PRIVACY POLICY

B2B-Platform.io

1. BASIC PROVISIONS AND SCOPE

1.1. This Privacy Policy (the "Policy") describes how MASSA CONSULTING LIMITED, a company incorporated under the laws of Hong Kong with company registration number 78172075 and registered office at 14/F., China Hong Kong Tower, 8 Hennessy Road, Wanchai, Hong Kong (the "Operator", "we", "us" or "our"), collects, uses, holds, protects and, where permitted, discloses personal data in connection with B2B-Platform.io.

1.2. B2B-Platform.io, available at https://b2b-platform.io (the "Platform"), is a private, closed-access business-to-business software-as-a-service environment for approved legal entities. It facilitates the discovery of prospective commercial counterparties, requests for quotation, business communications and preparation of trade documents, including commercial invoices. The Operator is not a bank, payment institution or payment agent and does not process or settle payments between Participants.

1.3. This Policy covers individuals whose personal data we handle in connection with enquiries, access applications, KYB/AML onboarding, sanctions screening, account administration or Platform operation. Such individuals may include directors, officers, shareholders, ultimate beneficial owners, authorised signatories, representatives, employees, designated payers, commercial contacts and other relevant natural persons connected with an Applicant, Participant or proposed transaction.

1.4. "Applicant", "Participant", "Authorised User", "Account" and "Trade Document" have the meanings used in the Platform Terms of Service (the "Terms"). A Participant is the admitted legal entity; an Authorised User is an individual acting on its behalf. The Terms govern the contractual relationship with the Participant; this Policy concerns personal data of living individuals. The initial submission of an access application does not itself constitute acceptance of the Terms.

1.5. This Policy is prepared primarily under the Personal Data (Privacy) Ordinance (Cap. 486) of Hong Kong (the "PDPO") and its applicable Data Protection Principles. Other laws may apply to particular individuals, activities or locations where legally relevant. References in this Policy to lawful collection, use, disclosure and retention are subject to the laws applicable at the relevant time.

2. DATA USER, PRIVACY CONTACT AND COLLECTION NOTICE

2.1. For the personal data collected and used for our own onboarding, access-control, account-management, security, administration and compliance purposes, MASSA CONSULTING LIMITED acts as the data user within the meaning of the PDPO. A Participant may independently determine the purposes of personal data it submits in connection with its business transactions and is responsible for its own applicable privacy obligations.

2.2. Privacy contact: Privacy Contact, MASSA CONSULTING LIMITED. Registered office: 14/F., China Hong Kong Tower, 8 Hennessy Road, Wanchai, Hong Kong. Website: https://b2b-platform.io.

2.3. Before or at collection, we will take all practicable steps required by the PDPO to inform affected individuals of the purposes of collection, the classes of potential recipients, whether providing the requested information is obligatory or voluntary, the consequences of withholding it and the applicable rights to request access to and correction of their data. This Policy forms part of that information and may be supplemented by notices on application forms, the Website or within the Account.

2.4. Business-identification information and the personal data reasonably requested for mandatory internal KYB/AML onboarding and sanctions screening are required for an Applicant to be considered for admission and for continued access where re-verification is required. Refusal or failure to provide sufficiently complete information may result in an application being declined or deferred, or an Account being restricted, suspended or

terminated. Information requested solely for optional services or communications will be identified as optional where applicable.

2.5. This Policy does not assume that an individual gives unrestricted consent merely by providing information or visiting the Website. Where consent is required by law for a particular use, including use for a new purpose not directly related to the original purpose, we will obtain the appropriate consent or rely on a specific lawful exception.

3. PURPOSES AND PRINCIPLES OF PERSONAL DATA PROCESSING

3.1. We collect and use personal data only for purposes connected with the Platform and reasonably necessary for the relevant function, including: responding to enquiries and access applications; contacting prospective business users; assessing eligibility of legal entities; verifying identity, authority, ownership and control; conducting internal KYB/AML and sanctions screening; managing risk and preventing unlawful or deceptive use; creating and administering Accounts; recording acceptance of the Terms; and maintaining access controls.

3.2. We also use information as necessary to provide private-network features selected by Participants, including displaying appropriately authorised profiles and offers, managing enquiries and requests for quotation, enabling communications, generating and managing Trade Documents, auto-populating commercial invoices with information supplied or confirmed by Participants, maintaining supporting records and offering technical or operational support.

