Subcontractor Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the agreement ("**Agreement**") between "**Solo**" (as defined in the signature block of the Agreement) and "**Subcontractor**" (as defined in the signature block of the Agreement) for the services performed pursuant to the Agreement.

This DPA describes the commitments of Solo and Subcontractor concerning the Processing of Personal Data in connection with the performance of Professional Services by Subcontractor for or on behalf of Solo contemplated by the Agreement.

The capitalized terms used in this DPA have the meaning set forth in this DPA. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement.

Solo and Subcontractor agree as follows:

1. **Definitions**

1.1 "**Applicable Data Protection Laws**" means, to the extent applicable to a party's Processing of Solo Personal Data under the Agreement, (i) European Data Protection Laws; (ii) Canadian Privacy Laws; and (iii) US Privacy Laws; in each case as may be amended, superseded, or replaced.

1.2 "**Authorized Affiliate**" means an Affiliate of Solo who has not signed an Order Form but acts as a Controller or Processor for the Solo Personal Data Processed by Subcontractor pursuant to the Agreement, for so long as such entity remains a Solo Affiliate.

1.3 "**Canadian Privacy Laws**" means, as applicable, (i) the federal Personal Information Protection and Electronic Documents Act (PIPEDA), the provincial Personal Information Protection Act in place in each of Alberta and British Columbia, and an Act Respecting The Protection of Personal Information In The Private Sector (Québec) as amended by An Act to modernize legislative provisions as regards the protection of personal information (Law 25), and each of their implementing regulations; (ii) the Canada Anti-Spam Act Legislation (CASL) and its implementing regulations; and (iii) other Canadian data privacy and security laws and regulations to the extent applicable to the Processing of Personal Data under the Agreement; in each case as may be amended, superseded, or replaced.

1.4"**Controller**" has the meaning attributed to the term in the relevant Applicable Data Protection Law or, if not defined, then means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data. If the CCPA applies to Subcontractor hereunder, then a reference to Controller when the context indicates use in connection with the CCPA means "business," as such term is defined in the CCPA.

1.5 "**EEA**" means the countries that are parties to the agreement on the European Economic Area.

1.6 "**European Data Protection Laws**" means, as applicable, (i) Regulation 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) ("**GDPR**"); (ii) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC (e-Privacy Directive); (iii) any applicable national implementations of (i) and (ii); (iv) the Switzerland Federal Act on Data Protection, as amended by the Federal Act of 25 September 2020 on Data Protection (nFADP), and its ordinances ("**Swiss DPA**"); and (v) the United Kingdom ("**UK**") Data Protection Act 2018 and the GDPR as saved into UK law by virtue of Section 3 of the UK's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of Section 2 of the UK's European Union (Withdrawal) Act 2018; in each case as may be amended, superseded, or replaced.

1.7 "**Personal Data**" means any information that relates to an identified or identifiable natural person and that is protected as "personal data," "personal information," "personally identifiable information," or a like defined term under the relevant Applicable Data Protection Law.

1.8 "**Process**," "**Processes**," "**Processed**," and "**Processing**" has the meaning attributed to the term in the relevant Applicable Data Protection Law or, if not defined, then means any operation or set of operations performed on Personal Data, including access, storage, and use.

1.9 “**Processor**” has the meaning attributed to the term in the relevant Applicable Data Protection Law or, if not defined, then means a natural or legal person that Processes Solo Personal Data. If the CCPA applies to Subcontractor hereunder, then a reference to Processor when the context indicates use in connection with the CCPA means “service provider,” as such term is defined in the CCPA.

1.10 “**Restricted Transfers**” means (i) where the GDPR applies, a transfer of Solo Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission (an “**EEA Restricted Transfer**”); (ii) where the UK GDPR applies, a transfer of Solo Personal Data from the UK to any other country which is not subject to adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018 (a “**UK Restricted Transfer**”); and (iii) where the Swiss DPA applies, a transfer of Solo Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner (a “**Swiss Restricted Transfer**”).

1.11 “**Security Incident**” means the accidental or unlawful destruction, loss, or alteration or unauthorized disclosure of or unauthorized access to Solo Personal Data transmitted, stored, or otherwise Processed by Subcontractor or its Sub-processors in connection with the Agreement that is known by or reasonably suspected by Subcontractor or would be reasonably suspected by a commercially reasonable person exercising a commercially reasonable level of care and diligence.

