Junip Data Processing Addendum

Last Updated: April 3, 2023

This Data Processing Addendum ("**DPA**") is incorporated by reference into the Junip Terms of Service or other agreement governing the use of Junip Services (the "**Agreement**") entered by and between you, the Client (collectively, "**you**", "**your**", "**Client**"), and Junip, Inc. or an Affiliate ("**Junip**," "**we**," "**us**," or "**our**") to reflect the parties' agreement with regard to the Processing of Personal Data by Junip on behalf of the Client. Both parties shall be referred to as the "**Parties**" and each, a "**Party**"..

Capitalized terms not otherwise defined in this DPA shall have the meaning ascribed to them in the Agreement.

By using the Services, Client accepts this DPA and you represent and warrant that you have full authority to bind the Client to this DPA. If you cannot, or do not agree to, comply with and be bound by this DPA, or do not have authority to bind the Client or any other entity, please do not provide Personal Data to us.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. DEFINITIONS

Unless otherwise defined in the Agreement (including this DPA), all terms in this DPA shall have the definitions given to them in Applicable Data Protection Laws.

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Mandatory Clauses;

"**Authorized Affiliate**" means any of Client's Affiliate(s) which is permitted to use the Service pursuant to the Agreement between Client and Junip but has not entered directly into its own agreement with Junip and is not a "Client" as defined under the Agreement.

"**CCPA/CPRA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq, and its implementing regulations, as may be amended from time to time, including the California Privacy Rights Act.

The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CCPA/CPRA.

For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent that the CCPA/CRPA applies. In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider.

"**Data Protection Laws**" means all applicable laws, rules, regulations and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time.

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

"**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Mandatory Clauses**" means "**Part 2: Mandatory Clauses**" of the Approved Addendum;

"**Personal Data**" or "**Personal Information**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly,

to or with an identified or identifiable natural person or Consumer, to the extent such information is processed by Junip on behalf of Client, under this DPA and the Agreement between Client and Junip.

"**Security Measures**" means the security measures applicable to the Services used by Client, as updated from time to time, and accessible via https://junip.co/legal/security-measures.

"**Sensitive Data**" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Laws.

"**Standard Contractual Clauses**" shall mean (i) the standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("EU SCCs"); or (ii) where the UK GDPR applies, the International Data transfer Addendum to the EU SCCs issued by the Information Commissioner's Office in the UK, as applicable.

"**Sub-processor**" means any third party that Processes Personal Data under the instruction or supervision of Junip.

"**UK GDPR**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Personal Data performed on behalf of Client, (i) Client is the Controller of Personal Data, (ii) Junip is the Processor of such Personal Data, (iii) for the purposes of the CCPA/CPRA (and to the extent applicable), Client is the "Business" and Junip is the "Service Provider" (as such terms are defined in the CCPA/CPRA), with respect to Processing of Personal Data described in this

Section 2.1. The terms "**Controller**" and "**Processor**" below hereby signify Client and Junip, respectively.

2.2 Client's Processing of Personal Data. Client, in its use of the Service, and Client's instructions to the Processor, shall comply with Data Protection Laws. Client shall establish and have any and all required legal bases in order to collect, Process and transfer to Processor the Personal Data, and to authorize the Processing by Processor, and for Processor's Processing activities on Client's behalf, including the pursuit of 'business purposes' as defined under the CCPA/CPRA.

2.3 Processor's Processing of Personal Data. When Processing on Client's behalf under the Agreement, Processor shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Client as part of its provision of the Services; (iii) Processing to comply with Client's reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed; (iv) rendering Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder; (v) Processing as required under the laws applicable to Processor, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Processor shall inform Client of the legal requirement before Processing, unless such law or order prohibit such information on important grounds of public interest.

Processor shall inform Client without undue delay if, in Processor's opinion, an instruction for the Processing of Personal Data given by Client infringes applicable Data Protection Laws. To the extent that Processor cannot comply with an instruction from Client, Processor (i) shall inform Client, providing relevant details of the issue, (ii) Processor may, without liability to Client, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend Client's access to the Services, and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Client may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Client shall pay to Processor all the amounts owed to Processor or due before the date of termination. Client will

have no further claims against Processor (including, without limitation, requesting refunds for Service) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by Processor is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of Processing) to this DPA.

