DATA PROCESSING AGREEMENT

This Data Processing Agreement and its attached Annexes ("**DPA**") supplements and forms part of the Kubex Customer Subscription Agreement ("**Agreement**") between you ("**Customer**") and Evenkeel Inc. (d/b/a Kubex) ("**Supplier**") (together, the "**Parties**" and each, a "**Party**"), when the GDPR or other applicable Data Protection Laws applies to Customer's use of the Kubex Subscription services more particularly described in the Agreement (the "**Services**") to process Customer Personal Data.

SECTION 1: INTERPRETATION

1.1 This DPA forms an integral part of the Agreement. The provisions of the Agreement therefore apply to this DPA. All capitalized terms not defined in this DPA will have the meaning set forth in the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Member State**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3 Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

"**Customer Personal Data**" means any Personal Data Processed by Supplier on behalf of Customer pursuant to or in connection with the Agreement;

"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other jurisdiction including, as applicable, Brazil's LGPD, the California Consumer Privacy Act (CCPA), the UK's Data Protection Act 2018 ("UK GDPR") (including the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR including the standard data protection clauses issued by the commissioner under s119A(1) of the UK GDPR as revised from time to time), and the Swiss Federal Act on Data Protection ("Swiss DPA") (including the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner);

"**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The relevant categories of Data Subjects are identified in **Annex 1**, attached hereto.

"**Data Transfer**" means a transfer of Customer Personal Data from Customer to Supplier, or an onward transfer of Customer Personal Data from Supplier to a Sub-Processor, or between two establishments of Supplier, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of this DPA and any other data transfer agreement put in place to address the data transfer restrictions of Data Protection Laws);

"**EEA**" means the European Economic Area;

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR (including the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council (available as of June 2021 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), (the "EU SCCs")); "**GDPR**" means EU General Data Protection Regulation 2016/679;

"**Personal Data**" means any information related to an identified or identifiable Data Subject. The relevant categories of Personal Data that are provided to Supplier by, or on behalf of, Customer are identified in **Annex 1**, attached hereto;

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed; and

"**Sub-Processor**" means any person appointed by or on behalf of Supplier to Process Personal Data on behalf of the Customer in connection with the Agreement.

SECTION 2: PROCESSING OF CUSTOMER PERSONAL DATA

2.1 **Customer's role and obligations**. The Parties agree that Customer is the Data Controller for the Personal Data Processed for the purpose of the provision of the Services under this Agreement.

2.2 **Supplier's role and obligations**. The Parties agree that Supplier shall be considered the Data Processor in the event Supplier collects or otherwise processes Personal Data on behalf of Customer when performing the Services. The Parties agree that:

(i) Supplier shall Process Customer Personal Data on behalf of Customer only as required or as contemplated by the Agreement, or otherwise only upon receiving separate written instructions from Customer;

(ii) Supplier shall notify Customer if, in Supplier's opinion, Customer's instruction for the Processing of Customer Personal Data infringes Data Protection Laws;

(iii) Supplier shall comply with Data Protection Laws and its obligations under this DPA in connection with the Processing of Customer Personal Data; and

(iv) Supplier shall use commercially reasonable efforts to cooperate with and assist Customer in fulfilling Customer's obligations under Data Protection Laws, including to respond to Data Subject requests, Personal Data Breach notifications, requests for audit or investigation or other requests made pursuant to applicable Data Protection Laws.

2.3 A more detailed description of the subject matter and particulars of the Processing of Customer Personal Data, including the duration of Processing, the nature and purpose of Processing, the types of Personal Data to be Processed, and the categories of Data Subjects

the Personal Information to be Processed is about, is contained in Annex A, attached hereto, and in the Agreement.

2.4 If a Data Subject contacts Supplier directly in order to exercise their individual rights such as requesting a copy, correction or deletion of their Personal Data or wanting to restrict or object to the Processing activities, Supplier will promptly direct such Data Subject to Customer. In such cases, Supplier shall provide Customer's basic contact information to the requesting Data Subject, and, to the extent disclosed by Data Subject, Data Subject's basic contact information and a summary of the request to Customer. Customer shall inform Data Subjects that they may exercise their rights solely vis-à-vis Customer. Customer agrees to answer to and comply with any such request of a Data Subject in line with Data Protection Law.