1.12 “**Standard Contractual Clauses**” or “**SCCs**” means the standard contractual clauses as adopted by the EU Commission by means of the Implementing Decision EU 2021/914 of June 4, 2021 found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

1.13 “**Sub-processor**” means any Processor that Processes Solo Personal Data on behalf of Subcontractor.

1.14 “**Solo Personal Data**” means the Personal Data that Subcontractor has access to or receives from or on behalf of Solo or a Subscriber in connection with the Agreement, and includes the Personal Data described in Section 2.6.6 of this DPA.

1.15 “**UK Addendum**” means that certain international data transfer addendum to the SCCs issued by the UK Information Commissioner for Parties making transfers of Personal Data from the UK to any other country which is not deemed adequate under Article 46 of the UK GDPR.

1.16 “**US Privacy Laws**” means all United States federal and state data privacy, information security, and data breach notification laws and implementing regulations to the extent applicable to the Processing of Solo Personal Data by Subcontractor in connection with the Agreement, including but not limited to the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (CPRA) (together the “**CCPA**”), the Virginia Consumer Data Protection Act (VCDPA), the Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA), and the Utah Consumer Privacy Act (UCPA), and each of their implementing regulations.

1.17 The terms “**data subject**” and “**supervisory authority**” shall have the meanings given to them in the applicable European Data Protection Laws; and the terms “**business purpose**”, “**consumer**”, and “**sell**” shall have the meanings given to them in the CCPA or, to the extent applicable, another US Privacy Law. Sell includes “sale of personal data” as such term is defined by an applicable US Privacy Law.

2. **Roles and Scope of Processing**

2.1 **Scope**. This DPA applies to the extent that Subcontractor Processes in its capacity as a Processor any Solo Personal Data in connection with the Agreement.

2.2 **Roles of the Parties**. The parties acknowledge and agree that (i) Solo is a Processor acting on behalf of its own customers, who may be Controllers or Processors, with respect to the Processing of Solo Personal Data received from such customers; and (ii) Subcontractor shall Process Solo Personal Data (a) only as a Processor on behalf of Solo, as further described in this DPA, including in Sections 2.3 and 2.6; and (b) in accordance with the Applicable Data Protection Laws.

2.3 **Subcontractor Processing of Personal Data**. Subcontractor agrees that it shall Process Solo Personal Data only for the purposes described in the Agreement and in accordance with Solo’s documented instructions. The parties agree that the Agreement and this DPA set out Solo’s instructions to Subcontractor in relation to the Processing of Solo Personal Data. Solo understands that additional instructions outside the scope of the Agreement or this DPA shall be agreed to in writing between Subcontractor and Solo. Subcontractor shall notify Solo in writing, unless prohibited from doing so under Applicable Data Protection Laws, (i) if Subcontractor becomes aware or believes that any Processing instructions from Solo violates Applicable Data Protection Laws and, in such event, Subcontractor may suspend performance of such instruction until Solo modifies the instruction in writing, provides written confirmation that the instruction is lawful, or withdraws the instruction; or (ii) if Subcontractor is unable to follow Solo's Processing instructions.

2.4 **Solo Affiliates**. Subcontractor's obligations set forth in this DPA shall also extend to Authorized Affiliates**.**

2.5 **Details of Processing**. Details of Processing by Subcontractor are set forth below:

2.5.1 **Subject Matter of Processing**. Solo Personal Data that Solo or Subscriber elects to transfer to Subcontractor in connection with Subcontractor's performance of the Agreement.

2.5.2 **Frequency and Duration of Processing**. The frequency of the Processing is continuous during the performance of an applicable SOW under the Agreement. Subcontractor shall Process Solo Personal Data for the duration of an SOW until disposal of the Solo Personal Data at the conclusion of an SOW, and Section 6 of this DPA.

2.5.3 **Nature of Processing**. The nature of the Processing is to perform the Professional Services under the Agreement.

2.5.4 **Purpose of Processing**. The purpose of the Processing is as necessary to perform the Professional Services under the Agreement.

2.5.5 **Categories of Data Subjects**. Categories of data subjects is as determined by Solo and includes natural persons whose Personal Data Solo or Subscriber elects to transfer to Subcontractor for the performance of the Professional Services set forth in an applicable SOW under the Agreement. This may include but is not limited to: (i) prospects, customers, business partners and vendors of Solo or Subscriber (who are natural persons); (ii) employees or contacts persons of Customer's prospects, customers, business partners and vendors; and/or (iii) employees, agents, and advisors of Solo or Subscriber (who are natural persons).

