DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the Business Services Agreement or similar agreement (the "**Agreement"**) between Marketplacer ("**Marketplacer**") and Sample Customer ("**Operator**" (collectively the "**Parties**")).

1. Subject Matter and Duration.

a) Subject Matter. This Addendum reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Operator Personal Data in connection with Marketplacer's execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

b) Duration and Survival. This Addendum will become legally binding upon the Start Date of the Agreement (as defined therein) or upon the date upon which both Parties have signed this Addendum, if it is completed after the Effective Date of the Agreement. Marketplacer will Process Operator Personal Data until the relationship terminates as specified in the Agreement. Marketplacer's obligations and Operator's rights under this Addendum will continue in effect so long as Marketplacer Processes Operator Personal Data.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "Applicable Data Protection Law(s)" means the relevant data protection and data privacy laws, rules and regulations to which the Operator Personal Data are subject. "Applicable Data Protection Law(s)" shall include, but not be limited to, EU General Data Protection Regulation 2016/679 ("GDPR") principles and requirements, the United Kingdom Data Protection Act 2018, and the California Consumer Privacy Act of 2018 ("CCPA"), and its implementing regulations. For the avoidance of doubt, if Marketplacer's processing activities involving Operator Personal Data are not within the scope of an Applicable Data Protection Law, such law is not applicable for purposes of this Addendum.

b) "Operator Personal Data" means Personal Data Processed by Marketplacer to provide the Services. The Operator Personal Data and the specific uses of the Operator Personal Data are detailed in **Exhibit 1** attached hereto, as required by the GDPR.

c) "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

d) "Personal Data" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

e) "Process," "Processes," "Processing," "Processed" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

f) "Processor" means a natural or legal person, public authority, agency or other body which Processes Operator Personal Data on behalf of Operator subject to this Addendum.

g) "Security Incident(s)" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Operator Personal Data Processed by Marketplacer.

h) "Services" means any and all services that Marketplacer performs under the Agreement.

i) "Standard Contractual Clauses" means the UK Standard Contractual Clauses, and/or the 2021 Standard Contractual Clauses.

j) "Third Party(ies)" means Marketplacer's authorized contractors, agents, vendors and third party service providers that Process Operator Personal Data on behalf of Marketplacer or Third Parties as

applicable (including the Marketplacer subprocessors listed on its website available at: https://marketplacer.com/legal/global-subprocessor-list/).

k) "**UK Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ and completed as described below.

l) "**2021 Standard Contractual Clauses**" means the Standard Contractual Clauses issued pursuant to the EU 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 Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described below.

3. Data Use and Processing.

a) Compliance with Laws. Operator Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

b) Purpose Limitation. Marketplacer will not Process Operator Personal Data for any purpose other than for the specific purposes set forth in the Agreement, unless obligated to do otherwise by applicable law. In such case, Marketplacer will inform Operator of that legal requirement before the Processing unless legally prohibited from doing so.

c) Documented Instructions. Marketplacer and its Third Parties shall Process Operator Personal Data only in accordance with the documented instructions of the Operator. The Agreement, including this Addendum, along with any applicable statement of work, constitute Operator's complete and final instructions to Marketplacer regarding the Processing of Operator Personal Data, including for purposes of the Standard Contractual Clauses. Marketplacer will, unless legally prohibited from doing so, inform Operator in writing if it reasonably believes that there is a conflict between Operator's instructions and applicable law or otherwise seeks to Process Operator Personal Data in a manner that is inconsistent with Operator's instructions.

d) Authorization to Use Third Parties. To the extent necessary to fulfill Marketplacer's contractual obligations under the Agreement or any statement of work, Operator hereby authorizes (i) Marketplacer to engage Third Parties and (ii) Third Parties to engage subprocessors.

e) Marketplacer and Third Party Compliance. Marketplacer agrees to: (i) enter into a written agreement with Third Parties regarding such Third Parties' Processing of Operator Personal Data that imposes on such Third Parties (and their subprocessors) data protection and security requirements for Operator Personal Data that are at least as restrictive as the obligations in this Addendum and, where the Standard Contractual Clauses are applicable and where the subprocessor is located in a third country which does not provide adequate protection for Personal Data, enter into Standard Contractual Clauses with the subprocessor; and (ii) remain responsible to Operator for Marketplacer's Third Parties' (and their subprocessors if applicable) failure to perform their obligations with respect to the Processing of Operator Personal Data.