3.3. Further purposes include protecting the Platform, authentication, system administration, troubleshooting, audits, fraud and security incident prevention, responding to complaints, enforcing the Terms, establishing or defending legal rights, internal recordkeeping, meeting applicable legal requirements and responding to competent authorities where disclosure is lawfully required or otherwise permitted.

3.4. Our internal KYB/AML checks and sanctions screening are conducted as conditions of Platform admission and for risk management. They do not make the Operator a regulated bank or payment intermediary, and a designation such as "Verified Platform Participant" does not certify the financial condition, reliability, honesty or performance of an entity or any proposed transaction.

3.5. Personal data will not be used for a new purpose unrelated to the original collection purpose or a directly related purpose without the data subject's prescribed consent, unless an exemption or other lawful basis for that use is available under the PDPO. We do not sell personal data or use KYB records for independent third-party marketing. We do not use personal data for direct marketing without complying with any applicable notification and consent requirements.

3.6. We seek to limit collection and processing to data that are necessary, adequate and not excessive for the stated purposes; take practicable steps to maintain accuracy; and review ongoing necessity in accordance with the PDPO.

4. CATEGORIES AND SOURCES OF PERSONAL DATA

4.1. Identity and contact information may include full legal name, former names where relevant, date and place of birth, citizenship and nationality, identification or passport number, copies of identity or travel documents, portrait photographs appearing in such documents, residential or business address, telephone number, email address, position, role and authorised-signatory details. Additional identity evidence, including photographic or video verification material, will be requested only where reasonably necessary for an identified verification purpose.

4.2. Business ownership and relationship information may include company affiliation, directorships, shareholdings, ultimate beneficial ownership, ownership and control structures, appointment documents, powers

of attorney, business activity, relevant registration and corporate documents, and details of persons authorised to represent an Applicant or Participant.

4.3. Verification and compliance information may include the results of sanctions, politically exposed person, adverse-media and comparable risk screening; relevant public-register checks; information about business activities and geographical exposure; and, where justified by the risk assessment, information or documents concerning the source of funds or source of wealth, beneficial ownership, the purpose of a commercial relationship, or matters relevant to lawful trade and compliance.

4.4. Trade and Platform content may contain the names, business contact details and other personal data of individuals mentioned in requests for quotation, correspondence, commercial documents, delivery details, invoice fields and transaction-related records. A commercial invoice may identify an executing Payer or designated settlement entity and the relevant Beneficiary, including associated contact or bank-account particulars supplied for documentary purposes. The Operator does not take custody of funds or execute any resulting payments.

4.5. Account and technical information may include user identifiers, authentication records, access permissions, login and session history, approximate location derived from network information, IP address, browser and device attributes, timestamps, system logs, security events, communication preferences, service requests and support correspondence. We use appropriate credential-protection measures and do not require Participants to provide their own bank-login credentials or payment-card security codes.

4.6. Website information may include data obtained through necessary session cookies, persistent preferences or analytics tools, as further described in Section 9. We may also hold correspondence and documents voluntarily provided in connection with a privacy request, complaint or enquiry.

4.7. Data may be obtained directly from the individual; from the Applicant or Participant that the individual represents; from authorised staff or representatives; from corporate and beneficial-ownership registers; from lawfully accessible official records, sanctions lists, public sources or professional verification databases; and, where used, from service providers performing checks for the Operator. We do not treat information from public or third-party sources as automatically accurate.

4.8. Participants must ensure that personal data they provide about directors, owners, employees, counterparties or any other individuals have been collected and shared lawfully and that relevant notices, authorisations and consents have been provided or obtained where required. This does not remove the Operator's obligations in respect of the personal data it controls.

5. PERSONAL DATA STORAGE, LOCATION AND RETENTION

5.1. We maintain personal data through centralised records and electronic systems used for account administration, internal verification, document management, security, operational continuity and lawful recordkeeping. Personal data are retained while the relevant business relationship is active and thereafter only for purposes permitted under applicable law.

5.2. Our standard retention period for personal data connected with an admitted Participant and its Account is five (5) years following termination of the relevant business relationship, to the extent necessary for compliance, records, risk management, legitimate claims or other notified and lawful purposes. Information shall be erased, destroyed or irreversibly anonymised earlier when it is no longer necessary for any lawful purpose, subject to applicable record-preservation requirements.