SECTION 3: SUPPLIER PERSONNEL

3.1 Supplier will not disclose Personal Data to any third party, except: (i) as Customer directs; (ii) as stipulated in this DPA and the Agreement; (iii) as required for Processing by Subprocessors in accordance with Section 5 hereof; or (iv) as required under applicable law.

3.2 Supplier shall ensure that any employees or personnel authorized to Process Customer Personal Data, including employees or personnel with access to Customer Data, are committed, under a written agreement, to confidentiality and to only Processing Customer Personal Data as permitted under this DPA and not for any other purposes, except on written instructions from Customer or as required under applicable law.

SECTION 4: SECURITY

4.1 Supplier shall in relation to Customer Personal Data maintain appropriate technical and organizational measures to provide a level of security appropriate to the risk levels associated with Processing, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 Supplier maintains technical and organizational security measures that are consistent with industry accepted best practices, as more particularly described in Annex B, attached hereto. Supplier may adapt such measures from time to time, for example, as a result of the development of regulations, technology and other industry considerations. In any event, Supplier's technical and organizational measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Customer Personal Data to be protected, also taking into account the state of technology and the cost of their implementation.

SECTION 5: SUB-PROCESSING

5.1 Customer acknowledges and expressly agrees that Supplier may transfer Customer Personal Data to third party Sub-Processors for the provision of the Services, provided that:

(i) Supplier has entered into a written agreement with each Sub-Processor containing data protection obligations no less protective than those in this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Sub-Processor;

(ii) any such Sub-Processors will be permitted to access Customer Personal Data only to deliver the services Supplier has retained them to provide, and they are prohibited from using Customer Personal Data for any other purpose;

(iii) where Supplier transfers Customer Personal Data to an international organisation or an entity located outside the EU and/or EEA, UK, or Switzerland, Customer hereby expressly grants Supplier a mandate to enter into a written agreement in the name of and on behalf of Customer in order to ensure an adequate level of protection of Customer Personal Data. Supplier must also enter into any appropriate data protection agreement between Supplier and Sub-Processor, as required by this Section 5.1, to ensure that the receiving entity implements an adequate level of protection to Customer Personal Data; and

(iv) Supplier shall be liable for the acts and omissions of its Sub-Processors to the same extent Supplier would be liable if performing the services of each Sub-Processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.2 Where required by Data Protection Laws, Supplier will make available for Customer a list of Sub-Processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

SECTION 6: PERSONAL DATA BREACH

6.1 Supplier shall notify Customer without undue delay upon Supplier becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection Laws.

6.2 Supplier shall co-operate with Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

6.3 Customer shall notify Supplier without undue delay upon Customer becoming aware of any security issue related to its use of the Services.

6.4 A Party's obligation to report or respond to a Personal Data Breach is not and will not be construed as an acknowledgement by the reporting or responding Party of any fault or liability with respect to the Personal Data Breach.

SECTION 7: DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 Where Customer is obligated by Data Protection Laws to execute a data protection impact assessment ("**DPIA**"), Supplier shall provide reasonable cooperation and assistance to Customer for the execution of the DPIA to allow Customer to comply with its obligations. Supplier shall be entitled to invoice Customer on a time and material basis at the Supplier's then current rates for any time expended for any such assistance.

SECTION 8: DELETION OR RETURN OF CONTROLLER PERSONAL DATA

8.1 **Customer Data**. Promptly following termination of the Agreement, and in any event within 10 business days of the effective date of termination of the Agreement, Supplier shall delete Customer Personal Data on its systems unless otherwise instructed by Customer prior to the effective date of termination, subject to Data Protection Laws. Supplier shall cooperate reasonably and in a timely manner with the efforts by Customer, or party acting on Customer's behalf, to provide for an orderly transition of the applicable Services to Customer or another service provider (the reasonable costs attached to such transition assistance shall be at Customer's expense).

8.2 **Supplier Data**. Notwithstanding anything to the contrary, Supplier may retain or dispose of Supplier records that may contain Customer Personal Data as reasonably required for Supplier's legitimate business purposes or as required by applicable law. This Data Protection Agreement shall continue to apply for the duration of the period during which Supplier retains Customer Personal Data.