f) Right to Object to Third Parties. Operator agrees that Marketplacer shall be entitled to use the subprocessors listed on the legal hub on Marketplacer's website at https://marketplacer.com/legal/global-subprocessor-list/. Prior to engaging any new Third Parties that Process Operator Personal Data, Marketplacer will (i) update the list of subprocessors on its website or (ii) notify Operator by email if it adds any new subprocessors if Operator has requested in writing to privacy@marketplacer.com to be notified by email, at least fourteen (14) days' prior to allowing such subprocessor to process Operator Personal Data. Operator may object in writing to Marketplacer's appointment of a new subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Operator, as its sole and exclusive remedy, may terminate the Agreement (including this DPA) for convenience. If Operator does not reply to Marketplacer's request for subprocessor approval within the requisite period, Marketplacer shall be entitled to deem such non-reply as approval of the relevant subprocessor(s).

g) Confidentiality. Any person or Third Party authorized to Process Operator Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

h) Personal Data Inquiries and Requests. Upon written request from Operator, Marketplacer agrees to provide reasonable assistance and comply with all reasonable instructions from Operator related to any requests from individuals exercising their rights in Operator Personal Data granted to them under Applicable Data Protection Laws (e.g., access, rectification, erasure, data portability, etc.). Operator is responsible for ensuring such requests are handled in accordance with Applicable Data Protection Laws. If a request is sent directly to Marketplacer, Marketplacer shall promptly notify Operator and shall not respond to the request unless Operator has authorized Marketplacer to do so.

i) Government Access Requests. Unless prohibited by applicable law or a legally-binding request of law enforcement, Marketplacer shall promptly notify Operator of any request by government agency or law enforcement authority for access to or seizure of Operator Personal Data, and shall render reasonable assistance to Operator, if Operator wishes to contest the access or seizure.

j) Data Protection Impact Assessment and Prior Consultation. Upon written request from Operator, Marketplacer agrees to provide reasonable assistance at Operator's expense to Operator where, in Operator's judgment, the type of Processing performed by Marketplacer is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

k) Sale of Operator Personal Data Prohibited. Marketplacer shall not sell Operator Personal Data as the term "sell" is defined by the CCPA.

l) CCPA Certification. Marketplacer hereby certifies that it understands its restrictions and obligations set forth in this Addendum and will comply with them.

4. Cross-Border Transfers of Personal Data.

a) Cross-Border Transfers of Personal Data. Operator authorizes Marketplacer and its Third Parties to transfer Operator Personal Data across international borders, including from the European Economic Area (the "**EEA**"), the United Kingdom, and Switzerland to countries including Australia, New Zealand, the United States and others. Marketplacer and Operator agree to use the Standard Contractual Clauses as the adequacy mechanism supporting the transfer and Processing of Operator Personal Data, as further detailed below.

b) 2021 Standard Contractual Clauses. For transfers of Operator Personal Data out of the EEA that are subject to Section 4(a) of this DPA, the 2021 Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the 2021 Standard Contractual Clauses will apply as set forth in this Section 4(b). "Module Two: Transfer controller to processor" will apply and all other module options will not apply. Under Annex 1 of the 2021 Standard Contractual Clauses, the "data exporter" is Operator and the "data importer" is Marketplacer and the information required by Annex 1 can be found in **Exhibit 1**. For the purposes of Annex 2 of the Standard Contractual Clauses, the technical and organizational security measures implemented by the data importer are those listed in clause 5 of this Addendum ("**Information Security Program**"). Clause 7 ("Docking clause") will not apply. For clause 9 (Use of sub-processors), the Parties choose Option 2 (General Written Authorization) and the Parties agree that the time period for prior notice of Third Party changes will be as set forth in Section 3(f) of this Addendum. For clause 11 ("Redress"), the optional language will not apply. For clause 17 ("Governing law"), the Parties choose Option 1 and the Parties agree that the governing law will be England & Wales. For clause 18 ("Choice of forum and jurisdiction"), the Parties agree that the courts of England & Wales will apply for subsection (b).