5.3. Where an application is withdrawn, rejected or never results in a business relationship, we retain the application and verification record only for as long as necessary to document the decision, prevent misuse, satisfy relevant lawful requirements or address potential disputes, ordinarily not longer than five (5) years after the final decision unless a longer period is justified under applicable law.

5.4. A longer period may be necessary where information must be preserved under applicable law, a lawful request from an authority, a litigation hold, an active dispute, a security incident or another specific lawful ground. When that reason ends, we reassess whether the data should be retained. Backup copies and archived records will be deleted or de-identified as practicable in accordance with applicable policies and law.

5.5. Information may be stored or processed using infrastructure within or outside Hong Kong, where lawful. This Policy does not specify a fixed server location or provider. In all cases, we will take reasonably practicable steps to protect personal data and to apply appropriate contractual, organisational and technical safeguards, including for any lawful cross-border processing.

6. DISCLOSURE OF PERSONAL DATA AND CROSS-BORDER PROCESSING

6.1. The Platform is a closed network. We do not publish a public list of Participants, expose KYB files or identity documents on unrestricted Website pages, sell or rent personal data, or disclose general network information to unrelated third parties for their independent commercial use.

6.2. Personal data may be accessed by the Operator's authorised directors, employees and representatives only to the extent necessary for their duties. Where technical, security, hosting, support or verification providers are engaged to process data for the Operator, access is limited to necessary operational purposes and is subject to suitable confidentiality, security and other contractual safeguards. Such service providers are not authorised to use the data for unrelated independent marketing.

6.3. Other approved Participants may receive the limited personal data necessary for specific user-directed Platform functions, such as identified business contacts, messages, RFQs or Trade Documents. This does not entitle them to the underlying KYB dossier, copies of private identity documents, the identity of unrelated network members or information about transactions in which they are not involved.

6.4. We may disclose information to courts, regulators, competent public authorities or law-enforcement bodies when required by applicable law, a binding order or an otherwise lawful request, or where disclosure is legitimately necessary to establish, exercise or defend legal rights. We seek to limit such disclosure to information lawfully required and, where legally permissible and practicable, apply appropriate notice and confidentiality safeguards.

6.5. As provided in Section 11.7 of the Terms, following a formal written request from a licensed banking institution, payment service provider or regulatory authority involved in a specific transaction, the Operator may issue an individual Confirmation of Platform Registration & KYB Verification (a "KYB Verification Letter") stating the relevant Payer's internal verification status for that transaction. Any such confirmation is limited to what may lawfully be disclosed, does not involve routine transmission of the complete KYB file or disclosure of the general participant registry, and does not certify or guarantee the Payer or the transaction.

6.6. Except for the limited categories described in this Section and any disclosure otherwise lawfully authorised for a notified purpose, we do not disclose personal data to third parties. No transfer of personal data for an unrelated new purpose will take place without prescribed consent or a lawful exemption where such consent is required by the PDPO.

6.7. If processing, storage or support involves a provider or location outside Hong Kong, we will assess the applicable legal requirements and risks and use appropriate protections intended to preserve privacy and security. Measures may include contractual restrictions on use and onward disclosure, restricted access, information-security controls and procedures for handling personal data requests. Cross-border arrangements remain subject to any restrictions that are legally in force when the transfer occurs.

7. CONFIDENTIALITY, SECURITY AND DATA INTEGRITY

7.1. We take reasonably practicable technical and organisational measures appropriate to the nature of the data and the relevant risks to guard against unauthorised or accidental access, processing, erasure, loss, disclosure or misuse. These may include role-based access restrictions, authentication controls, secure transmission and storage arrangements, system monitoring, personnel confidentiality obligations, incident management and appropriate security arrangements with service providers.

7.2. Identity documents, beneficial-ownership details, compliance screening information and non-public commercial information are treated as restricted information. Access is limited to personnel or properly authorised service providers with a legitimate need to know. Information shared within the private network remains subject to the confidentiality protections and usage restrictions set out in the Terms.

7.3. We take practicable steps to keep personal data accurate and up to date, considering its intended use. Applicants, Participants and relevant individuals should notify us when material identity, authority, ownership or contact information changes. We may request renewed verification before continuing access.

7.4. If we become aware of an actual or suspected data security incident, we will assess and investigate the circumstances, take appropriate containment and remedial measures, preserve relevant evidence where necessary, and make notifications to affected persons or competent authorities where legally required or otherwise appropriate in light of applicable regulatory guidance and risk.