SECTION 9: AUDIT RIGHTS

9.1 Subject to this Section 9, Supplier will assist Customer in demonstrating compliance with this DPA by making available upon request of Customer, or of a third party mandated by Customer, information reasonably necessary to demonstrate such compliance. As applicable under Data Protection Laws, Supplier shall immediately inform Customer if, in its opinion, any instructions given pursuant to this Section 9 violate Data Protection Laws.

9.2 Information and audit rights of Customer only arise under Section 9.1 to the extent that the Agreement does not otherwise give Customer information and audit rights meeting the relevant requirements of applicable Data Protection Laws and shall in any event arise in the event of a Personal Data Breach involving Customer Personal Data.

9.3 The Parties agree that Supplier may, except in the event of a Personal Data Breach involving Customer Personal Data, charge Customer at Supplier's then-current reasonable rates for any support provided by Supplier pursuant to this SECTION 9, which charges shall be paid by Customer in accordance with the terms set out in any written invoicing documentation provided by Supplier to Customer in respect of charges under this SECTION 9.

SECTION 10: DATA TRANSFER

10.1 Supplier may not transfer or authorize the transfer of Data to countries outside the EU and/or the EEA, UK and Switzerland without the prior written consent of Customer. If Customer Personal Data is transferred from a country within the EEA, UK, or Switzerland to a country outside the EEA, UK, or Switzerland, the Parties shall ensure Customer Personal Data are adequately protected, pursuant to Section 5.1(iii) of this DPA.

SECTION 11: CUSTOMER RESPONSIBILITIES

11.1 Customer shall comply with applicable Data Protection Laws as well as any other laws applicable to Customer or Customer's industry. If compliance with any such applicable laws requires any actions in connection with data protection on the part of Supplier in addition to the obligations set forth in this DPA, such actions will only be taken upon mutual agreement between the Parties. For the avoidance of doubt, Supplier will use commercially reasonable

efforts to accommodate additional requirements but shall not be obligated to do so. In any event, Customer will provide reasonable advance notice of the required actions, cooperate fully with Supplier in respect thereof and compensate Supplier for any such efforts that require additional services or investment or modifications in the Services.

11.2 Customer represents and warrants that, where it provides any Personal Data to Supplier:

(i) Customer has duly informed the relevant Data Subjects of their rights and obligations, and in particular has informed them of the possibility of Supplier Processing their Personal Data on Customer's behalf and in accordance with its instructions;

(ii) Customer has complied with all applicable Data Protection Laws in the collection and provision to Supplier of such Personal Data and has ensured that Supplier can collect such Personal Data in accordance with Data Protection Laws; and

(iii) the Processing of such Personal Data in accordance with the instructions of Customer is lawful.

11.3 Customer shall take reasonable steps to keep Personal Data up to date to ensure the data are not inaccurate or incomplete with regard to the purposes for which they are collected.

11.4 With regard to components that Customer provides or controls in connection with its use of the Services, Customer shall implement and maintain the required technical and organizational measures for data protection.

SECTION 12: PRIVACY AND DATA PROTECTION REPRESENTATIVE

12.1 The Parties shall appoint an individual responsible for privacy and data protection matters (a "**Privacy Contact Person**"), including, where applicable, a data protection officer.

For Supplier:

Director, IT Security and Compliance privacy@kubex.com

Evenkeel Inc.
200-120 East Beaver Creek Road
Richmond Hill, ON L4B 4V1

12.2 Upon the effective date of the Agreement, Customer shall notify Supplier's Privacy Contact Person identified in this Section 12 of the identify of its Privacy Contact Person and/or data protection officer. In the event Customer does not provide such contact information pursuant to this Section 12, Supplier may use the process for notices set forth in the Agreement

SECTION 13: GENERAL TERMS

13.1 **Confidentiality**. Each Party must keep the information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of

the other Party except to the extent that disclosure is required by law, or the relevant information is already in the public domain.

