DATA PROCESSING AGREEMENT

[CUSTOMER] ("**Customer**"), has contracted with [Vendor Inc.] ("**Vendor**"), to perform certain data processing functions on behalf of the Customer pursuant to a [services agreement] entered into between them dated [insert date] ("**Services Agreement**"), including the processing of Personal Data (as defined in the Definitions section below).

1. Introduction

This agreement is made in light of the requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**GDPR**") and applicable Data Protection Legislation (as that term is defined below). Definitions used in this agreement shall have the same meaning as set out in the GDPR. This Data Processing Agreement (this "**Agreement**") is based on the requirements set out in article 28 of the GDPR.

The purpose of this Agreement is to ensure that Vendor provides the services under the Services Agreement ("**Services**") to Customer in a manner that complies with the Data Protection Legislation.

2. General

In respect of the parties' rights and obligations under this Agreement regarding the Personal Data, the parties hereby acknowledge and agree that Customer is the "**Data Controller**" and Vendor is the "**Data Processor**" and accordingly Vendor agrees that it shall process all Personal Data in accordance with its obligations pursuant to this Agreement and otherwise in accordance with the Data Controller's written instructions.

3. Engagement of Sub-Processors

Where the Data Processor engages another processor (sub-processor) for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out this processor agreement or other legal act between the Data Controller and the processor as referred to in article 28, paragraph 3, of the GDPR, shall be imposed on that other processor (sub-processor) by way of contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor (sub-processor) fails to fulfil its data protection obligations, the initial Data Processor shall remain fully liable to the Data Controller for the performance of that other processor's (sub-processor's) obligations.

The Data Processor shall not engage another processor without prior specific or general written authorization of the Data Controller.

The Data Processor uses the sub-processors listed at https://static.wixstatic.com/ugd/7bc1e9_77400286ac1a4421a94e5d2a3ef17414.pdf, which list may be updated from time to time with notice by the Data Processor to the Data Controller. Data Controller hereby provides general authorization for Data Processor to engage sub-processors.

4. Subject-Matter and Duration of the Processing

The type of Personal Data processed pursuant to this Agreement, including the subject matter, duration, nature and purpose of the processing, and the categories of Data Subjects, is as described in Annex 1.

5. Compliance with Controller's Instructions

The Data Processor shall process the Personal Data only on documented instructions from the Data Controller, including any transfer of data to a third countries or international organizations.

If, in the performance of this Agreement, Data Processor transfers any Personal Data received from or on behalf of Data Controller to any third party (which shall include without limitation any affiliates of Data Processor) where such third party is located outside the European Economic Area, Data Processor shall in ensure that such transfer is in accordance with the GDPR, which may include:

(a) the requirement for Data Processor to execute or procure that the third party execute Standard Contractual Clauses for transfers from Data Controllers to Data Processors approved by the Commission pursuant to Decision 2010/87/EU, as amended by Commission Implementing Decision (EU) 2016/2297;
(b) the requirement for the third party to be certified under the Privacy Shield framework; or
(c) the existence of any other specifically approved safeguard for data transfers (as recognized under the GDPR) and/or a European Commission finding of adequacy.

[NOTE - IF PERSONAL DATA IS BEING EXPORTED OUTSIDE THE EU/ EEA, THEN THE PARTIES MUST ALSO EXECUTE A DATA TRANSFER AGREEMENT (STANDARD CONTRACTUAL CLAUSES) AS ISSUED BY THE EU COMMISSION OR OTHERWISE MEET ONE OF THE REQUIREMENTS SET OUT IN (a) to (c). CANADA CURRENTLY HAS AN ADEQUACY FINDING.]

6. Customer's Obligations.

Data Processor shall, where applicable in respect of any Personal Data processed pursuant to this Agreement, provide full cooperation and assistance to Customer to allow Customer to comply with Customer's obligations set out under Articles 32 – 36 of the GDPR to:

(a) ensure the security of the processing;
(b) notify the relevant supervisory authority, and any data subject(s), where relevant, of any breaches relating to Personal Data;
(c) carry out any data protection impact assessments ("**DPIA**") of the impact of the processing on the protection of Personal Data; and
(d) consult the relevant supervisory authority prior to any processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk.

7. Confidentiality

The Data Processor shall take reasonable steps to ensure that only authorized personnel have access to Personal Data and that any persons whom it authorizes to have access to the Personal Data will respect and maintain all due confidentiality.