c) UK Standard Contractual Clauses. For transfers of Operator Personal Data out of the United Kingdom that are subject to Section 4(a) of this Addendum, the UK Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the UK Standard Contractual Clauses will apply as set forth in this Section 4(c). For Table 1 of the UK Standard Contractual Clauses, (i) the Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Annex 1 of the 2021 Standard Contractual Clauses and (ii) the Key Contacts shall be the contacts set forth in Annex 1 of the 2021 Standard Contractual Clauses. The

Approved EU SCCs referenced in Table 2 shall be the 2021 Standard Contractual Clauses as executed by the Parties pursuant to this Addendum. For Table 3, Annex 1A, 1B, and II shall be set forth in Annex 1 of the 2021 Standard Contractual Clauses. For Table 4, either party may end the UK Standard Contractual Clauses as set out in Section 19 of the UK Standard Contractual Clauses.

d) Switzerland Transfers. For transfers of Operator Personal Data out of Switzerland that are subject to Section 4(a) of this DPA, the 2021 Standard Contractual Clauses will apply and will be deemed to have the differences set forth in this Section 4(d), to the extent required by the Swiss Federal Act on Data Protection ("FADP"). References to the GDPR in the 2021 Standard Contractual Clauses are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR. The term "member state" in the 2021 Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the 2021 Standard Contractual Clauses. References to personal data in the 2021 Standard Contractual Clauses also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope. Under Annex I(C) of the 2021 Standard Contractual Clauses (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the 2021 Standard Contractual Clauses insofar as the transfer is governed by the GDPR.

e) Each party's signature to this Addendum shall be considered a signature to the Standard Contractual Clauses. If required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the Standard Contractual Clauses as separate documents. In case of conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses will prevail.

5. Information Security Program.

a) 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 to the rights and freedoms of natural persons, Marketplacer agrees to implement appropriate technical and organizational security measures designed to protect Operator Personal Data as required by Applicable Data Protection Law(s) (the "I**nformation Security Program**") as set out in **Annex 1** Technical and Organizational Security Measures.

b) Marketplacer's Technical and Organizational Measures are subject to technical progress and further development. Accordingly, Marketplacer reserves the right to modify the Technical & Organizational Measures provided that the functionality and security of the Services are not degraded.

6. Security Incidents.

a) Security Incident Procedure. Marketplacer will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Operator Personal Data in a timely manner.

b) Notice. Marketplacer agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) (but in no event longer than seventy-two (72) hours) to Operator's Designated POC upon becoming aware that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Operator to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

7. Audits.

a) Right to Audit; Permitted Audits. On written request, Marketplacer shall make available to the Operator and its regulators all information reasonably necessary to demonstrate compliance with Applicable Data Protection Laws and this Addendum. On written request, the Operator and its regulators shall have the right to inspect Marketplacer's architecture, systems, and documentation which are relevant to the security and integrity of Operator Personal Data, or as otherwise required by a governmental regulator:

i) Following any notice from Marketplacer to Operator of an actual or reasonably suspected Security Incident involving Operator Personal Data;

ii) Upon Operator's reasonable belief that Marketplacer is not in compliance with Applicable Data Protection Laws, this Addendum or its security policies and procedures under the Agreement; or

iii) As required by governmental regulators, but only to the extent that the Operator's own records are not sufficient,

subject to the requirements of subclause (b).

b) Audit Terms. Any audits described in this Section shall be subject to the following:

i) Conducted by Operator or its regulator, or through a third party independent contractor or auditor selected by one of these parties, at the Operator's sole cost and responsibility and to whom Marketplacer does not reasonably object.

ii) Conducted during reasonable times and normal business hours at the applicable Marketplacer location, subject to Marketplacer policies.

iii) Conducted upon reasonable advance notice to Marketplacer (such notice to be provided in writing and at least 30 days prior to the proposed audit commencement date).

iv) Of reasonable duration and scope (such duration and scope to be mutually agreed in writing between the Parties prior to the commencement of the audit) and shall not unreasonably interfere with Marketplacer's day-to-day operations or business activities.

v) Conducted in such a manner that does not violate any agreement between Marketplacer and its service providers, including cloud providers, or other customers, or violate or cause Marketplacer to violate its reasonable policies related to security and confidentiality or otherwise jeopardize the confidentiality of Marketplacer's or Marketplacer's customers' information.

