Privacy Policy

1. Introduction

1.1 In order to service our clients E-Global Trade & Finance Group, Inc., Legal address: First Floor, Mandar House, Johnson's Ghut, P.O. Box 3257, Road Town, Tortola, British Virgin Islands, Reg. No.: 1384287 (the "Company" "we" or "us"), needs to collect personal data from our clients and/or potential clients, agents, contractors, partners and employees.

In light of the above, the Company wants to ensure a high level of data protection as privacy is a cornerstone in gaining and maintaining the trust of our clients, employees and other concerned parties, thus ensuring the Company's future business.

Protection of personal data requires that appropriate technical and organizational measures are taken to demonstrate a high level of data protection. The Company has adopted the necessary data protection policies and procedures, which must be followed by employees of the Company.

Where appropriate, the Company will monitor, audit and document internal compliance with the data protection policies and applicable statutory data protection requirements.

The Company will also take the necessary steps in order to enhance data protection compliance within the organisation. These steps include the assignment of responsibilities, raising awareness and training of staff involved in processing operations. Please note that this privacy policy will be reviewed as necessary to take into account any new obligations. Retention and processing of personal data will be governed by our most recent policy.

This privacy policy, along with internal procedures, constitutes the overall framework for processing personal data within the Company.

1.2 "Personal data" is any information which may be related to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, location data, phone number, age, gender, an employee, a job applicant, clients, suppliers and other business partners. This also includes special categories of personal data (sensitive personal data) and confidential information such as health information, account number, identification number,

location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. We may collect, use, store and transfer various kinds of your personal data, such as, but not limited to:

- Identity Data such as first name, last name, proof of identity, username or similar identifier, title, date and place of birth, gender, country of residence and citizenship.
- Contact Data such as billing address, email address, telephone number(s), proof of address.
- Professional Data such as level of education, profession, employer name, work experience, financial awareness, trading experience.
- Tax Data such as country of tax residence, tax identification number.
- Financial Data such as annual income, net worth, source of funds, anticipated account turnover, bank account, bank statements, payment card details and copy thereof, e-wallet information.
- Transaction Data such as details about payments to and from you, information on products and services you have purchased from us, deposit methods, purpose of transactions with us.
- Technical Data such as device ID, internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access website and our services.
- Profile Data such as your username and password, purchases or orders made by you, your interests, preferences, feedback, survey responses.
- Usage Data such as information about how you use our website, products, services, app interactions, in-app search history, app installation state, other related activities.
- Marketing and Communications Data such as your preferences in receiving marketing from us and any third-party companies on our behalf and your communication preferences.
- User-generated images, videos, and screenshots such as those uploaded by users of the application to help diagnose technical problems via support services. Such images are only used for the purpose of providing technical support.

1.3 For a better experience with our services, we may require you to provide us with certain personally identifiable information as noted above. The information that we request will be

retained by us and used as described in this privacy policy. In addition, the app does use third-party services that may collect information used to identify you. Link to the privacy policy of third-party service providers used by the app is provided below:

- Google Play Services
- Google Analytics for Firebase
- Firebase Crashlytics
- Instabug
- Branch

1.4 Whenever you use our services and an error occurs in the app, we collect data such as crash logs, diagnostic information, other app performance data, and information (through third-party products) on your phone called Log Data. This Log Data may include information such as your device ID, Internet Protocol ("IP") address, device name, operating system version, the configuration of the app when utilizing our Service, the time and date of your use of the services, and other statistics. This information helps us analyze the error and fix it.

1.5 The Company collects and uses personal data for a variety of legitimate business purposes, including establishment and management of customer and supplier relationships, completion of purchase agreements, recruitment and management of all aspects of terms and conditions of employment, communication, fulfilment of legal obligations or requirements, performance of contracts, providing services to clients, etc.

1.6 Although information regarding companies/businesses is not as such personal data, please note that information relating to contacts within such companies/businesses, e.g., name, title, work email, work phone number, etc. is considered personal data.

1.7 Personal data shall always be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which data are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which data are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.8 The Company is responsible for the above as part of the Company's compliance policy.

---

2. Legal basis for processing personal data

2.1 Processing of personal data requires a legal basis. The most predominant legal basis for processing personal data within the Company are:

- Consent from the data subject(s) for one or more specific purposes;
- The performance of a contract to which the data subject is party;
- A legal obligation or requirement;
- Legitimate interests pursued by the Company.

2.2 Consent

2.2.1 If the collection, registration and further processing of personal data regarding clients, suppliers, other business relations and employees are based on such a person's consent to the processing of personal data for one or more specific purposes, the Company shall be able to demonstrate that the data subject has consented to processing of such personal data.

2.2.2 Consent shall be: freely given, specific, informed and unambiguous. The data subject must actively consent to the processing of personal data by a statement or by a clear affirmative action.

