing shall cease immediately.
- 12.10. Right Not to be Subject to Automated Decision-Making:** Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless authorized by law or contract with appropriate human intervention safeguards.
- 12.11. Right to Withdraw Consent:** Where processing is based on consent, data subjects have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- 12.12. Impact of Withdrawal:** If a data subject withdraws consent for processing essential to service provision, the Company may be unable to continue providing certain investment services or maintain the contractual agreement. The Company shall inform the data subject of the specific operational and contractual consequences prior to executing the withdrawal request.
- 12.13. Right to Lodge a Complaint:** Data subjects have the right to lodge a complaint with a supervisory authority, specifically the Office of the Commissioner for Personal Data Protection in Cyprus, if they consider that the processing of their personal data infringes applicable data protection regulations.

13. RESTRICTION OF RESPONSIBILITY

- 13.1. **Third-Party Websites and Services:** The Company's website, platforms, or applications may contain hyperlinks to external third-party websites, plug-ins, or applications. The Company does not operate, control, or endorse these third-party platforms and assumes no responsibility for their operational practices, content, security protocols, or privacy policies.
- 13.2. **Limitation of Liability for External Data Collection:** The Company shall not be held liable for any personal data or information provided by the client to, or collected by, any unoperated third-party websites. Any data submitted to or collected by external platforms is recorded independently by those third parties and remains strictly governed by their respective terms of service and privacy notices.
- 13.3. **Client Due Diligence:** Whenever a client leaves the Company's platform or follows a link to an external site, the Company strongly encourages the client to review the privacy statement and data protection terms of each third-party website visited prior to providing any personal data.

14. REVIEW AND AMENDMENTS OF THE PRIVACY POLICY

- 14.1. **Periodic Review:** To ensure this Privacy Policy remains fully compliant with evolving statutory obligations under applicable data protection regulations and reflects changes in Company operations, services, or processing practices, this Privacy Policy shall be subject to regular periodic review and may be updated or amended at any time.
- 14.2. **Notification of Material Changes:** Where material changes are made to this Privacy Policy that significantly affect data subjects' rights or the scope of processing, the Company shall provide advance notice through prominent channels—such as website publication, account notifications, or direct email communication.
- 14.3. **Applicability:** The most current version published on the Company's website shall govern the processing of all personal data held by the Company. Data subjects are encouraged to review the Privacy Policy periodically to stay informed about how their personal data is protected.

15. QUERIES AND CONTACT DETAILS

- 15.1. **Contact Information:** Any inquiries, requests to exercise data subject rights under Section 12, or complaints concerning the processing of personal data and the contents of this Privacy Policy should be directed to the Company's Data Protection Officer (DPO) using the following contact details:
- Attention: Data Protection Officer
 - Email: dpo@gate-securities.eu
- 15.2. **Response Timeline:** The Company shall acknowledge receipt and respond to any request or query without undue delay and, in any event, within one (1) month of receiving a verified request. That period may be extended by two (2) further months where necessary, taking into account the complexity and number of the requests, provided the data subject is informed of any such extension within the initial month.

DATE: 31.08.2026