2.5.6 **Type of Personal Data**. Includes Personal Data types that are included in data that Solo or Subscriber elects to transfer to Subcontractor for the performance of the Professional Services. The may include but are not limited: (i) first name and last name, name of individual's employer, business mailing address, job title, business email address, business telephone number, the individual's area of responsibility, and the information automatically collected by commercially available email and network systems such as Microsoft's Outlook or Google's Gmail product (such as the sender's IP address); (ii) IP addresses, usage data, cookie data, location data, and (iii) any non-production data that includes Personal Data.

3. **Sub-Processing**

3.1 **Authorized Sub-processors**. Solo acknowledges and agrees that Subcontractor may engage third-party Sub-processors to Process Solo Personal Data on Solo's behalf. The list of such Sub-processors is set forth in an applicable SOW. Solo hereby consents to the Sub-processors listed in an SOW for performing the Professional Services under such SOW.

3.2 **Sub-processor Obligations**. Subcontractor, as applicable, shall enter into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those set forth in this DPA with respect to the protection of Solo Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. Subcontractor shall remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Subcontractor to breach any of Subcontractor's obligations under this DPA.

3.3 **Changes to Sub-processors**. Subcontractor shall notify Solo in writing before Subcontractor adds to or replaces its Sub-processors under an SOW. Solo may object in writing to Subcontractor's appointment of a new Sub-processor by notifying Subcontractor promptly in writing within thirty (30) calendar days of the date Subcontractor issues such notice. If Solo objects to the appointment to a Sub-Processor, then Subcontractor shall not appoint the objected to Sub-processor.

4. **Security and Audits**

4.1 **Subcontractor Security Measures**. Subcontractor shall implement and maintain appropriate technical and organizational security measures designed to protect Solo Personal Data from Security Incidents and to preserve the security and confidentiality of the Solo Personal Data ("**Security Measures**"). Such measures will include, at a minimum: (i) measures for certification or similar assurance of data protection in processes and products; (ii) measures for ensuring data minimization; (iii) measures for ensuring data quality; (iv) measures for ensuring limited data retention; (v) measures for ensuring accountability; (vi) measures for allowing data portability where required by Applicable Data Protection Law; and (vii) measures for ensuring erasure, and such measures are further described in Annex II of this DPA. Subcontractor shall ensure that any person who is authorized by Subcontractor to process Solo Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.2 **Security Incident Response**. Upon becoming aware of a Security Incident, Subcontractor shall notify Solo within 48 hours of becoming aware of such Security Incident and shall: (i) provide timely information relating to the Security Incident, including a summary of the known circumstances of the Security Incident and the corrective actions taken or to be taken by Subcontractor, as such incident becomes known or as is reasonably requested by Solo; (ii) promptly take steps, necessary to contain, investigate, and remediate any Security Incident; and (iii) communicate and cooperate with Solo concerning its responses to the Security Incident.

4.3 **Security Audits**. Subcontractor shall maintain an audit program to help ensure compliance with the obligations set out in this DPA, and shall provide Solo with information demonstrating its compliance with the obligations set out in this DPA, including but not limited to: (i) any audit reports as stated in Section 4.3.1; and (ii) any other written responses (on a confidential basis) to all reasonable requests made by Solo related to Subcontractor's processing of Solo Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Subcontractor's compliance with this DPA. The exercise of any audit rights under the SCCs are set forth below:

4.3.1 **Third-Party Certifications and Audits**. Upon Solo's request, at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Subcontractor shall make available to Solo or Solo's Third-Party Auditor (as defined in Section 4.3.4) information regarding Subcontractor's compliance with the obligations set forth in this DPA in the form of a copy of Subcontractor's then most recent third-party audits or certifications, such as a Service Organization Control (SOC) 2 or a comparable report ("**Subcontractor Audit Reports**"). Such third-party audits or certifications may also be disclosed to Solo's competent supervisory authority on its request. Upon request, Subcontractor shall also provide Solo with a report and/or confirmation of a report of any Third-Party Auditors' audits of Sub-processors that have been made available by those external Sub-processors to Subcontractor, but solely to the extent that the external Sub-processor allows Subcontractor to disclose such reports or evidence to Solo ("**Sub-processor Audit Reports**"). Solo acknowledges that (i) Subcontractor Audit Reports shall be the Confidential Information of Subcontractor; and (ii) Sub-processor Audit Reports shall be the Confidential Information of Subcontractor as well as the confidential information of the Sub-processor.