2.2.3 A request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

2.2.4 To process special categories of personal data (sensitive personal data) the consent shall also be explicit.

2.2.5 The data subject is entitled to withdraw consent at any time and upon such withdrawal, we will stop collecting and/or processing personal data about the data subject unless we are obligated or entitled to do so based on another legal basis.

2.3 Performance of a contract:

2.3.1 It will be legitimate to collect and process personal data relevant to 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. This applies to all contractual obligations and agreements signed with the Company, including the pre-contractual phase irrespective of the success of the contract negotiations.

2.4 Compliance with a legal obligation

2.4.1 The Company must comply with various legal obligations and requirements, which are based on applicable law. Such legal obligations, to which the Company is subject, may be sufficient as a legitimate basis for the processing of personal data.

2.4.2 Such legal obligations include obligations to collect, register and/or make available certain types of information relating to employees, clients, etc. Such legal requirements will then form the legal basis for us to process the personal data, however, it is important to note whether the provisions allowing or requiring the Company to process certain personal data also set out requirements in relation to storage, disclosure and deletion.

2.5 Legitimate interests

2.5.1 Data will only be processed where it is necessary for the purposes of the legitimate interests pursued by the Company, and these interests or fundamental rights are not overridden by the interests of the data subject. The Company will, when deciding to process data, ensure that the legitimate interests do not override the rights and freedoms of the individual and that processing will not cause unwarranted harm. An example of legitimate interest of the Company is to process personal data on potential clients in order to expand the business and develop new business relations. The data subject must be given information on the specific legitimate interest if a processing is based on this provision, cf. section 4.1 below.

3. Processing and transfer of personal data

3.1 The Company as the Data Controller

3.1.1 The Company will be considered a data controller to the extent that we decide by which means the data subject's personal data shall be processed, e.g., when a data subject signs an agreement with the Company.

3.2 Use of data processors

3.2.1 An external data processor is a company which processes personal data on behalf of the Company and in accordance with the Company's instructions, e.g., in relation to HR systems, third party IT providers, etc. When the Company outsources processing of personal data to data processors, the Company ensures that this external data processor, at a minimum, applies the same degree of data protection as the Company. If this cannot be guaranteed, the Company will choose another data processor.

3.3 Data processing agreements

3.3.1 Prior to transfer of personal data to the data processor, the Company enters into a written data processing agreement with the data processor. The data processing agreement ensures that the Company controls and is responsible for the processing of personal data, which takes place outside of the Company.

3.3.2 If the data processor/sub-data processor is located outside of the EU/EEA, the conditions of clause 3.4.4 below will apply.

3.4 Disclosure of personal data

3.4.1 Before disclosing personal data to others, it is the responsibility of the Company to consider whether the recipient is employed by us or not. Furthermore, we may only share personal data within the Company if the disclosure is based on a legitimate business purpose.

3.4.2 The Company's ensures that the recipient has a legitimate purpose for receiving personal data, and sharing of personal data is restricted and kept to a minimum.

3.4.3 The Company uses caution before sharing personal data with persons, data subjects or entities outside of the Company. Personal data may only be disclosed to third parties acting as

individual data controllers if a legitimate purpose for such data transfer exists. If the recipient is acting as a data processor, please refer to clause 3.2 above.

3.4.4 If the third party recipient is located outside the EU/EEA in a country that does not ensure an adequate level of data protection, the transfer can only be completed if a transfer agreement has been entered into between the Company and the third party. The transfer agreement is based on the EU Standard Contractual Clauses.

---

4. Rights of data subjects

4.1 Duty of information

4.1.1 When the Company collects and registers personal data on data subjects, the Company is obligated to inform such persons about:

- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The categories of personal data concerned;
- The legitimate interests pursued by the Company, if the processing is based on a balancing of interests;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, the fact that the Company intends to transfer personal data to a third country and the legal basis for such transfer;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the Company access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- Where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- The right to lodge a complaint with the Company via the correct procedure or with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.2 Right to access

4.2.1 Any person whose personal data the Company is processing, including but not limited to, the Company's employees, job applicants, external suppliers, clients, potential clients, business partners, etc. has the right to request access to personal data which the Company processes or stores about this particular person.

4.2.2 If the Company processes or stores personal data about the data subject, the data subject shall have the right to access the personal data and inquire of the reasons for the data to be processed in relation to the criteria set out in 4.1.1.

4.3 The data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning the data subject.

4.4 The data subject shall have the right to obtain from the Company erasure of personal data concerning the data subject, and the Company has the obligation to erase personal data without undue delay, unless it is required by law to retain any information for a prescribed period of time, for example, by financial regulators, employment laws or tax authorities.