8. Security of Processing

The Data Processor shall implement appropriate technical and organizational measures in accordance with article 32 of the GDPR to ensure a level of security appropriate to the risk, including as appropriate:

(a) the pseudonymization and encryption of data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
(d) a process for regularly testing, accessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

9. Requests by Data Subjects

As further set out in Chapter III of the GDPR, Data Subject has certain rights (e.g. information and access to Personal Data, rectification and erasure, restriction of processing, data portability, right to object and automated individual decision-making). The Data Controller is obliged to facilitate the exercise of these Data Subject rights under Articles 15 to 22 of the GDPR. The Data Processor shall assist the Data Controller by appropriate technical and organizational measures for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR.

10. Personal Data Breach,

As further set out in Articles 32 to 36 of the GDPR, Data Controller has certain obligations (e.g. notification of data breach to the supervisory authority, and communication of data breach to the Data Subject).

The Data Processor shall notify the Data Controller of any actual or suspected data breaches involving Data Controller's Personal Data and in all other aspects assist the Data Controller in ensuring compliance with Articles 32 to 36 of the GDPR. In particular, the Data Processor shall promptly provide the Data Controller with cooperation and assistance in respect of the data breach and all information in Data Processor's possession concerning the data breach, including the following:

(a) the probable cause and consequences of the breach;
(b) the categories of Personal Data involved;
(c) a summary of the probable consequences for the relevant Data Subjects;
(d) a summary of the unauthorized recipients of the Personal Data; and
(e) the measures taken by Data Processor to mitigate any damage.

11. Return and Deletion of Personal Data

The Data Processor shall, at the choice of Data Controller, delete or return all the Personal Data to the Data Controller at the end of the provision of Services relating to processing, and delete any existing copies unless Union or Member State law requires storage of the Personal Data.

12. Audit, Compliance and Duty to Inform

The Data Processor shall maintain written records of all categories of processing activities carried out on behalf of the Data Controller.

The Data Processor shall make available to the Data Controller all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

If Data Controller believes that an on-site audit is necessary, upon reasonable notice of Data Controller, Data Processor agrees to give Data Controller access to Data Processor's premises, (subject to any reasonable confidentiality and security measures at a mutually acceptable time), and to any stored Personal Data and data processing programs it has on-site. Data Controller is entitled to have the audit carried out by a third party.

13. No additional compensation

The Data Processor's compensation is being included in the Services charges set out in the Services Agreement referred above, and the Data Processor shall thus not be entitled to any additional compensation for carrying out its obligations under this Addendum.

14. Governing law and dispute resolution

The governing law and dispute resolution clause set out in the Services Agreement referred to above shall also be applicable to this Data Processing Agreement, provided that to the extent required by Applicable Law, this Addendum shall be governed by the laws of Ireland.

15. Definitions

"**Data Controller**" has the meaning set out in the Data Protection Legislation;

"**Data Processor**" has the meaning set out in the Data Protection Legislation;

"**Data Protection Legislation**" means all privacy laws applicable to any Personal Data processed under or in connection with this Agreement, including, without limitation, the Data Protection Directive 95/46/EC (as the same may be superseded by the General Data Protection Regulation 2016/679 (the "**GDPR**")), the Privacy and Electronic Communications Directive 2002/58/EC and all national legislation implementing or supplementing the foregoing and all associated codes of practice and other guidance issued by any applicable data protection authority, all as amended, re-enacted and/or replaced and in force from time to time;

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**Personal Data**" has the meaning set out in the Data Protection Legislation and relates only to personal data of which Customer is the Data Controller and in relation to which the Vendor is providing the Services under the Services Agreement;

"**process**" and other derivations such as "processed" and "processing" means any use of or processing applied to any Personal Data and includes "processing" as defined in the Data Protection Legislation;

***

Acknowledged by:

_____	_____
[Insert Customer name]	**NOIBU TECHNOLOGIES INC.**
[Name]	**[Name]**
[Title]	**[Title]**
[Date]	**[Date]**

ANNEX 1

For the purposes of the Agreement, the parties set out below a description of the Personal Data being processed under the terms of the Agreement and further details required pursuant to the GDPR.

1. **TYPES OF PERSONAL DATA:**

- Customer Account Information: business contact information, including the company name and address. Noibu may also collect credit card billing information in order to process payments for the Noibu Service and Professional Services.
- End Users: name, address, email, username, and details related to the purchase transaction, as well as browser type, device type, and IP address.

2. **DURATION OF PROCESSING**:

- The duration of the processing shall be the term of the Services agreement.

3. **NATURE OF PROCESSING**:

- Capturing a video recording of check-out process during e-commerce transaction.
- Identifying and resolving transaction errors.

4. **PURPOSE OF PROCESSING**:

- Administering customer accounts, including providing the Services.
- Allow Customer to identify and resolve potential errors on their e-commerce website and check-out process.

5. **CATEGORIES OF DATA SUBJECT**:

- Customer and end users of customers (e.g. shoppers).