SELLING.COM DATA PROCESSING ADDENDUM

Controller:	CUSTOMER

and

Controller:	"**SELLING.COM**"

Have entered into a Master Services Agreement, insertion order, or other agreement in which SELLING.COM provides services ("**Services**") to CUSTOMER ("**Agreement**"). This SELLING.COM Data Processing Addendum ("**DPA**"), supplements, is in addition to, and is hereby incorporated by reference into the Agreement.

This DPA reflects SELLING.COM and CUSTOMER's agreement on the terms governing SELLING.COM's Processing of Personal Data under the Agreement in regions where Applicable Privacy Law applies and are in addition to any rights or obligations set forth in the Agreement. SELLING.COM may make reasonable changes to this DPA from time to time, and such changes shall become effective upon immediate notice to CUSTOMER. If there is any conflict between the Agreement and the terms of this DPA, this DPA will govern.

This DPA is dated as of the later of the date of last signature of a party below (the "**DPA Effective Date**").

1. **DEFINITIONS**

1.1 **"Affiliate"** means an entity that owns or controls, is owned, controlled by, or under common control or ownership with SELLING.COM, or CUSTOMER (as applicable), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 "**Applicable Privacy Law**" means all applicable privacy and data security laws, including state, federal and extraterritorial or international laws as well as all regulations applicable to the Services being provided under the Agreement. "Applicable Privacy Laws" include, for example, the EU General Data Protection Regulation 2016/679 ("GDPR") and national laws implementing the GDPR; the GDPR as it forms part of retained EU law in the United Kingdom, as defined in European Union (Withdrawal) Act of 2018, as amended ("UK GDPR"); the EU Privacy and Electronic Communications Directive 2002/58/EC, as implemented; and the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"), and any statute or regulations promulgated thereunder.

1.3 "**Authenticate**" means to use reasonable means to determine that a request to exercise Consumer data rights afforded under Applicable Privacy Law is being made by, or on behalf of, the Consumer who is entitled to exercise such Consumer rights with respect to the Personal Data at issue.

1.4 "**Auditing Party**" means a party chosen by CUSTOMER to conduct an audit under this DPA.

1.5 "**CUSTOMER Data**" means any Personal Data that is provided or otherwise made available to SELLING.COM by CUSTOMER and Processed by SELLING.COM in connection with the Services set forth in the Agreement.

1.6 **"SELLING.COM Data"** means any Personal Data that is provided or otherwise made available to CUSTOMER by SELLING.COM in relation to the Services set forth in the Agreement.

1.7 **“Data Subject”** means the identified or identifiable natural person to whom Personal Data relates.

1.8 **“Data Subject Request”** means a request from a Data Subject to exercise the Data Subject’s rights under Data Protection Laws and Regulations in relation to Personal Data, including with respect to: (a) access, rectification and/or erasure (i.e., “right to be forgotten”) of their Personal Data; (b) restriction of or objection to Processing; (c) data portability; or (d) automated decision-making (including profiling).

1.9 **“EEA”** means the European Economic Area

1.10 **“GDPR”** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.11 **“Permitted Purpose(s)”** means the receipt and subsequent use of Personal Data: (i) as permitted by Data Protection Laws and Regulations; (ii) as instructed by the providing Controller; and/or (iii) as specifically set out in this Addendum.

1.12 **“Personal Data”** means any information or data provided or otherwise made available by SELLING.COM to CUSTOMER or by CUSTOMER to SELLING.COM, that (a) can be used to identify, describe, contact or locate a specific individual; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as “personal data”, “personal information” or is protected as such under applicable Data Protection Laws and Regulations. This includes both CUSTOMER Data and SELLING.COM as defined in this Addendum.

1.13 **“Personnel”** means the officers, employees, agents, consultants, representatives and other personnel of the parties and/or of their Sub- processors, if applicable, that process Personal Data on their behalf.

1.14 **“Process” or “Processed” or “Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, including, but not limited to, 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.

1.15 “**Processing Signal**” means any flag or signal mutually agreed by the parties in writing that indicates a Consumer has opted out of the Sale, Share, or Processing for purposes of Targeted Advertising of their Personal Data.

1.16 **“Processor”** means an entity which Processes personal data on behalf of the Controller.

