LAST UPDATED: MARCH 3, 2025

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this **"Addendum"**) applies to any product, service, or offering where Okoora Trade Flow Ltd. and its Affiliates **("we"** or **"Okoora")** provide the Services to the Customer (**"you"** or **"Customer"**).

This Addendum forms an integral part of the applicable agreement governing Okoora's provision of the Services (the **"Agreement"**). In the event of any conflict or inconsistency between the terms of this Addendum and the Agreement, the terms of this Addendum shall prevail.

Capitalized terms used but not defined herein shall have the meanings assigned to them in the Agreement.

This Addendum is effective as of the later of (i) the effective date specified in the Agreement or (ii) the effective date stated in the notice posted or provided to you in connection with this Addendum. We may amend this Addendum from time to time. The revised version will be effective at the time we post it on our website, unless otherwise noted. If you do not agree with any change to this Addendum, you may discontinue your use of the Services.

1. Definitions

The following terms have the following meanings when used in this Addendum:

"**Controller**" means an entity that determines the purposes and means of the processing of Personal Data, or, if such term (or terms addressing similar data protection and privacy roles) is defined in Applicable Data Protection Law, "Controller" shall have the meaning as defined in the Applicable Data Protection Law including a "Business" as defined in the CCPA.

"**Data Protection Laws**" means any applicable data protection laws, regulations, directives, and regulatory requirements applicable to Okoora's provision of the Services, including any amendments thereto and any associated regulations or instruments (e.g., the California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100 et seq ("CCPA"), the General Data Protection Regulation (EU) 2016/679 (GDPR), the Australian Privacy Act 1988 (Cth) the Personal Information Protection and Electronic Documents Act (Canada), the Personal Data (Privacy) Ordinance (Cap.486) (HongKong), the Brazilian General Data Protection Law, Federal Law no. 13,709/2018 and the PersonalData Protection Act 2012 (Singapore)).

"**End-user(s)**" means your clients who use the Services and are data subjects for the purposes of this Addendum.

"**End-user Data**" means the Personal Data that (i) the End-user provides to you and you pass on to Okoora through the use by you of the Services and (ii) Okoora may collect from the End-user's device and browser through use by you of the Services.

"**Personal Data**" means any information relating to an identified or identifiable natural person (a "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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Process**" or "**Processed**" or "**Processing**" means any operation or set of operations performed upon Personal Data, including collection, recording, retention, sharing, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction.

2. Okoora As a Controller

Okoora shall comply with the requirements of the Data Protection Laws applicable to Controllers with respect to the Processing of End-user Data under this Addendum (including, without limitation, by implementing and maintaining at all times all appropriate security measures in relation to the processing of End-user Data) and shall not knowingly do anything or permit anything to be done with respect to the End-user Data that likely would lead to a breach by Customer of the Data Protection Laws. Okoora shall only transfer End-user Data to third parties, sub-processors, or members of the Okoora Group, who shall sign written agreements which contain terms for the protection of End-user data, which are no less protective than the terms set out in this Addendum.

3. Processing of End-user Data in Connection with the Services

The parties acknowledge and agree that Customer and Okoora are each independent Controllers in respect of all End-user Data Processed in connection with the Services. As such, Okoora independently determines the purpose and the means of the Processing of such End-user Data and is not a joint Controller with the Customer with respect to such End-user Data.

The parties acknowledge and agree that Okoora is permitted to use, reproduce and Process End-user Data and payment transaction data for the following limited purposes:

- as reasonably necessary to provide and improve the Services to Customer and its End-users, including in connection with its fraud protection tools;
- to monitor, prevent and detect fraudulent payment transactions and to prevent harm to Customer, Okoora and to third parties,
- to comply with legal or regulatory obligations applicable to the Processing and retention of payment data to which Okoora is subject, including applicable anti-money laundering and identity verification obligations;
- to analyze, develop and improve Okoora's products and services;
- internal usage, including but not limited to, data analytics and metrics;
- to compile and disclose End-user Data and payment transaction data in the aggregate where your individual or user End-user Data is not identifiable, including calculating your averages by region or industry;

- complying with applicable legal requirements and assisting law enforcement agencies by responding to requests for the disclosure of information in accordance with laws; and
- any other purpose that it notifies Customer so long as such purpose is in accordance with Data Protection Laws.