vi) Operator acknowledges that access to any of Marketplacer's sub-processors' facilities, systems and/or staff that may be required in connection with any audit pursuant to this Section, is subject to agreement from the relevant sub-processor and that Marketplacer cannot guarantee such access to that subprocessor's facilities, systems or staff or their assistance with any audit.

c) Third Parties. In the event that Operator conducts an audit through a third party independent auditor or a third party accompanies Operator or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Marketplacer's and Marketplacer's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

d) Audit Results. Upon Marketplacer's request, after conducting an audit, Operator shall notify Marketplacer of the audit results and manner in which Marketplacer does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein and, on Marketplacer's request, provide a copy of the relevant audit report or written findings, unless prohibited by law. Upon such notice, Marketplacer shall use reasonable efforts to make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Operator when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Operator may conduct a follow-up audit within six (6) months of Marketplacer's notice of completion of any necessary changes (subject to the Audit Terms set out in this Section 7). To the extent that an Operator audit identifies any material security vulnerabilities, Marketplacer shall use reasonable efforts to promptly remediate those vulnerabilities. The parties agree that the audit report is the confidential information of Marketplacer and shall be subject to all restrictions related to confidential information contained in the Agreement.

8. Data Storage and Deletion.

a) Data Storage. Marketplacer will not store or retain any Operator Personal Data except as necessary to perform the Services under the Agreement or otherwise as may be required by law.

b) Data Deletion. Marketplacer will abide by the following with respect to deletion of Operator Personal Data:

i) Within ninety (90) calendar days of the Agreement's expiration or termination, Marketplacer will

securely destroy (per subsection (iii) below) all copies of Operator Personal Data (including automatically created archival copies).

ii) Upon Operator's request, Marketplacer will promptly return to Operator a copy of all Operator Personal Data within thirty (30) calendar days and, if Operator also requests deletion of the Operator Personal Data, will carry that out as set forth above.

iii) All deletion of Operator Personal Data will be conducted in accordance with standard industry practices for deletion of sensitive data.

iv) Tapes, printed output, optical disks, and other physical media will be physically destroyed by a secure method, such as shredding performed by a bonded provider.

v) Upon Operator's request, Marketplacer will provide evidence that Marketplacer has deleted all Operator Personal Data. Marketplacer will provide the "Certificate of Deletion" within thirty (30) calendar days of the Operator's request.

9. Contact Information.

a) Marketplacer and the Operator agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- Marketplacer Designated POC: Roxanne Quinlan, General Counsel, privacy@marketplacer.com.
- Operator Designated POC: Sample Legal Notices Contact, Sample Title, sample@customer.com. If no individual and email is specified here, Marketplacer may use the Operator notice email specified in the Notices section of the Agreement.

Marketplacer Company	Sample Customer **("Operator")**
Signature:	Signature:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:

ANNEX 1 - Technical and Organizational Security Measures

1. INFORMATION SECURITY POLICY

1.1. Marketplacer shall maintain for the Term an information security policy (the "**Security Policy**") that is aligned to meet or exceed commonly-accepted standards of similarly-situated software-as-a-service providers ("**good industry practice**") and that satisfies the requirements set out in this Annexure.

1.2. The objective of Marketplacer's Security Policy and related information security program is to implement data security measures and a formal controls framework based on, among other things, formal audit standards such as ISO27001 (the "Objective"). In order to meet such Objective, Marketplacer shall:

1.2.1. implement and maintain appropriate technical, organizational and security programs and procedures designed to protect the privacy, confidentiality, integrity and availability of Operator Data in accordance with good industry practice;

1.2.2. protect against accidental, unauthorized, unauthenticated or unlawful access, copying, use, processing, storage, disclosure, alteration, transfer, loss, encryption or destruction of the Operator Data (each, a "**Security Incident**") in accordance with good industry practice; and

1.2.3. comply with Applicable Laws that are relevant to the handling, processing and use of the Operator Data in accordance with the Agreement.

1.3. Marketplacer must take all reasonable steps to ensure that its subcontractors meet equivalent requirements to those set out in this Annexure, which the parties agree will be satisfied by inclusion of terms in contracts with subcontractors which are no less onerous than those contained herein.

1.4. Marketplacer will periodically (and, in any event, no less frequently than annually) review, test and, where applicable, update such Security Policy.

