Suite 305, Griffith Corporate Centre, Kingstown,
St. Vincent and Grenadines
info@abtrade.org
+1 408 8786818

PRIVACY POLICY

AB TRADE COMPANY

1.The client automatically accepts the terms of this Policy upon acceptance of the Investment support offer, which is available on the official site of the Company: http://abtrade.org/. The Client is taken to have read and agreed to the Privacy Policy and responsible for accepting the terms of this Policy. The Client agrees to the processing of his/her personal data.

2.This policy aims to regulate the processing of Clients' personal data, which is provided in documentary and/or computerized databases.

3.The Company may act as the Personal Data Operator, as well as the Company has the right to entrust the processing of personal data to a third party under the signed agreement. If the Company entrusts the processing of personal data to another Personal Data Operator, the Company shall be responsible for the actions taken by Personal Data Operator. In its term, the Personal Data Operator that processes personal data on behalf of the Company bears full responsibility for its actions. The Personal Data Operator is required to comply with the principles and rules of the personal data processing established by the Company.

4.Personal data used for processing under this Privacy Policy is provided by filling in the appropriate form when registering the Client's personal account on the site of the Company: http://abtrade.org/.

5.The content and volume of processed personal data must comply with the declared processing goals and legal principles established by law.

6.The Company aims to protect the rights and freedoms of the Clients while processing their personal data, including the protection of privacy and the confidentiality of this information.

7.The personal data must be processed legitimately, and its processing is limited to achieving specific, predetermined and legitimate goals.

8.The Personal Data Operator must ensure the accuracy, sufficiency, and relevance of personal data. The Personal Data Operator takes all the necessary measures deleting inaccurate or clarifying incomplete data.

9.Personal data is stored in documentary and/or electronic forms in the specially organized depository for a period of five years.

10.The Personal Data Operator and other persons who have gained access to personal data are required not to disclose to third parties and not to distribute personal data without the consent of the subject of personal data unless otherwise is provided by law.

11.The cross-border transfer of personal data is carried out to execute the agreement, or to protect the life, health, other vital interests of the Counterparty or third parties if it is not possible to obtain written consent of the Counterparty in

cases stipulated by law. Prior to the cross-border transfer of personal data and its further processing, the Company guarantees adequate protection of the rights of the subject of personal data and is also obliged to make sure that the foreign state into whose territory personal data is transferred, provides adequate protection of the rights of the personal data subjects. Cross-border transfer of personal data in foreign countries that do not provide adequate protection, can be carried out in the cases of:

- obtaining the written consent of the personal data subject on the cross-border transfer of personal data;
- execution of a contract to which the subject of personal data is a party.

12.It is forbidden to disclose personal data to third parties, except when it is necessary to prevent a threat to the life and health of the subject of personal data, as well as in cases provided by law. It is forbidden to disclose personal data for any purposes that are not consistent with the purposes of this Policy.

13.The Personal Data Operator is obliged to notify the persons receiving personal information that this data can only be used for special purposes and require written confirmation from these persons (or confirmation issued in electronic form) that rule is followed. Persons receiving personal data are required to maintain confidentiality.

14.The Personal Data Operator is obliged to assign an official, responsible for ensuring the security of personal data. An official (employee) controls the transfer of necessary and sufficient personal data to perform specific purposes provided for in the Policy.

15.The company and the persons responsible for the processing of personal data are required to take all necessary measures to counteract actual threats to the security of personal data, including:

- unauthorized access to personal data during the creation, operation, maintenance and (or) repair, modernization, decommissioning of the personal data;
- the impact of malicious code external to the personal data information system;
- unauthorized access to the personal data carriers;
- loss of personal data carriers, including portable personal computers of users;
- unauthorized access to personal data, using vulnerabilities in the organization of personal data protection;
- unauthorized access to personal data, using vulnerabilities in the software;
- unauthorized access to personal data, using vulnerabilities in ensuring

the protection of network interaction and data transmission channels;

•unauthorized access to personal data, using vulnerabilities in ensuring the protection of computer networks;

•unauthorized access to personal data, using vulnerabilities caused by non-compliance with the cryptographic protection means.

16. The operator ensures the security of personal data.

The security of personal data processed by the Personal Data Operator is ensured by the implementation of legal, organizational and technical measures necessary in accordance with the personal data protection legislation. To prevent unauthorized access to personal data by the Operator, the following organizational and technical measures are applied:

•the appointment of officials responsible for organizing the processing and protection of personal data;

- limiting the number of persons having access to personal data;

•familiarization of subjects with the requirements of legislation and regulatory documents of the Personal Data Operator for the processing and protection of personal data;

•organization of accounting, storage, and circulation of information carriers;

•verification of the readiness and effectiveness of the use of information security tools;

•differentiation of user access to information resources and software and hardware information processing;

•registration and accounting of actions of users of personal data information systems;

•use of anti-virus and recovery tools for the system of protection of personal data;

•the use of necessary means of firewalling, intrusion detection, security analysis and cryptographic protection of information; ensuring the safety of personal data carriers;

•organization of access control to the Personal Data Operator's territory, the security of premises with technical means for processing personal data.

17.In the case of illegal processing of personal data, the Personal Data Operator is obliged to block improperly processed personal data or to ensure their blocking upon receipt of such a report. In the event that inaccurate personal data is detected by the subject of personal data, the Personal Data Operator is obliged to block personal data related to such an entity or to ensure their blocking upon receipt of

such a report if the blocking of Personal data does not violate the rights and legitimate interests of the specified entity or other persons.

18.In the case of inaccuracy of personal data, the Personal Data Operator is obliged to clarify personal data or to ensure their clarification within seven working days from the date of submission of such information.

19.In case the Company detects illegal processing of personal data by the Personal Data Operator, as well as by third parties, such persons must stop illegal processing of personal data within three business days from the date of such detection. If it is not possible to ensure the legitimacy of the processing of personal data, these persons must destroy such personal data or ensure its destruction within a period not exceeding 3 working days from the date of detection of illegal processing of personal data. These persons shall notify the Company of the elimination of violations or the destruction of personal data.

20.Having achieved the goals of personal data processing, the Personal Data Operator must stop processing personal data or ensure its termination and destroy personal data or ensure their destruction.

21.If the Client withdraws his/her consent to the processing of personal data, the Personal Data Operator must stop processing personal data or ensure its termination, and also if the storage of personal data is no longer required, destroy personal data or ensure its destruction. Revocation of consent to the processing of their personal data may be submitted personally to the Personal Data Operator in writing, or through their representative, or through electronic communication.

22.In case of loss or disclosure of personal data, the Personal Data Operator shall immediately inform the parties.

23.The Personal Data Operator must ensure the confidentiality and security of material carriers of personal data and exclude unauthorized access to them from the moment of acquisition of the data until the expiration of their storage period and further destruction. In order to protect the confidentiality of personal data, the Company provides all necessary legal support, including appealing to the competent authorities, international organizations, and officials.

24.Violation of the law regarding the processing of personal data entails legal liability in accordance with applicable law, including in the event of unauthorized or accidental access to personal data of third parties.