DATA PROTECTION ADDENDUM

1. SCOPE

a. IP Styler or its Affiliate, as identified in the Agreement ("Company") and Partner (each "Party"), as defined below, are parties to the Agreement, as defined below, to which this Data Protection Addendum applies. If Company Processes Personal Data on behalf of the Partner as part of the Agreement then Company shall comply with the terms and conditions of this Data Protection Addendum ("Data Protection Addendum").

2. DEFINITIONS

All capitalized terms not defined in this Data Protection Addendum have the meanings set forth in the Agreement.

a. "Affiliate" means any person or entity directly or indirectly controlling, controlled by, or under common control with a Party. For the purpose of this definition, "control" (including, with correlative meanings, the terms "controlling", "controlled by" and "under common control with") means the power to manage or direct the affairs of the person or entity in question, whether by ownership of voting securities, by contract or otherwise.
b. "Agreement" means the agreement between Company and Partner which involves Company having access to or otherwise Processing Personal Data;

c. "Approved Jurisdiction" means a member state of the EEA, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacydecisions_en.

d. "Breach Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

e. "Data Protection Laws" means any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, as updated from time to time, including the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including 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 ("GDPR").

f. "EEA" means those countries that are member of the European Economic Area.

g. "Partner" refers to the legal entity, regardless of the form of organization, which entered into the Agreement. h. "Personal Data" or "personal data" has the meaning as defined in the Data Protection Laws.

i. "Process" or "process" has the meaning as defined in the Data Protection Laws. "Processes" or "processes" and "Processing" or "processing" shall be construed accordingly.

j. "Special Categories of Data" has the meaning as defined in the Data Protection Laws.

3. DATA PROTECTION AND PRIVACY

a. If Partner wishes Company to Process Personal Data on its behalf, then Partner hereby represents and warrants that:

i. Partner is and will be throughout the term of the Agreement in compliance with all applicable requirements of Data Protection Laws with respect to the Processing of Personal Data;

ii. Without derogating from the generality of the above, Partner acknowledges and agrees that it will be solely responsible for: (a) the accuracy, quality, and legality of Personal Data and the means by which Partner acquired such Personal Data; (b) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations; (c) ensuring that Partner has the right to transfer, or provide access to, the Personal Data to Company for Processing in accordance with the terms of the Agreement (including this DPA); (d) ensuring that Partner's Instructions to Company regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws;

b. If Company has access to or otherwise Processes Personal Data, then Company shall:

i. only Process the Personal Data in accordance with Partner's documented instructions and on its behalf, and in accordance with the Agreement and this Data Protection Addendum;

ii. take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process, Personal Data; ensure persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and ensure that such personnel are aware of their responsibilities under this Data Protection Addendum and any Data Protection Laws (or Company’s own written binding policies are at least as restrictive as this Data Protection Addendum);

iii. assist Partner as needed to cooperate with and respond to requests from supervisor authorities, data subjects, customers, or others to provide information (including details of the services provided by Company) related to Company’s Processing of Personal Data;

iv. notify the Partner without undue delay after becoming aware of a Breach Incident;

v. provide full, reasonable cooperation and assistance to Partner in:

a. allowing data subjects to exercise their rights under the Data Protection Laws, including (without limitation) the right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or the right not to be subject to an automated individual decision making;

b. ensuring compliance with any notification obligations of personal data breach to the supervisory authority and communication obligations to data subjects, as required under Data Protection Laws;

c. Ensuring compliance with its obligation to carry out data protection impact assessments with respect to the Processing of Personal Data, and with its prior consultation with the supervisory authority obligation (as applicable).

vi. only process or use Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;

vii. upon termination of the Agreement, or upon Partner's written request at any time during the term of the Agreement, Company shall cease to Process any Personal Data received from Partner, and within a reasonable period will at the request of Partner, securely and completely destroy or erase all Personal

Data in its possession or control (including any copies thereof), unless and solely to the extent the foregoing conflicts with any applicable laws.

4. SUBCONTRACTING

a. Partner hereby grants a general authorization to the Company to subcontract its obligations under this Data Protection Addendum to another person or entity ("Contractor(s)"), in whole or in part.

b. Company is hereby permitted to continue the processing of Personal Data by those Contractors engaged by Company as at the date of this Data Protection Addendum.

c. Company can at any time and without justification appoint a new Contractor provided that Company provides seven (7) days' prior notice and the Partner does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Contractor's non-compliance with Data Protection Law.

d. Company will execute a written agreement with each Contractor containing substantially similar terms to this Data Protection Addendum.

e. Company shall be responsible for the acts or omissions of Contractors to the same extent it is responsible for its own actions or omissions under this Data Protection Addendum.

5. THE TRANSFER OF PERSONAL DATA

a. If the Company is required to Processes Personal Data from the EEA in a jurisdiction that is not an Approved Jurisdiction, Company shall ensure that it has a legally approved mechanism in place to allow for the international data transfer, including, without limitation, entering into the Standard Contractual Clauses where the Partner shall be deemed the Data Exporter and the Company shall be deemed as the Data importer.

6. SECURITY STANDARDS

a. Company shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed; all other unlawful forms of Processing; including (as appropriate):

(i) the pseudonymisation and encryption of personal data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

7. GENERAL

a. Partner shall have the right to: (a) require from Company all information necessary to, and (b) conduct its own audit and/or inspections of Company in order to: demonstrate compliance with the Data Protection Addendum and the applicable Attachments. Such audit and/or inspection shall be conducted with at least thirty (30) days' advanced notice to Partner, and shall take place during normal business hours to reasonably limit any disruption to Company’s business and no more than once each calendar year.