2. RISK ASSESSMENTS

2.1. Marketplacer shall:

2.1.1. carry out, at least annually, risk assessments designed to identify material threats (both internal and external) to data in Marketplacer's control (including Operator Data), the likelihood of those threats occurring, and the impact of those threats upon Marketplacer's organization ("**Risk Assessments**");

2.1.2. manage, control and as soon as reasonably practicable remediate threats identified in the Risk Assessments consistent with the Objective and commensurate with the risk, and the sensitivity of the Operator Data;

2.1.3. on an annual basis, engage an appropriate, independent external party to conduct periodic reviews of Marketplacer's information security practices. Marketplacer shall have a process to review, evaluate and as soon as reasonably practicable remediate any risk findings from this testing. Marketplacer shall provide a summary report of the periodic review to the Operator upon request.

3. ORGANIZATIONAL SECURITY AND ACCESS CONTROLS

Employee Screening, Training, Access and Controls

3.1. Marketplacer shall maintain policies and practices that include the following controls and safeguards applied to Marketplacer staff who have access to Operator Data and/or provide Services to the Operator:

3.1.1. pre-hire background checks on job candidates, which are conducted by a third-party background check provider and in accordance with applicable Laws and generally accepted industry standards;

3.1.2. periodic security awareness training on at least an annual basis; and

3.1.3. access to Marketplacer IT systems only from approved Marketplacer-managed devices with appropriate technical security controls (including two-factor authentication).

Physical Security

3.2. Marketplacer shall:

3.2.1. ensure that the Operator Data is hosted on servers located in the AWS region selected by the Operator;

3.2.2. implement and maintain appropriate physical security controls consistent with good industry practice to deter and prevent the unauthorized viewing, copying, alteration or removal of Operator Data from any Marketplacer controlled media on which Operator Data is stored; and

3.2.3. without prejudice to the generality of the foregoing, shall not store Operator Data stored on personal computers, mobile devices, external hard drives or removable media (e.g. USB Thumb Drives, CDs or DVDs) except that Operator permits the storage of non-production data on local devices for testing and debugging purposes provided that such non-production data does not contain any Operator Personal Data.

Access Controls

3.3. Marketplacer shall:

3.3.1. have controls that are designed to:

3.3.1.1. maintain logical separation such that access to Marketplacer systems hosting Operator Data and/or being used to provide the Services to Operator and the Service Recipients will uniquely identify each individual requiring access, and

3.3.1.2. grant access only to authorized Marketplacer Personnel based on the principle of least privileges and prevent unauthorized access to Operator Data;

3.3.2. promptly disable access to Operator Data by any Marketplacer Personnel who no longer requires such access;

3.3.3. ensure only its system administrators have privileges to create access accounts to Marketplacer systems containing Operator Data;

3.3.4. use multi-factor authentication credentials, or another comparably strong authentication mechanism, when accessing Marketplacer systems containing Operator Data or when remotely accessing Marketplacer's internal network; and

3.3.5. maintain details of all Marketplacer Personnel with access to Operator Data.

4. COMMUNICATIONS AND OPERATIONS MANAGEMENT

Penetration Testing

4.1. Marketplacer shall, on an annual basis, engage an appropriate, independent external party to conduct a penetration test on Marketplacer’s networks and applications having access to or holding or containing Operator Data. Marketplacer shall have a process to review, evaluate and as soon as reasonably practicable remediate any risk findings from this testing. Marketplacer shall provide a summary report of the penetration testing to the Operator upon request.

Data Protection

4.2. Marketplacer shall:

4.2.1. encrypt in accordance with good industry practice Operator Data at rest and in transit; and

4.2.2. implement and maintain appropriate security and anti-virus programs in accordance with good industry practice designed to detect the introduction or intrusion of viruses or malicious code on the Platform. Marketplacer shall ensure its anti-virus programs are up-to-date.

5. INCIDENT EVENT

5.1. Each party shall:

5.1.1. if it becomes aware of any actual or potential compromise of the security of the Operator Marketplace or the Operator Data or suspects that any virus or malicious code has been transmitted, uploaded or introduced, notify the other party as soon as is reasonably practicable; and

5.1.2. if it becomes aware of any actual or suspected Security Incident or compromise of Operator's or a Seller's Marketplacer account, promptly notify the other party by email with reasonable details regarding the breach of security or compromise, reasonably cooperate with the other party to enable that party to meet its obligations under Applicable Law, and shall not disclose details about the breach of security to any third party without the prior written consent of the other party (not to be unreasonably withheld or delayed), unless required by Applicable Law or its contractual commitments to third parties (provided that it does not make reference to Operator in such disclosures and notifies Operator prior to such disclosure).