13.2 **Notices**. All notices and communications given under this Agreement must be in writing and will be sent by email to email address set out in the Agreement or at such other email addresses as notified from time to time by the Parties changing email address. The Parties agree that:

(i) unless legally prohibited from doing so, Supplier shall promptly notify Customer if it or any of its Sub-Processors, with regard to Customer Personal Data: receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing; or intends to disclose Customer Personal Data to any competent public authority outside the scope of the Services of the Agreement. At the request of Customer, Supplier shall provide a copy of the documents delivered to the competent authority to Customer;

(ii) any notification under this DPA, including a Personal Data Breach notification, will be delivered to one or more of Customer's Privacy Contact Persons via email. Upon request of Customer, Supplier shall provide Customer with an overview of the contact information of the registered Customer's Privacy Contact Persons. It is Customer's sole responsibility to timely report any changes in contact information and to ensure Customer's Privacy Contact Persons maintain accurate contact information; and

(iii) if either Party is subject to an inquiry by a data protection authority, regulator or agency, the scope of which includes operations or information within the other Party's control, each Party agrees to provide reasonable cooperation to the other Party.

13.3 **Termination**. This DPA shall terminate at the time the Agreement terminates.

SECTION 14: GOVERNING LAW

14.1 This DPA and any rights and obligations arising out of it shall be interpreted to and governed by the law governing the Agreement.

ANNEX 1
Subject Matter and Particulars of Personal Data Processing

Category of Particular	Explanation of Particular
Subject Matter of Processing	The Processing relates to the provision of the Services as an extension of the Customer's business. Supplier will have access to and process certain information belonging to the Data Subjects that is in the custody of Customer and for which the Customer is the Controller.
Duration of Processing	The processing will continue from the effective date of the Agreement until the date of termination of the Agreement, subject to Customer's data retention requirements.
Nature and Purpose of Processing	The nature of the Processing is login authentication for Customer's users of the Kubex Service and for response to technical support issues. Personal Data will be Processed for the following purposes: • For login authentication purposes to enable Customer employees requiring access to access and use the Kubex Service. • For communication purposes in connection with Customer employees to report technical support issues concerning the Kubex Service.
Categories of Personal Data to be Processed	To be Processed: • Business contact information only of Customer employees that are users of the Kubex service (predominantly only name and email address of the Customer user). Note that no personal information of any of Customer's clients is processed by the service. Special categories to be Processed: • None Accessible to Supplier and potentially Processed: • None
Categories of Data Subjects	Personal Data about the following categories of Data Subjects will be Processed: • Employees of Customer requiring access to the Kubex service.

ANNEX 2
Technical and Organizational Measures

Domain	Practices
Physical Security	Kubex relies on the cloud infrastructure for physical security compliance. The virtual and physical servers are in either AWS, IBM, or Google, which are secure data centers. Annual audits are verified that physical security controls are designed and implemented. Production critical data is never stored on physical media outside of the cloud provider's production environments. Both the data centres and Kubex head office maintain the following controls: Perimeter Security Physical Entry Controls Securing Rooms and Offices Access Card Readers, CCTV Cameras, Security Guard Presence
Data Security	Strict firewall rules control access to the necessary ports for the usage of the service and to ensure limited access to the production environment, to our VPN network, and authorized systems. The corporate network has no additional access to the production environment. Customer data is never stored on employee workstations or removable media. Encryption is enforced on all removable media. Vulnerability Scanning is conducted weekly and patches are applied based on severity Cybersecurity software (3rd party SOC2 Type II) is engaged and agents are installed for threat analytics and file integrity checking Log management and SIEM functions have been implemented with Splunk for monitoring and providing alerts on potential risks to assets Annual risk assessments(internal) are conducted to ensure current controls are in place to protect all assets. External audits (SOC 2 Type II) are also conducted. External penetration tests are conducted annually to address any vulnerabilities, and mitigation plans are put into place to correct any findings All Kubex servers which are part of the production Kubex environment run current, and active anti-virus software with real-time monitoring and are updated at least daily.