1.17 **“Regulator”** means any person or regulatory body with responsibility for monitoring and/or enforcing compliance with the Data Protection Laws and Regulations.

1.18 **“Restricted Transfer”** means any transfer of Personal Data between the parties where such transfer would be prohibited by the GDPR in the absence of adequate safeguards approved by the European Commission.

1.19 **“Security Breach”** means any actual loss, unauthorized or unlawful Processing, destruction, damage, alteration, or unauthorized disclosure of, or access to Personal Data (accidental or otherwise), and/or any other irregularity in Processing that compromises the availability, authenticity, integrity and/or confidentiality of Personal Data.

1.20 **“Services”** means services, products and/or other activities to be supplied to CUSTOMER or carried out by SELLING.COM for CUSTOMER pursuant to the Agreement.

1.21 “**Standard Contractual Clauses” or “SCCs”** means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914

of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj and equivalent clauses for international transfer of data issued by the Information Commissioner for the United Kingdom under S119A(1) Data Protection Act 2018.

1.22 "**Subprocessors**" means third-parties authorized under this DPA to have logical access to and Process CUSTOMER Data in order to provide parts of the Services and any related technical support.

The terms "**Business**", "**Business Purpose**", "**Controller**", "**Consumer**", "**Cross-Contextual Behavioral Advertising**", "**Personal Data**", "**Processor**", "**Sale**" or "**Sell**", "**Service Provider**", "**Share**" or "**Sharing**", "**Supervisory Authority**", "**Targeted Advertising**" and "**Third Party**" as used in this DPA will have the meanings ascribed to them in Applicable Privacy Law. References in this DPA to "**Personal Data**" and "**Consumer**" include "**Personal Information**" and "**Data Subject**" respectively.

2. PROCESSING OF DATA

2.1 **Party Responsibilities**. Each party to this DPA: (a) is an independent controller of Personal Data under Applicable Data Protection Law; (b) will individually determine the purposes and means of its processing of Personal Data; and (c) will comply with the obligations applicable to it under Applicable Data Protection Law with respect to the processing of Personal Data. Nothing in this Section 2 shall modify any restrictions applicable to either party's rights to use or otherwise process Personal Data under the Agreement, and you will process Personal Data solely and exclusively for the purposes specified in the Agreement.

2.2 **CUSTOMER Processing**. CUSTOMER may have the ability to take Personal Data from the Platform, including in transaction logs, event feeds, or other mechanisms. CUSTOMER hereby acknowledges that it has the responsibility to ensure that it has a legal basis for any Processing of any data that it acquires from the Platform.

2.3 **CUSTOMER Responsibilities**. The Parties will: (a) ensure that their personnel engaged in the Processing of Personal Data have committed themselves to confidentiality obligations; (b) implement appropriate technical and organizational measures to safeguard Personal Data 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; (c) upon reasonable request by either Party, make available all information in the other Party's possession necessary to demonstrate their compliance with their obligations under Applicable Privacy Law; and (d) taking into account the nature of the Processing and information available to the Parties, by appropriate technical and organizational measures, insofar as reasonably practicable, assist one another in meeting their obligations as Controllers under Applicable Privacy Law.

2.4 **CUSTOMER Data Provided to SELLING.COM**. CUSTOMER shall have sole responsibility for the accuracy, quality, and legality of CUSTOMER Data CUSTOMER provides to SELLING.COM and the means by which CUSTOMER obtained the CUSTOMER Data. Without limiting anything in the Agreement and unless otherwise expressly agreed in the applicable Agreement, CUSTOMER shall not: provide to SELLING.COM, import into the Platform, or cause SELLING.COM to Process any (a) information regarding an individual that would be considered protected, sensitive, special or similar under Applicable Privacy Law, including any information that could be deemed PHI as defined under the Health Insurance Portability and Accountability Act of 1996; or (b) Directly Identifying Information. If CUSTOMER provides or causes SELLING.COM to Process any Directly Identifying Information, CUSTOMER shall, at CUSTOMER's sole cost: (a) immediately notify SELLING.COM in writing; and (b) take all necessary steps to assist SELLING.COM in removing Directly Identifying Information from SELLING.COM's systems.