5.2. Marketplacer shall:

5.2.1. develop and implement an incident response plan, specifying the actions to be taken upon the occurrence or threat of a security incident, including escalation and customer notification procedures; and

5.2.2. reasonably assist the Operator in the investigating of any actual, suspected or threatened security incident to the extent that such incident arose, or is likely to arise, in connection with Operator Data, at the Operator’s cost.

6. OPERATOR RESPONSIBILITIES

6.1. The Operator shall promptly comply with any reasonable directions and instructions given by Marketplacer in connection with the Operator's use of the Services for the purpose of protecting the security of systems, networks, data or software.

6.2. The Operator shall:

6.2.1. maintain and update its own operating systems, Internet browsers, anti-virus software, or other software that it uses to access and use the Services and ensure these are kept up to date;

6.2.2. implement and maintain appropriate security and anti-virus programs in accordance with good industry practice designed to detect the introduction or intrusion of viruses or malicious code on the Operator Marketplace and related systems and implement a process designed for removing such viruses and malicious code;

6.2.3. use reasonable endeavors to ensure the accuracy, quality and legality of the Operator Data, the means by which Operator acquires Operator Data, Operator's use of the Operator Data with the Services, and unless agreed otherwise in writing the interoperation of any third-party applications with which Operator uses the Platform or the Services; and

6.2.4. safeguard usernames, passwords or other credentials used to access Operator's account and any activity occurring in Operator's account (other than activity that Marketplacer is directly responsible for and which is not performed in accordance with Operator's instructions).

Exhibit 1

1.1 Subject Matter of Processing	The subject matter and duration of the processing are set out in the Agreement.
1.2 Duration of Processing	The subject matter and duration of the processing are set out in the Agreement.
1.3 Categories of Data Subjects	1.3.1 Operator employees including contractors, temporary employees or agents (authorised by the Operator to use the Services in Admin roles/account holder roles); 1.3.2 Operator customers (who are natural persons); and 1.3.3 Sellers on the Platform (natural persons in Admin/account holder roles authorised by the third party Seller to use the Services, or who are Sellers).
1.4 Nature and Purpose of Processing	Marketplacer processes Operator Personal Data to enable it to provide the Services to Operator and to comply with its obligations under the Agreement.
1.5 Types of Personal Information	The following categories of personal data will be processed: Operator customers/end-users, third party Sellers and employees may submit personal data to Marketplacer in connection with the Services, the extent of which may be determined by Operator's customers/end-users, third party Sellers and employees (as applicable) in their sole discretion, and which may include, but is not limited to the following categories of personal data per data subject category: **1.5.1 Operator's Customers/End-Users** Marketplacer primarily stores the following categories of personal data in connection with orders, invoices and shipments related to Operator customers/end users who purchase Sellers' products or services on the Operator's marketplace: • First and last name • Email address • Contact information (eg. company, phone/mobile number, business address) • Billing and shipping address (Address, City, Country, Postcode, State) • IP address • Shipping data (e.g. tracking link, tracking number) and any related data as may appear on orders or invoices (such as messages to Sellers and/or gift recipients). **1.5.2 Operator's third-party Sellers** Seller data stored by Marketplacer includes the following categories of personal data:-

	• Seller account details (such as username, first and last name, email address, billing address and phone number). • Seller address data (such as address, city, country, postcode, state, latitude, longitude). • Bank account data for the purposes of payouts due to Sellers from Operator, as applicable (such as account name, account code, account number). • Payment data to enable the Operator to charge Sellers for subscriptions and billing, as applicable (such as truncated credit card data and the authorization tokens from the external systems). • Data relating to Seller's authorised users (such as email address, first and last name, user name, IP address). **1.5.3 Operator's employees** Marketplacer processes certain categories of personal data in respect of the Operator's employees representing Operator in connection with the Agreement and/or authorised to access Operator's Operator Control Panel which may include: • Email address • User name • First and last name • Phone number • IP address

Exhibit 2

Available at https://marketplacer.com/legal/global-subprocessor-list/