Encryption	**Encryption In-Transit** Kubex uses industry standard Transport Layer Security (“TLS”) to create a secure connection using 128-bit Advanced Encryption Standard (“AES”) encryption. This includes all data sent between the web, Kubex Connector, and the Kubex servers. The Kubex Connector is also able to support a variety of customer proxy configurations for sending data to Kubex servers. All customer connections are made securely over HTTPS. **Encryption At-Rest** Kubex prioritizes security and recognizes the critical importance of data encryption to ensure data protection. All provider-managed data is encrypted by default. Additionally, the data drives on database servers that store customer information utilize full-disk encryption with industry-standard AES 256-bit encryption.
Human Resource Security	All employees enter into employment contracts with Kubex that include confidentiality obligations, including for the confidentiality of all Customer data. The employee’s confidentiality obligations survive the termination of their employment with Kubex. All employees must successfully pass, at a minimum, reference checks prior to joining Kubex Any position where employees may come in contact with our customers environment (currently Technical Services, Technical Support, Customer Success Management and Pre-Sales) must, in addition to the regular reference check, also successfully pass a more detailed list of checks (see below). Any staff transferring into one of these positions will need to successfully pass the more detailed checks prior to being transferred. Current employees do have the right to refuse completion of the background checks, which will not affect employment, however, will affect work restrictions and processes. Using a third-party company, Sterling Talent Solutions (formerly Backcheck), Kubex performs the following background checks for these individuals: o Criminal Background Check o Identity Check o Credit Check o Public Safety Verification (Globex sanctions checks) o Employment Verification o Education Verification

Asset Management	Kubex has developed an Asset Handling policy and procedures The following principles are applied and controls vary depending on data classification: • Secure processing • Storage • Transmission • Destruction • Logging The operations team maintains an asset inventory of all assets within the SaaS environment. These tools provide asset information which include location, software, GPO's current versions and owners

Access Control	**Access Overview** All customer data is considered highly sensitive and protected as such. Only authorized, vetted, and trained members of the Kubex operations team have direct access to the systems containing user data. Those who do have direct access to these systems are only permitted to view it them aggregate for operations activities or in detail for troubleshooting purposes. All operations team members undergo background checks outlined in the vetting section of this document and are approved by management. All access is based on least privilege. Application data is only viewed by Kubex Advisors for delivery of the service, and by Operations or other Kubex employees for troubleshooting purposes when consent has expressly been provided. A list is maintained of members of the Kubex team with access to the production environment. Access attestations are reviewed at a minimum every 3 months **Login Security/Password Policy** When customer users log into their Kubex instance using their email address and password, the Kubex service requires a minimum password compliance. • Password minimum length of 16 characters • Containing uppercase and lowercase characters, at least 1 digit and 1 symbol • Cannot use any of the last 16 historical passwords • Passwords expire every 90 days • Automatic account lock-out will occur after 3 failed login attempts Passwords are secured using a one-way hash algorithm. Password complexity, and other settings can be customized by the customer, but only when they increase overall password security. Multi-Factor (2 Factor) authentication and/or integration with an OpenID compatible provider are available. **Administrative Access** Multi-Factor (2 Factor) authentication is required to access the production environment for all operations staff, and where the customer deems it necessary.
Configuration Management	

Privacy Training	Kubex has established a security and privacy awareness policy. Monthly training has been established and modules have been selected to focus on various security risks, like phishing, employee behavior, GDPR and more
Maintenance Policies	Planned Maintenance When planned maintenance on the Kubex service is necessary, the Kubex Operations team will perform the work during a scheduled maintenance window. We will make reasonable efforts to announce at least 5 days prior to the event. Planned Maintenance Windows These windows have been selected with the goal of minimizing service downtime, slowness, or other impact to the people and businesses that rely on the Kubex service. Additionally, due to the nature of the Kubex service's overnight collection and analytics processes, maintenance windows are scheduled between 9 p.m. and midnight local customer time. We do our best to make outages as short as possible. Additionally, our maintenance schedule is evaluated frequently to ensure that we keep user impact as low as possible Emergency Maintenance From time to time, due to unforeseen events, we may have to perform emergency maintenance on Kubex infrastructure or software components. This maintenance might cause some or all the Kubex service to be inaccessible by our users for a period. It is our goal to do this as infrequently as possible. Any emergency maintenance will be announced by email to the identified customer contacts with as much notice as reasonably possible. As with planned maintenance, we do our best to minimize disruption caused by service outages.
Backup and Storage	A backup of the Customer's Kubex's primary database is taken once every 24 hours. All backups are encrypted and stored at offsite locations (backup data centres) to ensure that they are available in the unlikely event that a restore is necessary. All backups are immediately encrypted with 256-bit AES encryption. Encrypted backups can only be decrypted by members of the Kubex operations team who have received training and have been authorized to decrypt the backups. Only authorized members of the Kubex operations team have access to the backup locations, so they can monitor the performance of the backup processes