DATA PROCESSING AGREEMENT

BACKGROUND AND UNDERTAKINGS

A. The Service Provider and the Client have entered into an Agreement under which the Service Provider (herein also referred to as the **"Processor"**) has agreed to provide services to the Client and/or its Affiliates (herein also referred to as the "**Controller"). In rendering such services, the Service Provider may from time to time be provided with, or have access to, information of the Client which may qualify as Personal Data (as defined below).
B. Subject to the terms of this Data Processing Agreement (**DPA**), the Service Provider may process the Client or its end-user's Personal Data as part of the provision of the services under the Agreement.
C. By entering into the Agreement, the Client has accepted and agreed to the terms and conditions of this DPA.

NOW, THEREFORE, and in order to enable the Parties (as defined in the Agreement) to comply with the Applicable Data Protection Legislation, the Parties have entered into this DPA as follows:

1. DEFINITIONS

Terms not otherwise defined in this DPA shall have the meaning as defined in the Agreement. In this DPA the following terms have the following meanings:

"**Applicable Data Protection Legislation**" means all applicable laws and regulations, subject to the processing of Controller Data under this DPA, including without limitation (as applicable), (i) the General Data Protection Regulation (EU) 2016/679 (the "**GDPR"**) (ii) the New Zealand Privacy Act of 2020 (the "**PA**") and (iii) the Australian Privacy Act of 1988 "(**AUS PA'**").

"**Controller Data**" means any Privacy Data processed by Processor on behalf of Controller, pursuant to or in connection with the Agreement.

"**Personal Data"** means any information relating 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, an identification number, location data, an online identifier or as otherwise referred to as "**Personal Information**", "**Personally Identifiable Information**" or similar term defined in the Applicable Data Protection Legislation.

"**Personal Data Breach**" also referred to as "**Privacy Breach**" means an event where personal information is either inappropriately: disclosed, altered, lost, or accessed, whereas **Loss** includes either the destruction of information or the temporary inability to access information as set out in the **Privacy Breach Policy** of the Service Provider.

"**Sub-Processor/s**" means a Processor engaged to carry out Processing in respect of the Controller's data on behalf of the Controller.

The terms recognised by the GDPR, such as "**Controller**", "**Data Subject**", "**Process**", "**Processor**" "**Processing**", "**Supervisory Authority**" shall have the meanings set out therein even if such terms are not capitalised in this DPA.

2. PROCESSING OF CONTROLLER DATA

2.1 Each Party shall comply with the Applicable Data Protection Legislation at all times.
2.2 The Processor shall solely process the Controller's data (as defined in the Agreement) to the extent necessary to provide the service to the Controller.
2.3 The Processor agrees to only process the Controller's data, in accordance with Controller's documented instructions under this DPA, the Agreement and Applicable Data Protection Legislation.
2.4 Notwithstanding the above, the Controller hereby agrees and consents that the Processor may Process the Controller's data for the purpose of the ongoing operation of the service, and the improvement and development, security and controls thereof.
2.5 The Controller warrants and represents that it is, and will, at all relevant times remain duly and effectively authorised to give instructions to the Processor. The Controller shall have sole responsibility for the accuracy, quality and legality of Controller's data and how the Controller acquired Controller data. This DPA, the instructions and the Agreement are the Controller's complete and final instructions to the Processor for the Processing of the Controller's data. Any additional or alternate instructions must be agreed upon separately in writing between authorised representatives of both Parties.
2.6 The Processor shall immediately notify Controller if the Processor cannot fulfil its obligations under this DPA or if the Processor is of the view that instruction regarding the processing of the Controller data given by Controller would be in breach of Applicable Data Protection Legislation, unless if the Processor is prohibited from notifying the Controller under applicable Data Protection Legislation.
2.7 The Processor shall immediately notify the Controller in writing if the Supervisory Authority requests access to the Controller data which the Processor processes on behalf of the Controller.
2.8 The Parties acknowledge and agree that the Processor may qualify as a "Service Provider" as defined in the GDPR. In such a case, the Controller discloses Personal Information to the Processor solely for a valid business purpose and for the Processor to perform the service as set out in the Agreement. The Processor and its affiliates shall not: (i) sell or otherwise transfer the Controller data; or (ii) retain, use, or disclose the Controller Data for a commercial purpose other than providing the service under this DPA, the Agreement and the Processor's Privacy Policies (as referred to below).