3. DATA SUBJECT RIGHTS

3.1 The Parties shall assist one another with commercially reasonable cooperation in fulfilling their respective obligations to respond to Data Subject requests to exercise Data Subject rights under Applicable Privacy Law taking into account (i) the nature of the Processing and the information available

to SELLING.COM; (ii) the timing of the Data Subject request; and (iii) the extent to which CUSTOMER could respond to such requests itself through its use of, or receipt of or access to data from, the Services. CUSTOMER shall be responsible for ensuring adequate Authentication of all Data Subject requests.

3.2 The Parties shall, to the extent legally permitted, promptly notify one another if they receive a Data Subject request specific to the other Party to exercise Data Subject data rights including rights to access, correct, amend, seek deletion of or object to the Processing of Personal Data relating to such individual.

4. RESTRICTED TRANSFERS

4.1 **General Authorization**. The Party's acknowledge and agrees that Personal Data may be processed in jurisdictions other than the jurisdiction in which it was collected, including the United States, provided that all such transfers are compliant with the provisions on the transfer of Personal Data to third countries in accordance with Applicable Privacy Law such as, if necessary pursuant to transfers of Personal Data outside of the EEA, UK and Switzerland.

4.2 If SELLING.COM transfers Personal Data originating from the EEA to countries outside the EEA that have not received a binding adequacy decision by the European Commission, such transfers shall be made in compliance with applicable data transfer legal requirements. The parties acknowledge and agree to abide by the obligations set out in the Standard Contractual Clauses, attached as **ANNEX.2**, for any transfers of Personal Data from within the EEA to outside of the EEA.

4.3 If SELLING.COM transfers Personal Data originating from the UK to countries outside the UK that have not received an adequacy regulation by the UK Secretary of State for the Department for Digital, Culture, Media and Sport, then the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the "**UK Addendum**") attached as **ANNEX.2.1** to this DPA shall apply in addition to and supersede where inconsistent with the Standard Contractual Clauses in **ANNEX.2**. The parties acknowledge and agree to abide by the obligations set out in the UK Addendum.

4.4 In relation to transfers of Personal Data protected by the Swiss Federal Act on Data Protection ("**FADP**"), the Standard Contractual Clauses in **ANNEX.2** shall apply with the following modifications: (i) references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the FADP and the equivalent articles or sections therein; (ii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and "Swiss law"; (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "competent Swiss courts"; and (iv) the Standard Contractual Clauses shall be governed by the laws of Switzerland. The term "Member State" 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).

5. SECURITY

5.1 **Security Measures.** In Processing Personal Data, each party shall maintain the appropriate technical and organizational measures to protect Personal Data provided by the other party hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), and to ensure the confidentiality and integrity of such Personal Data.

5.2 **Notification Obligations**. In the event either Party becomes aware of any Security Breach that triggers the consumer and/or regulatory reporting requirements under Applicable Privacy Law, that Party will notify the other Party of the Security Breach without undue delay. CUSTOMER shall not be liable for Security Breaches to the extent they are caused by SELLING.COM or SELLING.COM's personnel or end users. SELLING.COM shall not be liable for Security Breaches to the extent they are caused by CUSTOMER or CUSTOMER 's personnel or end users.

5.3 **Manner of Notification**. Notification(s) of Security Breaches, if any, will be delivered to the other

Party's DPO reference in **ANNEX.1**. It is CUSTOMER's sole responsibility to ensure it maintains accurate contact information on SELLING.COM's support systems at all times.

5.4 **No Admission**. SELLING.COM's notification of or response to a Security Breach under this Section will not be construed as an acknowledgement by SELLING.COM of any fault or liability with respect to the Security Breach.

6. TERM; DESTRUCTION OF CUSTOMER DATA

6.1 **Term of DPA**. This DPA will take effect on the DPA Effective Date and will remain in full force and effect so long as the Agreement remains in effect and for a commercially reasonable time thereafter while SELLING.COM winds down and ceases its processing of CUSTOMER Data.