4. Customer Representations and Warranties

Throughout the duration of the DPA, Customer represents and warrants that :

1. Personal Data has been and will continue to be collected, processed and transferred by Customer to Okoora in accordance with the relevant provisions of Data Protection Laws ;
2. Customer is solely responsible for determining the lawfulness of the data processing; and that
3. The Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained any relevant consents or established other lawful grounds thereto
4. The Customer shall (i) notify End-users in their privacy policy that Okoora is an independent Controller for the purpose of Processing End-user Data as described in this Addendum and (ii) include a link to the Okoora Privacy Policy.

5. Mutual Assistance

The parties agree to co-operate with each other to the extent reasonably necessary to enable the other party to adequately discharge their responsibility as an independent Controller under Data Protection Laws. The parties agree that to the extent Customer receives a subject access request or any exercise by an End-user of its rights under Data Protection Laws, Customer shall respond to such End-user's access request directly. Customers also shall inform the End-user that they may exercise their data subject rights in connection with the Services with Okoora according to the instructions described in Okoora Privacy Policy. In addition, if in connection with any security incident, Okoora determines in its sole decision that it must notify affected End-users and Okoora does not have the necessary contact information about an affected End-user to make such communication, then Customer shall use commercially reasonable efforts to provide Okoora with information about End-user that Customer may possess for the limited purpose of Okoora's compliance with applicable notification obligations regarding affected End-users under Data Protection Laws.

6. Cross Border Data Transfers

The parties agree that Okoora may transfer End-user Data Processed under this Addendum outside the country where it was collected as necessary to provide the Payment Services. If Okoora transfers End-user Data protected under this Addendum to a jurisdiction for which the applicable regulatory authority for the country in which the data was collected has not issued an adequacy decision, Okoora will ensure that appropriate safeguards have been implemented for the transfer of End-user Data in accordance with applicable Data Protection Laws.

With respect to your data transfers to Okoora of your End-users located in the European Union, Switzerland, the Europeans Economic Area, and/or their member states or the United Kingdom, we agree that (i) to the extent applicable, your signing of the Agreement will be deemed to be signature and acceptance of the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the GDPR ("EU Transfer Clauses") by Customer, as the data exporter and in the role of controller, and will be deemed to be signature and acceptance of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (the "UK Transfer Clauses" or "UK Addendum"), as the data exporter (ii) to the extent applicable, Okoora's signature of the Agreement will be deemed to be signature and acceptance of the EU Transfer Clauses by Okoora, as the data importer and in the role of controller, and will be deemed to be signature and acceptance of the UK Transfer Clauses, as the data importer; and (iii) the parties shall be subject to the Module 1 provisions of the EU Transfer Clauses. In the event the European Commission or the UK Secretary of State (or other applicable UK authorized body) revises and thereafter publishes new EU Transfer Clauses or UK Transfer Clauses, respectively (or as otherwise required or implemented by the European Commission or the UK Secretary of State (or other applicable UK authorized body)), the Parties agree that such new EU Transfer Clauses or UK Transfer Clauses, as applicable, will supersede the present EU Transfer Clauses or UK Transfer Clauses, as applicable, and that the parties agree to take all such actions required to effect the execution of the new EU Transfer Clauses or UK Transfer Clauses, as applicable. The EU Transfer Clauses (Module 1) and the UK Transfer Clauses will be incorporated into the Agreement by reference and will be considered duly executed between the parties upon entering into force of this agreement. subject to the following details:

A) EU Transfer Clauses

The parties agree that the details required under the EU Transfer Clauses Appendix are as set forth in Attachment 1.

B) UK Transfer Clauses

The parties agree that the details required under Annex B of the UK Transfer Clauses are as set forth in Attachment 1 (to the extent applicable).