4.3.2 **Solo (On-Site) Audit**. Solo may request an (on-site) audit of Subcontractor's applicable controls related to the processing activities under this DPA when: (i) the information provided under Section 4.3.1 is not sufficient to demonstrate Subcontractor's compliance with the obligations set out in this DPA; (ii) required by Applicable Data Protection Laws or Solo's competent supervisory authority; or (iii) Subcontractor has experienced a Security Incident.

4.3.3. **Conduct of On-Site Audit**. Any on-site audit described in Section 4.3.2 above will (i) be limited to processing facilities operated by Subcontractor; (ii) be conducted reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Professional Services; (iii) conducted no more than one (1) time per twelve (12) months with at least two (2) weeks' notice unless an emergency justifies less notice, in which case, the parties will use good faith efforts to accommodate the shorter notice period; and (iv) conducted during Subcontractor's normal business hours and shall not unreasonably interfere with Subcontractor's day-to-day operations. Before any on-site audit, Solo and Subcontractor shall agree upon the scope, timing, and duration of the audit. Solo will promptly provide Subcontractor with information regarding any non-compliance discovered during the course of an On-Site Audit. The results of any On-Site Audit shall be considered Subcontractor's Confidential Information and may be disclosed to a third party (other than a Third-Party Auditor, where applicable) only with Subcontractor's prior written consent.

4.3.4 **Third-Party Auditor**. A "Third-Party Auditor" means a third-party independent contractor that is not a competitor of Subcontractor. An On-Site Audit can be conducted through a Third-Party Auditor if: (i) prior to the On-Site Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Subcontractor's and its customers' proprietary and confidential information.

4.4 **Data Protection Impact Assessments.** To the extent required under Applicable Data Protection Laws, Subcontractor shall provide reasonably requested information regarding Subcontractor's processing of Solo Personal Data under the Agreement to assist Solo to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.

5 **International Transfers**

5.1 **Processing locations.** Solo acknowledges and agrees that Subcontractor may transfer and Process Solo Personal Data to and in the United States unless expressly stated otherwise in an SOW or as reasonably necessary to provide the Professionals Services or as necessary to comply with the law or binding order of a governmental body. Vendor shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this DPA, which Processing shall at all times comply with the relevant jurisdiction specific terms set forth in Section 8.

6. **Deletion of Solo Personal Data**

6.1 Upon termination or expiration of the Agreement, Subcontractor shall delete all Solo Personal Data (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Vendor is required by applicable law to retain some or all of the Solo Personal Data, in which case Vendor shall retain such Solo Personal Data in compliance with all Applicable Data Protection Laws.

7. **Rights of Individuals and Cooperation**

7.1 **Data Subject Requests.** To the extent that Subscriber is unable to independently access the relevant Solo Personal Data and to the extent such information is available to Subcontractor, Subcontractor shall, taking into account the nature of the Processing, provide Solo with the reasonable cooperation and assistance necessary for Solo to respond to any requests from data subjects, consumers, or applicable supervisory authorities or government regulators relating to the Processing of Solo Personal Data under the Agreement. If Subcontractor receives any such request directly, Subcontractor shall not respond to such communication directly without Solo's prior authorization, except to acknowledge receipt of the request and to attempt to redirect the requestor to contact Solo directly. If Subcontractor's attempt is unsuccessful or if Subcontractor is otherwise required to provide a substantive response to such request, then, unless legally prohibited from doing so, Subcontractor shall promptly notify Solo and provide Solo with a copy of the request and, to the extent permitted by Applicable Data Protection Laws, Solo shall assume responsibility for providing such substantive response to the requestor.

7.2 **Subpoenas and Court Orders**. Notwithstanding anything to the contrary in the Agreement, if a law enforcement agency sends Subcontractor a demand for Solo Personal Data (for example, through a subpoena or court order), Subcontractor shall attempt to redirect such agency to contact Solo directly and, if Subcontractor's attempt is unsuccessful, then, except as otherwise prohibited by law or such demand, Subcontractor shall give Solo prompt written notice of the demand to allow Solo to seek a protective order or other appropriate remedy. If Subcontractor is legally prohibited from providing Solo with such notice, then, if, after careful assessment, Subcontractor's concludes that there are reasonable grounds to consider the demand or prohibition to be unlawful, Subcontractor shall take commercially reasonable steps to challenge such demand or prohibition. For the avoidance of doubt, nothing in this DPA shall be interpreted to require Subcontractor to pursue action or inaction that could result in a civil or criminal penalty for Subcontractor, Including without limitation a contempt of court.