3. SECURITY MEASURES

3.1 The Processor shall implement appropriate technical and organisational measures to protect and safeguard the Controller's data that is processed against Privacy Breaches.
3.2 The measures shall at least reach a level of security equivalent to what is prescribed by Applicable Data Protection Legislation, relevant Supervisory Authorities' applicable regulations and guidelines regarding security of the Controller's data and what is otherwise appropriate to the risk of the processing of the Controller's data against Privacy Breaches.

3.3 The Processor will maintain its security controls and audits, pursuant to, amongst others, ISO 27001 and regularly monitors compliance with these safeguards. The Processor will not materially decrease the overall security of the service during the term of the Agreement.

4. PERSONNEL; CONFIDENTIALITY

4.1 The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Processor who may have access to the Controller's data ("**Personnel**"), ensuring in each case that access is strictly limited to Personnel who need to know/access the Controller's data, as strictly necessary for the purposes of the Agreement, and to comply with the Applicable Data Protection Laws in the context of such Personnel's duties to the Processor.

4.2 The Processor will impose appropriate contractual obligations upon its Personnel who processes the Controller's data, including relevant obligations regarding confidentiality, data protection and data security. Personnel engaged are informed of the confidential nature of the Controller's data and have received appropriate training with respect to their responsibilities.

4.3 The Processor has appointed a Data Protection/Privacy Officer who can be reached at privacy@tradewindow.io for all data related queries.

5. SUB-PROCESSORS

5.1 The Controller authorises the Processor to appoint any such Sub-Processors as required in accordance with this clause 5 for the purpose of providing the services under the Agreement.

5.2 The Processor may continue to use those Sub-Processors already engaged by the Processor for the performance of certain Processing activities related to the service.

5.3 The Processor shall give the Controller prior adequate notice of the appointment of any new Sub-Processors, including relevant details of the processing activities to be performed by such Sub-Processors. If within seven (7) days of receipt of such notice, the Controller notifies the Processor in writing of any reasonable objection to the appointment, the Processor shall postpone the appointment until reasonable steps have been taken to address the Controller's objection. Where such steps are not sufficient to relieve the Controller's objection, to the extent that it relates to the services as set out in the Agreement which requires the use of such Sub-Processor, the Controller may, by written notice to the Processor, terminate the applicable Agreement.

5.4 Where a Sub-Processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Sub-Processor's obligations.

5.5 With respect to each Sub-Processor:

(i) the Processor shall before the Sub-Processor first Processes the Controller's Data, carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for the Controller's data required by the Agreement; and

(ii) ensure that the arrangement between the Processor and the Sub-Processor is governed by a written contract that substantially meets the same obligations under this DPA.

6. AFFILIATES

6.1 Some of Processor's obligations may be performed by Processor's Affiliates (as defined in the Agreement) and the Controller acknowledges that the Processor's Affiliates may Process the Controller's data on the Processor's behalf to perform the services under the Agreement.

6.2 The Processor will be liable for the acts and omissions of its Affiliates to the same extent which the Processor would be liable if performing the services under the Agreement.

6.3 The Controller hereby consents to the Processor's use of the Processor's Affiliates in the performance of the services in accordance with the terms of this clause 6 and the Agreement.

7. PERSONAL DATA BREACH

7.1 In the event of a Personal Data Breach, the Processor shall notify the Controller of the Personal Data Breach without undue delay when becoming aware of the breach as set out in the Processor's Privacy Breach Policy.

7.2 The Processor shall promptly after becoming aware of the Personal Data Breach:

(a) commence an investigation into the breach in order to determine the scope, nature and the likely consequences of the Personal Data Breach; and

(b) take appropriate remedial measures in order to mitigate the possible adverse effects of the Personal Data Breach and minimize damage resulting therefrom.

7.3 The Processor shall promptly provide the Controller with such details relating to the Personal Data Breach as the Controller reasonably requires in complying with its obligations under the Applicable Data Protection Legislation and its approved privacy policies.

7.4 The obligations in this Clause 7 shall not apply to incidents that are caused by the Controller or Controller's end-users.

8. RIGHTS OF DATA SUBJECTS

8.1 The Processor shall, to the extent legally permitted, promptly notify the Controller if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, or to object to processing, each a "**Data Subject Request**". The Processor will not respond to any such requests unless authorised to do so by the Controller (unless required to do so under Applicable Data Protection Legislation or under the instructions of a competent authority).