6.2 **Destruction of Personal Data**. Prior to the termination of the Agreement, upon either Party's reasonable request to delete Personal Data, the other Party will facilitate such deletion, insofar as possible taking into account the nature and functionality of the Services and unless Applicable Privacy Law or other applicable law requires storage. Upon termination of the Agreement and within thirty (30) days from the termination of the Agreement (unless a longer period is agreed in writing by the parties), CUSTOMER and/or their contracted Processor(s) will (a) cease all Processing of Personal Data; and (b) at the choice of SELLING.COM, either return to SELLING.COM or destroy all Personal Data, except to the extent that CUSTOMER is required under Applicable Privacy Law or other applicable law to keep a copy of the Personal Data.

CUSTOMER:	SELLING.COM:
_____	_____
Signature: _____	Signature: _____
Title: _____	Title: _____
Date: _____	Date: _____

ANNEX.1

Scope of Processing

A. LIST OF PARTIES

DATA IMPORTER DETAILS

Name:	CUSTOMER: As set forth in the Agreement.
Address:	As set forth in the Agreement.
Contact Details for Data Protection:	As set forth in the Agreement.
Activities:	As set forth in the Agreement.
Role:	Controller

DATA EXPORTER DETAILS

Name:	SELLING.COM
Address:	2385 NW Executive Center Drive, Suite 100, Boca Raton, FL 33431
Contact Details for Data Protection:	Les Riordan l.riordan@selling.com
Activities:	Direct data collection; parsing, formatting or transformation; presentation, access, reading, use or copy; storage and updates.
Role:	Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

1. Customers of either party and/or end users either party's products and services;
2. Prospective customers or sales prospects;

3. Business partners and vendors;
4. Employees, consultants, or other contacts of a party's customer, business partners, and/or vendors;
5. Employees, agents, advisors, contractors, freelancers of a party and
6. Any user authorized by Party 2 to use Party 1's services.

Categories of personal data transferred:

1. First and last name;
2. Business contact information (SELLING.COM, email, phone, physical business address);
3. Personal contact information (email, telephone and/or mobile number);
4. Employer;
5. Title;
6. Position and
7. Professional life data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): As set forth in the contract.

Nature of the processing:

- direct data collection (i.e., data are collected directly from individuals or recorded via a system);
- data acquired from other sources or third parties (i.e., data are received from an external system or third-party source);
- parsing, formatting or transformation (i.e., data are read and restructured, reformatted or specific types of data are extracted to make them easier to process);;
- presentation, access, reading, use or copy (i.e., data are retrieved and processed by presenting them to users, accessed by system users or processes, or otherwise accessed, used or copied);
- update (i.e., changes to the values in an existing data set; the update action is expected when a personal data set needs to be kept current and up-to-date);
- sharing with third parties (i.e., data are shared with or sent to a third party) and
- storage (i.e., data are hosted or stored as a structured or unstructured data set; the data set may be partitioned and stored in multiple locations for

Purpose(s) of the data transfer and further processing:

- direct data collection (i.e., data are collected directly from individuals or recorded via a system);
- data acquired from other sources or third parties (i.e., data are received from an external system or third-party source);
- parsing, formatting or transformation (i.e., data are read and restructured, reformatted or specific types of data are extracted to make them easier to process);;
- presentation, access, reading, use or copy (i.e., data are retrieved and processed by presenting them to users, accessed by system users or processes, or otherwise accessed, used or copied);
- update (i.e., changes to the values in an existing data set; the update action is expected when a personal data set needs to be kept current and up-to-date);
- sharing with third parties (i.e., data are shared with or sent to a third party) and
- storage (i.e., data are hosted or stored as a structured or unstructured data set; the data set may be partitioned and stored in multiple locations for performance, scalability or reliability reasons; includes data sets stored for archive or backup purposes).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

As set forth in the contract or, if not set forth in the contract, as long as reasonably necessary to performance of the contract. In addition, data may be retained for a period in excess of the contract requirements where necessary to meet legal requirements or where otherwise required by law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

See Schedule 1 to this Annex

C. COMPETENT SUPERVISORY AUTHORITY

In accordance with Clause 13 the competent supervisory authority will be:

If Customer is established in an EU Member State, then the supervisory authority of that Member State; or

If Customer is not established in an EU Member State, falls within the territorial scope of application of the regulation, and has appointed a representative, then the supervisory authority of the Member State that the representative is established; or

If Customer is not established in an EU Member State, falls within the territorial scope of application of the regulation, and has not appointed a representative, then the Irish Data Protection Commission.