2.5 Sensitive Data. The Parties agree that the Services are not intended for the processing of Sensitive Data, and that if Client wishes to use the Services to process Sensitive Data, it must first obtain the Processor's explicit prior written consent and enter into any additional agreements as required by Junip.

2.6 CCPA/CPRA Standard of Care; No Sale of Personal Information. Processor shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Client's behalf, nor shall it combine the Personal Information Processed on Client's behalf with any information it processes on behalf of any other parties, by way of logical separation, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA. Processor certifies that it understands the rules, requirements and definitions of the CCPA/CPRA and agrees to refrain from selling and/or sharing (as such term is defined in the CCPA/CPRA) any Personal Information Processed hereunder without Client's prior written consent or instruction, nor taking any action that would cause any transfer of Personal Information to or from Processor under the Agreement or this DPA to qualify as "selling" or "sharing" such Personal Information under the CCPA/CPRA.

3. DATA SUBJECT REQUESTS

As between the Parties, Client shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Consumer Personal Data ("**Data Subject**

Request"). Processor shall, to the extent legally permitted, notify Client or refer Data Subject or Consumer to Client, if Processor receives a Data Subject Request. Taking into account the nature of the Processing, Processor shall assist Client by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfillment of Client's obligation to respond to a Data Subject Request under Data Protection Laws. Processor may advise Data Subjects on available features for self-exercising their Data Subject Requests through the Services (where appropriate), and/or refer Data Subject Requests received, and the Data Subjects making them, directly to the Client for its treatment of such requests.

4. CONFIDENTIALITY

Processor shall ensure that its personnel and advisors engaged in the Processing of Personal Data have committed themselves to confidentiality.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Client acknowledges and agrees that (a) Processor's Affiliates may be engaged as Sub-processors; and (b) Processor and Processor's Affiliates on behalf of Processor may each engage third-party Sub-processors in connection with the provision of the Service.

5.2 List of Current Sub-processors and Notification of New Sub-processors.

> **5.2.1** Processor makes available to Client the current list of Sub-Processors used by Processor to process Personal Data. The Junip Sub-Processors List includes the identities of those Sub-processors and the entity's country ("**Sub-Processors List**"). The Sub-Processors List as of the date of first use of the Service by Client is hereby deemed authorized upon first use of the Services. Client will have no further claims against Processor due to (i) past use of approved Sub-processors prior to the date of the first use of the Services or (ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.2.2 Processor shall provide notification of any new Sub-processor(s) at least fifteen (15) days before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3 Objection to New Sub-processors. Client may reasonably object to Processor's use of a new Sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by notifying Processor promptly in writing within seven (7) days after receipt of a Processor notification. Such written objection shall include the reasons for objecting to Processor's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within seven (7) days following Processor's notice shall be deemed as acceptance of the new Sub-Processor. In the event Client reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Processor will use reasonable efforts to make available to Client a change in the Service or recommend a commercially reasonable change to Client's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Client. If Processor is unable to make available such change within thirty (30) days, Client may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Service which cannot be provided by Processor without the use of the objected-to new Sub-processor, by providing written notice to Processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Processor. Until a decision is made regarding the new Sub-processor, Processor may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Services. Client will have no further claims against Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.4 Agreements with Sub-processors. Processor or a Processor's Affiliate on behalf of Processor has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where Processor engages a Sub-processor for carrying out specific Processing activities on behalf of the Client, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular obligations to implement appropriate technical and organizational

measures in such a manner that the processing will meet the requirements of applicable Data Protection Laws. Where a Sub-processor fails to fulfill its data protection obligations concerning its processing of Personal Data, Processor shall remain responsible for the performance of the Sub-processor's obligations.

6. SECURITY & AUDITS

6.1 Controls for the Protection of Personal Data. Processor shall maintain industry-standard technical and organizational measures for protection of Personal Data Processed 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, confidentiality and integrity of Personal Data, including those measures set forth in the Security Measures), as may be amended from time to time. Upon the Client's reasonable request, Processor will reasonably assist Client, at Client's cost and subject to the provisions of Section 11.1 below, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to Processor.