8. **Jurisdiction Specific Terms**

8.1 **Restricted Transfers.**

8.1.1 **GDPR**. In connection with any transfer of Solo Personal Data by Solo to Subcontractor that is an EEA Restricted Transfer, Subcontractor agrees to abide by and Process Solo Personal Data in compliance with the Standard Contractual Clauses, which are hereby incorporated into this DPA by reference as follows:

8.1.1.1 Module 3 (*Processor to Processor Transfers*) shall apply;

8.1.1.2 For Clause 7, the optional docking clause shall apply;

8.1.1.3 For Clause 9(a), Option 1 shall apply and the time period for prior notice of Sub-processor changes shall be as set out in Section 3.3 of this DPA;

8.1.1.4 For Clause 9(c), where confidentiality restrictions prohibit Subcontractor from providing a copy of a Sub-processor agreement to Subscriber, Subcontractor shall (on a confidential basis) provide all information that it reasonably can in connection with such Sub-processor Agreement to Solo;

8.1.1.5 For Clause 11(a), the optional language shall not apply;

8.1.1.6 For Clause 13 and Annex I.C of the SCCs, Solo shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to Subcontractor on request.

8.1.1.7 For Clause 17, Option 1 shall apply, and the SCCs shall be governed by the law of The Netherlands;

8.1.1.8 For Clause 18(b), disputes shall be resolved before the courts of The Netherlands; and

8.1.1.9 For Annex I.A., the "data importer" shall be Subcontractor and the "data exporter" shall be Solo and any Authorized Affiliates that have acceded to the SCCs pursuant to this DPA.

8.1.1.10 For Annex I.B., the description of the transfer is as described in Section 2.6 of this DPA.

8.1.1.11 For Annex II, the technical and organizational measures are: (i) with respect to Subcontractor, those measures described in Section 4.1 of this DPA; and (ii) with respect to Solo, those measures described in Section 4.2 of this DPA.

8.1.1.12For Annex III, the Sub-processors shall be as described in Section 3.1 of this DPA.

8.1.2 **UK GDPR**. In connection with any transfer of Solo Personal Data to Subcontractor from Solo which is a UK Restricted Transfer to which the UK GDPR applies, the SCCs shall apply in accordance with Section 8.1.1 above, but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which are hereby incorporated into and form an integral part of this DPA but only for purposes of UK Restricted Transfers. Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Section 2.6 of this DPA, and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

8.1.3 **Swiss DPA**. In connection with any transfer of Solo Personal Data to Subcontractor which is a Swiss Restricted Transfer to which the Swiss DPA applies, the SCCs shall apply in accordance with Section 8.1.1 above, but with the following modifications:

8.1.3.1 any references in the SCCs to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein;

8.1.3.2 any references to "EU," "Union," "Member State," and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be;

8.1.3.3 any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and

8.1.3.4 the SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

8.2 **Standard Contractual Clauses Precedence**. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the SCCs. Accordingly, if any express term of this CPA conflicts with the SCCs, then the SCCs, if applicable, shall control as to that term, but only to the extent of an express ambiguity.

8.3 **Alternative Transfer Mechanism**. Subcontractor and Solo agree that Sections 8.1.1 to 8.1.3 shall apply only to the extent that in the absence of their application either party would be in breach of European Data Protection Laws in connection with the transfer of Solo Personal Data from Solo to Subcontractor. To the extent Subcontractor adopts an alternative mechanism for the lawful transfer of Solo Personal Data not described in this DPA ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall, upon notice to Solo, apply to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to the territories to which Solo Personal Data is transferred. In addition, if and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders or determines (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Solo Personal Data to Subcontractor, Solo acknowledges and agrees that Subcontractor may, at

Subcontractor’s sole discretion, implement any additional measures or safeguards that may be required to enable the lawful transfer of such Solo Personal Data and if Subcontractor chooses not to implement such additional measures or safeguards, then Subcontractor shall provide prompt written notice to Solo and the parties shall reasonable cooperate to determine a mutually agreeable accommodation that permits each party to meet its respective obligations under the applicable European Data Protection Laws.