Schedule 1

LIST OF SUB-PROCESSORS

Sub-Processor	Location	Description of Processing	Website & Contact Details
Amazon Web Services, Inc	USA	Cloud hosting and infrastructure provider	https://aws.amazon.com 440 Terry Avenue N Seattle, WA 98109
Calendly	USA	Calendar meeting scheduling platform	https://calendly.com/privacy 115 E. Main Street, Ste A1B Buford, GA 30518
Clari	USA	Conversation intelligence platform	https://www.clari.com/ 1154 Sonora Court Sunnyvale, CA 94086
Custify	Romania	Customer success and analytics platform	https://www.custify.com/ Bucharest, Zagazului Street, No. 4E Entrance A, First Floor, ap. 1A District 1, Romania
DocuSign, Inc.	USA	Contract administration and signature tool	https://www.docusign.com/ 221 Main Street Suite 1550 San Francisco, CA 94105
Google LLC	USA	Cloud hosting and infrastructure provider	https://www.google.com/ 1600 Amphitheatre Parkway Mountain View, CA 94043
Hubspot	USA	Inbound marketing management tool	https://www.hubspot.com/ Two Canal Park Cambridge, MA 02141 USA
Intercom	USA	Customer support and knowledgebase tool	https://www.intercom.com/ 55 2nd Street, 4th Fl., San Francisco, CA 94105
LuckyOrange	USA	Customer analytics tool	https://www.luckyorange.com/ 8665 W 96th St Suite #100 Overland Park, KS 66212
Microsoft	USA	Email service provider (Outlook)	https://www.microsoft.com/en-us/ One Microsoft Way Redmond, Washington 98052
Nylas	USA	Email integration provider	https://www.nylas.com/ 3223 Hanover St, Suite 110 Palo Alto, CA 94304
OpenAI, LLC	USA	Speech-to-text and text analytics tool	https://openai.com/ 3180 18th St. San Francisco, CA 94110
Salesforce, Inc.	USA	Customer relationship	https://www.salesforce.com/

		management platform	415 Mission St, 3rd Floor San Francisco, CA 94105
Slack Technologies, LLC	USA	Internal messaging channel	https://slack.com/ 500 Howard Street San Francisco, CA 94105
Stripe, Inc.	USA	Payment processing and subscription management tool	https://stripe.com/ 354 Oyster Point Boulevard South San Francisco, California, 94080
Twilio, Inc.	USA	Programmable communication tool	https://www.twilio.com/ 101 Spear Street, 5th Floor San Francisco, California, 94105
Zoom Video Communications, Inc.	USA	Video conferencing tool	https://zoom.us/ 55 Almaden Blvd, Suite 600 San Jose, CA 95113

ANNEX.2

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex.1 (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex.1 (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex.1.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b)

(iii) Clause 12(a) and (d)

(iv) Clause 13

(v) Clause 15.1(c), (d) and (e); ;

(vi) Clause 16(e)

(vii) Clause 18(a) and (b) ;

(b)Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those

terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex.1.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex.1.

(b) Once it has completed the Appendix and signed Annex.1, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex.1.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational

measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex.1. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would

otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d)Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a)Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b)If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c)The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a)The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(b) The Parties have agreed on the technical and organisational measures set out in Annex.3. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) it's likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or

biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a)Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b)The data importer shall make such documentation available to the competent supervisory authority on request.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b)The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Intentionally Left Blank

Clause 10

Data subject rights

(a)The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b)In particular, upon request by the data subject the data importer shall, free of charge:

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex.1; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a

democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body [11] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex.1, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which

the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex.1, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex.1, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a)The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX.2.1
UK Addendum

PART 1 – TABLES

Table 1 : Parties

Start Date	The date when Customer signs the Agreement that incorporates this Addendum
The Parties	As Set out in ANNEX.1

Table 2: Selected SCCs, Modules, and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses, or optional provisions of the Approved EU SCCs brought into effect for the purpose of this Addendum:				
Module	Module in Operation	Clause 7	Clause 11	Clause 9a Authorization	Clause 9a Time Period	Is personal data received from the importer combined with personal data collected by the Exporter?
	1	YES	YES	n/a	n/a	YES

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

ANNEX.1 Part A: List of Parties: ANNEX.1
ANNEX.1 Part B: Description of Transfer: ANNEX.1
ANNEX.3: Technical and Organizational measures including technical and organizational measures to ensure the security of the data: ANNEX.3

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ___ Importer ___ Exporter _x_ Neither Party

PART 2 – MANDATORY CLAUSES

Mandatory Clauses	Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

ANNEX.3

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Customer shall establish and maintain industry standard security measures that meet or exceed the security standards and certifications Selling.com employs as further described below. Customer shall be able to adequately demonstrate its compliance with these obligations to ZoomInfo upon request.