6.2 Audits and Inspections.

> **6.2.1** Upon Client's 14 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Client, Processor shall make available to Client that is not a competitor of Processor (or Client's independent, reputable, third-party auditor that is not a competitor of Processor and not in conflict with Processor, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Client to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Processor's prior written approval. Upon Processor's first

request, Client shall return all records or documentation in Client's possession or control provided by Processor in the context of the audit and/or the inspection).

6.2.2 In the event of an audit or inspections as set forth above, Client shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Processor's premises, equipment, personnel and business while conducting such audit or inspection.

6.2.3 The audit rights set forth in this paragraph above, shall only apply to the extent that the Agreement does not otherwise provide Client with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

6.3 Adequacy of Measures. Client acknowledges and agrees that, 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, Junip's Security Measures are appropriate to ensure the security of the Personal Data.

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Processor maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by Processor on behalf of the Client (a "**Data Incident**"). Processor shall make reasonable efforts to identify and take those steps as Processor deems necessary and reasonable in order to remediate and/or mitigate the cause of such Data Incident to the extent the remediation and/or mitigation is within Processor's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or anyone who uses the Services on Client's behalf. Client will not make, disclose, release or publish any finding,

admission of liability, communication, notice, press release or report concerning any Data Incident which directly or indirectly identifies Processor (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Processor's prior written approval, unless, and solely to the extent that, Client is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Client shall provide Processor with reasonable prior written notice to provide Processor with the opportunity to object to such disclosure and in any case Client will limit the disclosure to the minimum scope required.

8. RETURN AND DELETION OF PERSONAL DATA

Following termination of the Agreement and subject thereto, Processor shall, at the choice of Client (indicated through the Service or in written notification to Processor), delete or return to Client all the Personal Data it Processes on behalf of the Client, and Processor shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, Processor may also retain one copy of the Personal Data solely for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Transfers from the EEA, the United Kingdom and Switzerland to countries that offer adequate level of data protection**. Personal Data may be transferred from EU Member States, the three other EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), the United Kingdom ("**UK**") and Switzerland to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, the UK, and/or Switzerland ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.

9.2 Transfers from the EEA, the United Kingdom and Switzerland to other countries. If the Processing of Personal Data by Processor includes a transfer (either directly or via onward

transfer) from the EEA ("**EEA Transfer**"), the UK ("**UK Transfer**"), and/or Switzerland ("**Swiss Transfer**") to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Processor for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, as relevant) outside the EEA, the UK or Switzerland, as applicable, then (i) the terms set forth in the Standard Contractual Clauses (EEA Cross Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in Annex III (UK Cross Border Transfers) shall apply to any such UK Transfer ("**UK Addendum**"); (iii) the terms set forth in Annex IV (Swiss Cross Border Transfers) shall apply to any such Swiss Transfer; and (iv) the terms set forth in Annex V (Additional Safeguards) shall apply to any such transfers.

To the extent that the processing of Personal Data is subject to UK or Swiss Data Protection Laws, the UK Addendum and/or Swiss Addendum (as applicable) set out in Schedule 3 shall also apply.

9.3 Personal Data Subject to U.S. Data Privacy Laws. To the extent that the processing of Personal Data is subject to U.S. Data Protection Laws, the U.S. Addendum set out in Schedule 4 of this DPA shall apply.

9.4 Standard Contractual Clauses

The Parties agree that the terms of the Standard Contractual Clauses Module Two (Controller to Processor) and Module Three (Processor to Processor), as further specified in Schedule 2 of this DPA, are hereby incorporated by reference and shall be deemed to have been executed by the Parties and apply to any transfers of Personal Data falling within the scope of the GDPR from Client (as data exporter) to Junip (as data importer).

10. AUTHORIZED AFFILIATES

10.1 Contractual Relationship. The Parties acknowledge and agree that, by executing the DPA, the Client enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Client's obligations under this DPA, if and to the extent that Processor Processes Personal Data

on the behalf of such Authorized Affiliates, thus qualifying them as the "**Controller**". All access to and use of the Service by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Client.

