GDPR DATA PROTECTION POLICY

ABF Trade EU Limited

Version	v1.0
Effective Date	12 May 2026
Review Date	12 May 2027
Document Reference	ABF-DPP-001
CySEC Licence	171/12

ABF Trade EU Limited
162 Fragklinou Rousvelt, 1st & 2nd Floors
Limassol 3045, Cyprus
CySEC Licence No. 171/12
www.abftrade.com/eu

Table of Contents

Document Control

Version	Date	Description	Approved By
v1.0	12 May 2026	Initial version for ABF Trade EU Limited	Board of Directors

1. Policy Statement

ABF Trade EU Limited ("the Company") is committed to protecting the privacy and personal data of its clients, employees, and other stakeholders, and to processing all personal data in accordance with applicable data protection legislation, including the EU General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and the Cyprus Data Protection Law (Law 125(I)/2018).

This GDPR Data Protection Policy sets out the Company's approach to the collection, use, storage, and protection of personal data, and describes the rights of individuals in relation to their personal data. This Policy applies to all personal data processed by the Company, whether held in paper or electronic form.

This Policy should be read in conjunction with the Company's Privacy Policy, which is also available on the Website. This Policy governs the Company's data protection practices and the obligations of all personnel.

2. Grounds for Data Collection

The Company collects and processes personal data only where it has a lawful basis to do so under GDPR. Processing of personal data is lawful where at least one of the following conditions applies:

- Consent: The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Contractual necessity: Processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract.
- Legal obligation: Processing is necessary for compliance with a legal obligation to which the Company is subject.
- Vital interests: Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Public task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- 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 interests or fundamental rights and freedoms of the data subject.

3. Personal Information Collected

The Company collects and processes the following categories of personal information, although the specific information collected will depend on the context of the relationship with the individual:

3.1 Identity Information

First name, maiden name, last name, proof of identity (including passport, national ID card, or other government-issued document), username or similar identifier, marital status, date of birth, and nationality.

3.2 Contact Information

Address (residential and, where applicable, business), telephone numbers, and email addresses.

3.3 Personal Data

Data about age, ethnicity, gender, and nationality (to the extent relevant and where legally required, for example for AML/KYC purposes).

3.4 Financial Information

Annual income, net worth, source of funds, anticipated account turnover, bank account details, and financial history. This information is collected for the purposes of KYC, AML/CTF compliance, and the provision of investment services.

3.5 Transaction Information

Details about payments to and from the individual and other details of products and services purchased from the Company, including trading history, account statements, and settlement records.

3.6 Marketing and Communication Information

Preferences in receiving marketing communications from the Company, and communication preferences.

3.7 Non-Personal Information

We also record and collect data from or about the devices (for example, computers or mobile devices) through which individuals access our website and trading platform, including IP addresses, browser type and version, operating system, and usage data. This information may be used to improve our services and to ensure the security of our systems.

4. Purposes of Processing

The Company uses and processes personal information to:

- Carry out its statutory and regulatory functions, including KYC verification, AML/CTF screening, and reporting to CySEC and other regulatory authorities.
- Handle complaints and resolve disputes.
- Conduct investigations as required by applicable law.
- Improve and develop its services and technology platforms.
- Share information with third parties for the purpose of obtaining professional advice and in compliance with contractual obligations.
- Send information to clients that is relevant to their use of the Company's services, including account statements, trade confirmations, and regulatory disclosures.
- Comply with all legal and regulatory obligations applicable to the Company.
- Assess the appropriateness or suitability of the Company's services for a particular client.

5. Automated Decision-Making and Profiling

In order to perform the contract between the Company and its clients, and as authorised by applicable regulations (including Directive 2014/65/EU (MiFID II), the Law, and applicable CySEC Directives), the Company uses certain automated processes in relation to the following:

- Appropriateness Test: This test takes place when a prospective client applies to register as a client of the Company. The test assesses whether the client has sufficient knowledge and experience to understand the risks associated with CFD trading. The result of this automated assessment may affect the services that the Company is able to offer to the client.
- Suitability Test: This test takes place when a client requests portfolio management services. The Company assesses the client's investment objectives, risk tolerance, financial situation, and investment knowledge to determine whether portfolio management is suitable for that client.

Where automated decision-making produces legal or similarly significant effects for an individual, the individual has the right to request human review of the decision, to express their point of view, and to contest the decision. For further information, please contact the Company at the details set out below.

6. Data Protection Principles

The Company processes personal data in accordance with the following GDPR data protection principles:

- Lawfulness, fairness, and transparency: Personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Purpose limitation: Personal data is obtained for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation: Personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accuracy: Personal data is accurate and, where necessary, kept up to date. The Company takes every reasonable step to ensure that inaccurate personal data is erased or rectified without delay.
- Storage limitation: Personal data is not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed, subject to applicable regulatory retention requirements.
- Integrity and confidentiality: Personal data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures.
- Accountability: The Company is responsible for and can demonstrate compliance with the data protection principles.