Description of the technical and organizational measures implemented by SELLING.COM (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. Please note, where both parties are importers, the other party guarantees that its Technical and Organizational Measures are substantially similar to those of SELLING.COM below.

Technical and Organizational Security Measures

Area	Practices
Organization of Information Security	**Security Ownership**. SELLING.COM has an information security department under the Guidance of its Technology Director responsible for coordinating and monitoring Cybersecurity **Security Roles and Responsibilities**. SELLING.COM personnel with access to Customer Data are subject to confidentiality obligations. **Data Protection Office**. SELLING.COM has appointed a Data Protection Officer
Asset Management	**Asset Inventory**. SELLING.COM maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to SELLING.COM personnel authorized in writing to have such access.
Human Resources Security	**Security Training**. SELLING.COM informs its personnel about relevant security procedures and their respective roles **Data Protection Training**. SELLING.COM issues all staff with data protection training modules on induction and refresher training every year. Training modules cover data protection principles, data subject access request, data breach and keeping data secure.
Physical and Environmental Security	**Physical Access to Facilities**. SELLING.COM limits access to facilities where information systems that process Customer Data are located to identified, authorized individuals. **Protection from Disruptions**. SELLING.COM uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

	Component Disposal. SELLING.COM uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. SELLING.COM maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery**. SELLING.COM ensures off-site and on-site backup of Customer data are maintained. **Malicious Software**. SELLING.COM has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries**. SELLING.COM encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. **Event Logging**. SELLING.COM logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. SELLING.COM maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization**. SELLING.COM maintains and updates a record of personnel authorized to access SELLING.COM systems that contain Customer Data. **Least Privilege**. Technical support personnel are only permitted to have access to Customer Data when needed. SELLING.COM restricts access to Customer Data to only those individuals who require such access to perform their job function. **Authentication**. SELLING.COM uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, SELLING.COM requires that the passwords are renewed regularly.
Information Security Incident Management	**Incident Response Process**. SELLING.COM has a management team and process for information security incidents as set forth in its detailed Information Security Incident Response Policy. SELLING.COM provides notification of a security incident in compliance with appropriate laws, or regulations.
Data Protection	SELLING.COM encrypts data during transmission and at rest. SELLING.COM monitors data protection compliance and regularly tests the effectiveness of the measures in place. SELLING.COM tests staff adherence to data protection and information governance policies and procedures.
Business Continuity Management	SELLING.COM maintains emergency and contingency plans for the facilities in which SELLING.COM information systems that process Customer Data are

	located. SELLING.COM has a disaster recovery plan in place for the restoration of critical processes and operations of the Hosted Service at the hosting location from which the Hosted Service is provided.

SELLING.COM Supplemental Measures

Area	Practices
Technical	The personal data is processed using strong encryption during transmission. SELLING.COM Inc. has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems by third parties.
Contractual	SELLING.COM monitors changes to local law and will inform the data exporter/importer of any changes that will impact the maintenance of an 'essentially equivalent level of data protection' for the personal data transferred. SELLING.COM has a process in place to assess local laws to ensure the legality of any disclosure of personal data.
Organizational	SELLING.COM has a set of internal policies relating to requests from law enforcement agencies for access to personal data. SELLING.COM provides a training program for all staff on procedures and processes for dealing with law enforcement agencies for requests to access personal data. SELLING.COM keeps a register for requests from Public Authorities. SELLING.COM conducts audits and allows inspections to verify if data was disclosed to public authorities. SELLING.COM has appointed a Data Protection Officer who is consulted on all high risk transfers. Data Access and confidentiality policies and best practices in place and include regular review and audits.