10.2 Communication. Client shall remain responsible for coordinating all communication with Processor under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11. OTHER PROVISIONS

11.1 Data Protection Impact Assessment and Prior Consultation. Upon Client's reasonable request, Processor shall provide Client, at Client's cost, with reasonable cooperation and assistance needed to fulfill Client's obligation under the GDPR or the UK GDPR (as applicable) to carry out a data protection impact assessment related to Client's use of the Service, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide, at Client's cost, reasonable assistance to Client in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.1, to the extent required under the GDPR or the UK GDPR, as applicable.

11.2 Modifications. You acknowledge and agree that Junip may amend this DPA from time to time by posting the relevant amended and restated DPA on Junip's website, available at https://junip.co/legal/data-processing-addendum, and such amendments to the DPA are effective as of the date of posting. Your continued use of the Services after the amended DPA is posted to Junip's website constitutes your agreement to, and acceptance of, the amended DPA. If you do not agree to any changes to the DPA, do not continue to use the Services.

SCHEDULE 1 – DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Service to Client;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Client's instructions, where such instructions are consistent with the terms of the Agreement;
4. Sharing Personal Data with third parties in accordance with Client's instructions and/or pursuant to Client's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Client to facilitate the sharing of Personal Data between the Services and such third party services);
5. Complying with applicable laws and regulations;
6. All tasks related with any of the above.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Processor will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

The Personal Data processed may consist of name, email address, telephone number, email data, system usage data, location data (physical address, IP address), purchase information (e.g. details concerning products or services purchased and time of purchase, but excluding payment method details) and other electronic data submitted, stored, sent, or received by the Data Subjects.

Categories of Data Subjects

The Data Subjects are Client's end users and shoppers who purchase products and/or services from Client online, or submitted a review via the onsite reviews widget that is installed on the Client's website.

List of the Parties

1. Data Exporter

Client and/or the Client Affiliates operating in the countries which comprise the European Economic Area, UK and/or Switzerland and/or – to the extent agreed by the Parties – Client and/or the Client Affiliates in any other country to the extent the GDPR or corresponding Swiss law applies.

Client and Client Affiliate's contact person's position and contact details as well as (if appointed) the data protection officer's and (if relevant) the representative's contact details will be notified to Junip prior to the processing of personal data via email to privacy@juniphq.com or an available form provided by Junip in Client's account in the Services.

The activities relevant to the data transfer are defined by the Agreement and the data exporter who decides on the scope of the processing of Personal Data in connection with the Services further described in this Schedule 1 and in the Agreement.

2. Data Importer

Junip Inc.
101 Spadina Avenue, Unit 207
Toronto ON M5V 2K2 Canada

The data importer's contact person can be contacted at privacy@juniphq.com.

The data importer's activities relevant to the data transfer are as follows: the data importer processes Personal Data provided by the data exporter on behalf of the data exporter in connection with providing the Services to the data exporter as further specified in this Schedule 1 and in the Agreement.

SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES

As stipulated in clause 9.4 of the DPA, the Standard Contractual Clauses shall apply to any applicable processing of Personal Data as between Client and Junip. Unless otherwise defined in this attachment, capitalized terms used in these Standard Contractual Clauses have the meanings given to them in the DPA.

Junip agrees to implement the measures agreed upon and set forth in the applicable Standard Contractual Clauses and supplemental measures described herein in order to enable Client's compliance with requirements imposed on the transfer of personal data to third countries, as follows:

1. In general, Module Two shall apply in the case of the processing under the DPA and, in certain cases where Client functions as a processor on behalf of its customers where Client and Client's customer have concluded a data processing agreement in relation to the processing of Personal Data of Client's customers, Module Three shall apply.

2. Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

3. Clause 9(a) Option 2 (General written authorization) is selected, and the time period to be specified is determined in clause 5.2.2 of the DPA.

4. The option in clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.

5. With regard to clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that option one shall apply. The parties agree that the governing law shall be the law of the Republic of Ireland.