8.4 **US Privacy Laws.** To the extent that Subcontractor’s Processing of Solo Personal Data under the Agreement is subject to US Privacy Laws and to the extent required under applicable US Privacy Laws, Solo and Subcontractor agree that:

8.4.1 Without limiting the terms of Section 2.3 and Section 2.6, Subcontractor shall Process the Solo Personal Data to communicate with Solo personnel about the Solo Offerings and the Products, perform the Solo Offerings, and otherwise meet Subcontractor’s obligations under this DPA and the Agreement (collectively, the “**Permitted Purposes**”);

8.4.2 Subcontractor shall not collect, retain, use, or disclose Solo Personal Data outside of the direct business relationship between Solo and Subcontractor, or for any purpose other than for the Permitted Purposes, including retaining, using, or disclosing Solo Personal Data for a commercial purpose other than the Permitted Purposes, except as otherwise permitted by applicable US Privacy Laws;

8.4.3 Solo is not selling Solo Personal Data to Subcontractor and Subcontractor shall not sell Solo Personal Data;

8.4.4 Subcontractor shall not share Solo Personal Data except as otherwise permitted by this DPA, the Agreement, or the applicable US Privacy Laws, including without limitation for a business purpose;

8.4.5 Subcontractor shall not combine Solo Personal Data with Personal Data that Subcontractor receives from or on behalf of another Subcontractor customer, or that Subcontractor may collect from its own interaction with the consumer unrelated to the Agreement, except as otherwise permitted by applicable US Privacy Laws;

8.4.6 Subcontractor shall comply with the US Privacy Laws to the extent applicable to Subcontractor’s performance of the Solo Offerings, including, without limitation, implement the Security Measures; and

8.4.7 Subcontractor engages other Sub-processors to assist in the Processing of Solo Personal Data for the Permitted Purposes, as further described in Section 3.

9. **Miscellaneous**

9.1 Any ambiguity in this DPA shall be resolved to permit the parties to comply with the Applicable Data Protection Laws. If any express term of this DPA conflicts with the Agreement, then this DPA, if applicable, shall control as to that term. The Agreement shall control in all other instances, including, without limitation, notice, assignment, severability, and relationship of the parties.

9.2 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by the relevant Applicable Data Protection Law, and in such event, then only for purposes of this DPA and only for purposes of that specific jurisdiction.

ANNEX II to the SCCs

Description of the technical and organizational security measures implemented by the data processor/importer in accordance with the Standard Contractual Clauses

Subcontractor shall maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Solo Personal Data provided by the data exporter in connection with the Solo Offerings, including the following:

1.**Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed. These measures include:

- Establishing access authorizations for employees and third parties

- Access control system (ID reader, magnetic card, chip card)
- Key management, card-keys procedures
- Door locking (electric door openers etc.)
- Security staff, janitors
- Surveillance facilities, video/CCTV monitor, alarm system
- Securing decentralized data processing equipment and personal computers
- Additional measures as necessary to ensure the physical security of locations where personal data is processed

2.**Virtual access control**

- Technical and organizational measures to prevent data processing systems from being used by unauthorized persons. These measures include:
- User identification and authentication procedures
- ID/password security procedures (special characters, minimum length, change of password)
- Automatic blocking (e.g. password or timeout)
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempt
- Creation of one master record per user, user master data procedures, per data processing environment
- Encryption of archived data media
- Endpoint protection on workstations

3.**Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization. These measures include:

- Internal policies and procedures
- Control authorization schemes
- Differentiated access rights (profiles, roles, transactions and objects)
- Monitoring and logging of accesses
- Disciplinary action against employees who access Personal Data without authorization
- Reports of access
- Access procedure
- Change procedure
- Deletion procedure
- Encryption

4.**Disclosure control**

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed. These measures include:

- Encryption/tunneling
- Logging
- Transport security

5.**Entry control**

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems. These measures include:

- Logging and reporting systems
- Audit trails and documentation

6. **Control of instructions**

Technical and organizational measures ensuring Personal Data are processed solely in accordance with the Instructions of the Controller. These measures include:

- Unambiguous wording of the contract
- Formal commissioning (request form)

7.**Availability control**

Technical and organizational measures ensuring Personal Data are protected against accidental destruction or loss (physical/logical). These measures include:

- Backup procedures
- Mirroring of hard disks (e.g. RAID technology)
- Uninterruptible power supply (UPS)
- Remote storage of backups
- Anti-virus/firewall systems
- Disaster recovery plan

8.**Separation control**

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately. These measures include:

- Separation of databases
- “Internal client” concept / limitation of use
- Segregation of functions (production/testing)
- Procedures for storage, amendment, deletion, transmission of data for different purposes