8.2 The Processor shall provide commercially reasonable assistance to the Controller by taking appropriate technical and organisational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subjects' rights as laid down by Applicable Data Protection Legislation. Unless prohibited under the Applicable Data Protection Laws, the Controller will reimburse the Processor with any costs and expenses related to the Processor's provision of such assistance.

9. AUDITS

9.1 The Processor shall make available to the Controller, upon prior written request, all relevant information necessary to reasonably demonstrate compliance with its obligations detailed in this DPA.

9.2 The Processor shall allow for and contribute to audits, including inspections on its premises not more than once in each calendar year (except following a Privacy Data Breach) and during regular business hours. The audit may be conducted by the Controller, or a third-party auditor mandated by Controller, provided that such third-party auditor shall be subject to sufficient confidentiality obligations. The Controller shall give the Processor reasonable notice before exercising its audit rights.

9.3 Each Party shall bear its own costs in relation to such audit. However, where the Controller has mandated a third-party auditor to carry out the audit on its behalf, the Controller shall bear the costs for such a third-party auditor.

10. DATA IMPACT ASSESSMENTS; CONSULTATIONS

The Processor shall, upon the Controller's request, provide the necessary information in order to allow the Controller to fulfil its obligations to, where applicable, carry out data protection impact assessments ("**DPIAs**") and prior consultations with the relevant Supervisory Authority under Applicable Data Protection Legislation in relation to the processing of the Controller's data covered by this DPA.

11. DOCUMENTATION

The Processor shall maintain complete, accurate and up-to-date documentation of its processing activities and measures are taken hereunder, as required under the Applicable Data Protection Legislation, which the Processor shall make available to the Controller upon Controller's written request.

12. TRANSFERS

To provide the services, the Processor and its Sub-Processors may only transfer Controller data concerning residents of the EEA to a Sub-Processor or an Affiliate outside the EEA in accordance with a data transfer mechanism permitted by the Applicable Data Protection Legislation, or as authorised by the Controller in the Agreement.

13. DELETION; RETURN

The Processor shall promptly, and in any event within 30 days of termination of the Agreement or upon the Controller's request, delete or return all copies of the Controller's data, except where such copies are required to be retained in accordance with the Applicable Data Protection Legislation or where such destruction is not possible due to the decentralised blockchain storage system used by the Processor, provided that the processor will ensure the confidentiality of all such Controller data.

14. General Terms

14.1 Any amendments and additions to this DPA shall be in writing and duly signed by the Parties to be valid.

ANNEX 1

DETAILS OF PROCESSING

This Annex 1 includes details of the Processing of the Controller's data as required by Article 28(3) of the GDPR.

.

1. **Subject matter and duration of the Processing of Controller Data**

The subject matter and duration of the Processing of the Controller Data are set out in the Agreement and this Annex.

2. **The nature and purpose of the Processing of Controller Data**

The Processor has developed and owns various software solutions that provide guidance and engagement tools, analytics and automation for web, mobile and desktop applications, simplifying and improving end users' experience, and increasing user engagement (services as further defined in the Agreement). The Controller 's data is collected by the Processor when the Controller or an end user of the Controller uses the service. The Controller's data is processed for the purpose of providing the service, the ongoing operation thereof, and/or for security purposes.

3. **The types of Controller Data to be Processed**

3.1 End-Users' IP addresses, Web Application data (page title, URL) and location information (country and city). If the Controller requests in writing to use special features of the service (such special features include but are not limited to user behaviour tracking and visions and vary depending on the specific feature selected by the Controller) – The Processor may collect and/or process additional Privacy Information as detailed in the Processor's Privacy Policy at . https://tradewindow.io/legals/privacy-policy The Controller may opt-out of the special features, as detailed in the Privacy Policy, by contacting the Processor at privacy@tradewindow.io

3.2 Email addresses and log-in credentials of authorised Controller personnel inherent for the provision of the service, to create outputs and of those end users which contact the Processor in connection with the provision of technical support for the Service.

4. **The categories of Data Subject to whom the Controller Data relates**

Data Subjects are the end-users of the service and authorised Personnel (i.e. Processor's administrators).

5. **The obligations and rights of Controller**

The obligations and rights of the Controller are set out in this DPA, the Agreement and this Annex.

6. **Retention Periods**

The Processor will retain the Controller's data which it processes hereunder only for as long as required to provide the service pursuant to the Agreement. Data retention is managed in line with the Processor's **Information Retention Policy and Information Disposal Schedule,** available at https://www.tradewindow.io/legal.html