6. In clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of the Republic of Ireland.

7. For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.

8. For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 2 contains the technical and organizational measures.

9. The specifications for Annex III of the Standard Contractual Clauses, are determined by clauses 5.1 and 5.2 of the DPA. The Sub-processor's contact person's name, position and contact details will be provided by Junip upon request.

SCHEDULE 3 – UK AND SWISS ADDENDUM

1. UK ADDENDUM

With respect to any transfers of Personal Data falling within the scope of the UK GDPR from Client (as data exporter) to Junip (as data importer):

1.1 The Approved Addendum as further specified in this Schedule 3 shall form part of this DPA, and the Standard Contractual Clauses shall be read and interpreted in light of the provisions of the Approved Addendum, to the extent necessary according to clause 12 of the Mandatory Clauses.

1.2 In deviation to Table 1 of the Approved Addendum and in accordance with clause 17 of the Mandatory Clauses, the Parties are further specified in Schedule 1 of this DPA.

1.3 The selected Modules and Clauses to be determined according to Table 2 of the Approved Addendum are further specified in Schedule 2 of this DPA as amended by the Mandatory Clauses.

1.4 Annex 1 A and B of Table 3 to the Approved Addendum are specified by Schedule 1 of this DPA, Annex II of the Approved Addendum is further specified by the Security Measures of this DPA, and Annex III of the Approved Addendum is further specified by this DPA.

1.5 Junip (as data importer) may end this DPA, to the extent the Approved Addendum applies, in accordance with clause 19 of the Mandatory Clauses.

1.6 Clause 16 of the Mandatory Clauses shall not apply.

2. SWISS ADDENDUM

As stipulated in section 9.2 of the DPA, this Swiss Addendum shall apply to any processing of Personal Data subject to Swiss Data Protection Law or to both Swiss Data Protection Law and the GDPR.

<u>2.1 Interpretation of this Addendum</u>

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses as further specified in Schedule 2 of this DPA, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

(i) "This Addendum" means This Addendum to the Clauses.
(ii) "Clauses" means The Standard Contractual Clauses as further specified in Schedule 2 of this DPA.
(iii) "Swiss Data Protection Laws" means The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

(b) This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfills the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(c) This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

2.2 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

2.3 Incorporation of the Clauses

(a) In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA including as further specified in Schedule 2 of this DPA to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and
(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(b) To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs, as further specified in Schedule 2 of this DPA and as required by clause 2.1 of this Swiss Addendum, include (without limitation):

(i) References to the "Clauses" or the "SCCs" means this Swiss Addendum as it amends the SCCs and
(ii) Clause 6 Description of the transfer(s) is replaced with:"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 those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."
(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or "GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.
(iv) References to Regulation (EU) 2018/1725 are removed.
(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".
(vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws;
(vii) Clause 17 is replaced to state:"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".
(viii) Clause 18 is replaced to state:"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect Personal Data of legal entities and legal entities shall receive the same protection under the Clauses as natural persons.

2.4 To the extent that any processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, the DPA including the Clauses as further specified in Schedule 2 of this DPA will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by clauses 2.1 and 2.3 of this Swiss Addendum, with the sole exception that clause 17 of the SCCs shall not be replaced as stipulated under clause 2.3(b)(vii) of this Swiss Addendum.

2.5 Client warrants that it and/or Client Affiliates have made any notifications to the FDPIC which are required under Swiss Data Protection Laws.

SCHEDULE 4 - U.S. ADDENDUM

As stipulated in clause 9.3 of the DPA, this U.S. Addendum shall apply to any processing of Personal Data subject to US Data Protection Laws.

To the extent required by US Data Protection Laws, Junip is prohibited from:

(a) selling Personal Data or otherwise making Personal Data available to any third party for monetary or other valuable consideration;

(b) sharing Personal Data with any third party for cross-behavioral advertising;

(c) retaining, using, or disclosing Personal Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by US Data Protection Laws;

(d) retaining, using or disclosing Personal Data outside of the direct business relationship between the Parties; and

(e) except as otherwise permitted by US Data Protection Laws, combining Personal Data with Personal Data that Junip receives from or on behalf of another person or persons, or collects from its own interaction with the data subject.