7.5. No Internet-connected system can be guaranteed completely secure. Users must protect their Account credentials and promptly report suspected unauthorised access. Each Participant remains responsible for personal data that it independently downloads, stores or shares outside the Platform.

8. RIGHTS OF INDIVIDUALS AND HANDLING OF REQUESTS

8.1. Subject to the PDPO and its applicable exemptions, an individual has the right to ascertain whether we hold personal data about them and to request access to a copy of those data. An individual may also request correction of inaccurate personal data. We will respond to legally valid data access and correction requests within the applicable statutory period, generally forty (40) calendar days after receipt, or provide a timely explanation where an applicable ground prevents or delays compliance.

8.2. A data access request should be made in writing, using the form prescribed by the Privacy Commissioner for Personal Data where required under the PDPO, and sent to the Privacy Contact at the email address stated in Section 2.2. We may reasonably ask for evidence of identity and, where a request is submitted by another person, proof of authority. We may charge a fee for complying with a data access request only to the extent permitted by law; no fee is charged for a statutory data correction request.

8.3. If an individual believes personal data supplied in response to an access request are inaccurate, they may request correction and provide relevant supporting information. We will make the necessary correction where required by law, provide a copy of corrected data and, where the law requires, take practicable steps concerning previous recipients of inaccurate data.

8.4. An individual may request deletion or restriction of data, withdraw any optional consent previously given, or ask about the purposes, recipients or retention of their personal data. Such requests will be considered under the PDPO and any other applicable law; they do not create an unconditional right to immediate erasure where data remain lawfully necessary for verification, regulatory compliance, security, disputes or recordkeeping.

8.5. If we decline a request, we will explain the applicable reason to the extent permitted by law. Individuals may make a complaint to the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD), concerning personal data practices. Information about the PCPD and available complaint procedures is published at https://www.pcpd.org.hk.

8.6. A Participant that collects or supplies information about its employees, directors, owners or counterparties must give those individuals the relevant notices and assist with lawful requests where appropriate. A privacy request sent to the Operator is distinct from any independent request that an individual may need to make to the Participant.

9. WEBSITE, COOKIES AND RELATED TECHNOLOGIES

9.1. The Website and Account environment may use cookies and similar technologies to operate securely, recognise sessions, remember selected preferences and understand how the services are used. A cookie is a small file or identifier stored by a browser or device. The categories described below are used or may be enabled depending on the Platform's configuration.

9.2. Session cookies support authentication, account session continuity, navigation, basic operations and security. They are ordinarily limited to the current browsing session or a short technical duration. Blocking necessary session cookies may prevent sign-in or other essential features from functioning.

9.3. Persistent cookies may retain language settings, session preferences, user-interface choices or other permitted settings between visits, and may support technical or aggregated usage statistics. Their duration depends on their purpose and configuration, and they expire or are deleted in accordance with the relevant settings.

9.4. Third-party analytics cookies may be used where analytics functionality is enabled, including through tools such as Google Analytics. Such tools may collect information about page visits, navigation and device or browser characteristics. Where applicable, we will identify non-essential cookies and offer a means to accept or reject them in accordance with the legal requirements relevant to the visitor and the technology deployed.

9.5. Users may manage or delete cookies through browser settings and, where provided, Website cookie controls. Disabling optional cookies should not prevent basic service use, although some preferences or convenience functions may be affected. Certain necessary cookies may be required for authentication and security.

9.6. The Website may link to independent third-party sites. Those sites are operated under their own privacy practices, which are not controlled by the Operator. The Platform is intended for professional business use and not for children; we do not knowingly seek personal data from children for Account registration.

10. POLICY CHANGES, GOVERNING LAW AND INTERPRETATION

10.1. We may revise this Policy to reflect changes in the Platform, applicable law, privacy practices, service providers or security requirements. The current version will be made available on the Website and/or within the Account with an identifiable version or update date. Where required by applicable law, material changes will be notified or additional consent obtained before implementing the relevant new use of personal data.

10.2. This Policy is governed by and interpreted in accordance with the applicable laws of the Hong Kong Special Administrative Region, including the PDPO. Mandatory rights and protections under other applicable laws are not excluded to the extent they cannot lawfully be excluded.

10.3. Translations may be made available for convenience. In case of inconsistency between language versions, the English-language version will prevail to the extent permitted by applicable law. This Policy is to be read alongside the Terms and does not create a bank, payment, trustee, escrow or other financial-services relationship between the Operator and any Platform user.