7. Security of Processing

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risks to the rights and freedoms of natural persons, the Company implements appropriate technical and organisational security measures, including:

- The pseudonymisation and encryption of personal data where appropriate.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
- Access controls and authentication procedures, ensuring that only authorised personnel can access personal data, and only to the extent necessary for their role.
- Secure disposal of personal data when it is no longer required.

8. Guidelines for Company Personnel

All Company personnel who handle personal data are required to comply with the following guidelines:

- Only personnel who need access to personal data for their specific work responsibilities should have such access.
- Personal data must not be shared informally. When access to confidential information is required, employees must make a formal request to their line manager or the Compliance/DPO function.

- All employees receive training to help them understand their responsibilities when handling personal data.
- Employees must keep personal data secure by taking sensible precautions and following the Company's information security guidelines.
- Strong, unique passwords must be used for all systems containing personal data and must never be shared.
- Personal data must not be disclosed to unauthorised persons, either within the Company or externally.
- Personal data must be regularly reviewed and updated where it is found to be out of date. If no longer required and the retention period has expired, it must be deleted securely.
- Computer screens must always be locked when left unattended.
- Personal data must be encrypted before being transferred electronically outside the Company's secure network.
- Any suspected breach of personal data security must be reported immediately to the Data Protection Officer.

9. Data Breach Response

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

In the event of a personal data breach, the Company will:

- Contain the breach and recover the personal data where possible.
- Assess the likely risk to individuals and determine the severity of the breach.
- Notify the Office of the Commissioner for Personal Data Protection of Cyprus within 72 hours of becoming aware of the breach, where the breach is likely to result in a risk to the rights and freedoms of natural persons.
- Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.
- Document the breach, its effects, and the remedial action taken.

10. Rights of Data Subjects

Under GDPR, individuals whose personal data we process have the following rights:

- Right of access (Article 15): The right to obtain a copy of their personal data and supplementary information about how we process it.
- Right to rectification (Article 16): The right to have inaccurate personal data rectified, or to have incomplete data completed.
- Right to erasure (Article 17): The right to have personal data erased in certain circumstances ('right to be forgotten').
- Right to restriction of processing (Article 18): The right to request that we restrict the processing of their personal data in certain circumstances.
- Right to data portability (Article 20): The right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller.
- Right to object (Article 21): The right to object to processing based on legitimate interests or public task, and to direct marketing.
- Rights in relation to automated decision-making and profiling (Article 22): The right not to be subject to solely automated decisions that have a legal or similarly significant effect, and to request human review.

Requests to exercise any of the above rights must be submitted in writing to:

Data Protection Officer, ABF Trade EU Limited

162 Fragklinou Rousvelt, 1st & 2nd Floors, Limassol 3045, Cyprus

Email: support@abftrade.com

The Company will respond to all valid requests within one month of receipt. In complex cases, this period may be extended by a further two months, and the data subject will be notified of any extension.

11. Cooperation with Supervisory Authorities

The Company cooperates with the Office of the Commissioner for Personal Data Protection of Cyprus (the "Supervisory Authority") in the performance of its tasks. Where required by law, the Company will consult with and notify the Supervisory Authority in connection with data protection matters, including data breach notifications and Data Protection Impact Assessments.

If a data subject is not satisfied with the Company's response to a request or complaint, they have the right to lodge a complaint with the Supervisory Authority:

Office of the Commissioner for Personal Data Protection

1 Iasonos Street, 1082 Nicosia, Cyprus

P.O. Box 23378, 1682 Nicosia, Cyprus

Tel: +357 22 818 456

Website: www.dataprotection.gov.cy

Email: commissioner@dataprotection.gov.cy

12. Data Protection Officer

The Company has appointed a Data Protection Officer ("DPO") whose responsibilities include:

- Informing and advising the Company and its employees of their obligations under applicable data protection legislation.
- Monitoring compliance with GDPR and other applicable data protection law, and with the Company's own data protection policies.
- Providing advice where requested with regard to Data Protection Impact Assessments and monitoring their performance.
- Cooperating with the Supervisory Authority and acting as the contact point for the Supervisory Authority on issues relating to the processing of personal data.

Any questions about this Policy or data protection matters should be directed to the Data Protection Officer at: support@abftrade.com

13. Amendments

This Policy will be reviewed at least annually or when there is a change in applicable data protection law, the Company's business activities, or the technology used for processing personal data. Any material changes to this Policy will be communicated to relevant personnel.

This Policy is effective from 12 May 2026 and supersedes any previous versions.