4.5 The data subject shall have the right to obtain from the Company processing restriction, if applicable.

4.6 The data subject shall have the right to receive the personal data registered in a structured and commonly used and machine-readable format.

4.7 The data subject shall have the right to object, on grounds relating to the data subject's particular situation, at any time to processing of personal data concerning the data subject which is based on a balancing of interests, including profiling.

4.8 Any requests received from a data subject to exercise the rights in this clause will be answered as soon as reasonably possible, and no later than 30 days from the date of receipt. Requests shall be forwarded without delay to the Company's Privacy Team. The Privacy Team, if necessary, will be supported by the Company's engaged Data Protection Officer to process the request to meet the reply deadline.

---

5. Data Protection by Design and Data Protection by Default

5.1 New products, services, technical solutions, etc. must be designed so they meet the principles of data protection by design and data protection by default settings.

5.1.1 Data protection by design means that when designing new products or services, key considerations to data protection must be shown.

- The Company will take the following factors into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and impact on rights and freedoms of natural persons posed by the data processing.
- The Company, both at the time of the determination of the means for processing and at the time of the processing itself, implements appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet data protection requirements and protect the rights of data subjects.

5.1.2 Data protection by default requires that relevant data minimisation techniques are implemented.

- The Company implements appropriate technical and organisational measures ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.
- This minimisation requirement applies to the amount of personal data collected, the extent of data processing, the period of data storage and data accessibility.
- Such measures shall ensure that by default, personal data is not made accessible without careful consideration.

6. Records of processing activities

6.1 The Company as a data controller maintains records of processing activities under the Company's responsibility. The records shall contain the following information:

- name and contact details;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country, including the identification of that third country and, if relevant, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the applied technical and organisational security measures.

6.2 The Company shall make the records available to relevant data protection authorities upon request.

7. Deletion of personal data

7.1 Personal data shall be deleted when the Company no longer has a legitimate purpose for the continuous processing or storage of the personal data, or when it is no longer required to store the personal data in accordance with applicable laws and regulations.

7.2 Detailed retention periods with respect to various categories of personal data are specified in the Company's Data Retention and Information Sharing policy.

7.3 In compliance with privacy regulation and subject to clause 7.1 above, the Company's clients/potential clients have the right to request personal information relating to their account with the Company be deleted or anonymised when the client relationship with Company has

ended, unless the Company is required by law to retain any information for a prescribed period of time, for example, by financial regulators, employment laws or tax authorities.

7.4 The Company will balance the privacy rights of its clients/potential clients with other requirements of applicable regulations taking precedence over the deletion requirement. The registration of personal data in the Company's systems is regulated by a wide range of various legal requirements such as financial, bookkeeping rules, consumer protection, employment laws, KYC obligations, etc.

7.5 Personal data will be deleted or anonymised when there is no longer any legal basis for keeping it. The typical deletion deadline for clients is the current year plus five (5) years after the end of a client relationship.

7.6 For Company's potential clients, personal data relating to their engagement with Company will delete or anonymised upon their request and as soon as possible, but please be advised that it may take up to one (1) month to provide initial reply with such request and up to three (3) months to entirely process with such request.

7.7 Personal information about the Company's clients/potential clients who have incurred a loss to Company may be stored for a longer period of time to protect the Company from further loss or for the purpose of pursuing or preserving rights to a legitimate claim.

7.8 The Company will permanently delete or anonymise all personal data when required to by applicable laws and regulations.

---

8. Assessment of risk

8.1 If the Company processes personal data that is likely to result in a high risk for the persons whose personal data is being processed, a Data Protection Impact Assessment ("DPIA") shall be carried out.

8.1.1 A DPIA implies that the Company will, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with data protection requirements.

8.2 The technical and organisational measures shall be reviewed and updated where necessary.

8.2.1 Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the appropriate technical and organisational measures pursuant to this clause.

---

9. Profiling

9.1 “Profiling” in the context of this Privacy Policy is the use of an automated process to analyse personal data in order to assess or predict aspects of a person’s behaviour. The Company may use profiling in the following circumstances:

- To help identify potential cases of financial crime;

- To provide clients and leads with information on the Company’s products and services that seem likely to be of their interest;
- To assess creditworthiness.

---

10. National requirements

10.1 The Company shall comply with relevant data protection legislation, as applicable.

10.2 If national legislation requires a higher level of protection for personal data, such stricter requirements are to be complied with. If the Company’s policies/guidelines are stricter than the local legislation, our policies/guidelines must be complied with.

---

11. Contact and complaints

11.1 If you have any questions regarding the content of this policy, please contact Company at privacy@egobal-group.com.

11.2 If you would like to file a complaint about the Company's processing of personal data, you may contact the appropriate Data Protection Agency in the respective jurisdiction.