To the extent the UK Transfer Clauses applies, the following shall apply :

- All the information provided under the Standard Contractual Clauses shall apply to the UK Transfer Clauses with the necessary changes per the requirement of the UK Addendum.
- In Table 4 of the UK Addendum, either party may terminate the UK Addendum in accordance with section 19 of the UK Addendum .
- By entering into this DPA, the Parties hereby agree to the format changes made to the UK Addendum.

<u>Governing Provisions for Standard Contractual Clauses (SCCs)</u>

The parties agree that for the purpose of transfer of Personal Data between the Okoora and the Customer, the following shall apply:

- Clause 7 of the Standard Contractual Clauses shall not be applicable.
- In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
- In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Ireland (or any other European jurisdiction)
- In Clause 18(b) the Parties choose the courts of Dublin as their choice of forum and jurisdiction (or at any other European jurisdiction).

Attachment 1

Appendix to the EU Transfer Clauses and Annex B of the UK Transfer Clauses

A. The following is applicable, to the extent required, under the EU Transfer Clauses and the UK Transfer Clauses

Annex 1.A. List of Parties

Data Exporter

Name and Address: The data exporter is the Customer and the address is as provided in the Agreement

Contact person's name, position and contact details: as provided in the Agreement

Activities relevant to the data transferred under the Standard Contractual Clause: as provided in the Agreement

Signature and date: please see the "Cross Border Transfers" section of this Addendum

Role (controller/processor): controller

Data Importer

Name and Address: The data importer is Okoora and the address is as provided in the Agreement

Contact person's name, position and contact details: as provided in the Agreement

Activities relevant to the data transferred under the Standard Contractual Clause: as provided in the Agreement Signature and date: please see the "Cross Border Transfers" section of this addendum

Role (controller/processor): controller

Annex 1.B. Description of Transfer

Data subjects Whose Personal Data is Transferred

The Personal Data transferred concern the following categories of data subjects:

- The data exporter's End-users, employees and other business contacts.

Categories of Personal Data Transferred

The personal data transferred may include the following categories of data:

- Name, amount to be charged, date/time, bank account details, payment card details, CVC code, post code, country code, address, email address, fax, phone, website, expiry data, shipping details, tax status, unique End-user identifier, IP Address, location, and any other data received by Okoora under the Agreement.

Nature of the Processing

As set forth in the Agreement.

Purpose(s) of the Transfer(s)

The transfer is made for the following purposes:

- Performance of the services provided by data importer to data exporter in accordance with the agreement.
- To identify fraudulent activity and risk that is, or may, affect the data importer, the data exporter, or other End-users of the data importer.
- To comply with laws applicable to the data importer.
- As set forth in the Data Processing Addendum.

The Period for which the Personal Data will be Retained, or, if that is not Possible, the Criteria Used to Determine that Period

The data importer only retains personal data for as long as necessary to fulfill the relevant purpose(s) for which it was collected (please see the purposes above) and in compliance with its obligations under Applicable Law. To determine the appropriate retention period for personal data, the data importer considers the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of the personal data,the purposes for which the personal data is processed and whether such purposes can be achieved through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

For transfers to (Sub-) Processors, also Specify Subject Matter, Nature and Duration of the Processing

The data importer may share personal data with its Network Partners and any other Third-Party Service Providers that perform services and functions at the data importer's direction and on its behalf. These Third-Party Service Providers may, for example, provide an element of the services provided under the Agreement, such as End-user verification, transaction processing, or End-user support, or provide a service to the data importer that supports the services

provided under the agreement, such as storage. When determining the duration of the processing undertaken by the third-party service providers, the data importer applies the criteria provided above in this Annex1.B.

Annex 1.C. Supervisory Authority

In accordance with Clause 13(a) of the EU Transfer Clauses, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated, shall act as a competent supervisory authority.

B. The following applies to UK Transfer Clauses only

Recipients

The personal data transferred may be disclosed only to the following recipients:

- The data importer's service providers (as further detailed above), affiliates, and personnel performing services in accordance with the Agreement.

Annex A

Technical and Organizational Measures to Ensure the Security of the Data

This Annex forms part of the DPA and describes the technical and organizational security measures implemented by the data importer.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.