# CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**DPA**") is entered into by and between Loopio Inc., ("**Loopio**") and the entity identified as the Customer ("**Customer**") in the execution block below, as of the date of the last signature (the "**Effective Date**"). This DPA forms part of, amends or supplements the Master Services Agreement (the "**Agreement**") entered into by the Parties.

Each entity is referred to individually as a "**Party**" and collectively as the "**Parties**".

**HOW TO EXECUTE THIS DPA:**

1. In order for this DPA to be valid and legally binding, the Customer must have entered into a binding Agreement with Loopio.
2. The Customer must complete the required information and counter-sign on page 8 of this DPA; and
3. Submit the completed and signed DPA to Loopio at privacy@loopio.com.
4. Upon Loopio's receipt of the validly completed and signed DPA, in accordance with the instructions above, this DPA will become legally binding. Any questions regarding this DPA should be sent to privacy@loopio.com.

Now whereas, the Parties have entered into the Agreement for the provision of certain services (the "**Services**").

Whereas, in accordance with the Agreement, Loopio will act as a Processor and will process Personal Data on behalf of Customer, also the Controller, solely for the purposes of the Services set out in the Agreement.

Whereas, the Parties agree this DPA, and its applicable appendices shall, apply to the Processing of Personal Data by the Parties subject to the applicable Data Protection Laws in order to provide Services.

Whereas, the Parties agree to comply with applicable Data Protection Laws with respect to the process of Personal Data and Loopio agrees to process Personal Data as described in Appendix 1.

NOW, THEREFORE, in consideration of the premises set forth above and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree on the following:

## 1. DEFINITIONS

All capitalized terms shall have the meaning given to them below. Capitalized terms used in this DPA but not defined shall have the meanings given to them in the Agreement.

**1.1.** "**Commercial Purpose**", "**Controller**", "**Data Subject**", "**Processing"**, "**Processor**", "**Selling**", "**Service Provider**", "**Targeted Advertising**", "**Transfer**" shall have the meaning provided under applicable Data Protection Laws.

**1.2.** "**Adequate Country**" means a country or territory recognized as providing adequate protection for Personal Data transfers under an adequacy decision made from time to time by (as applicable) (i)

the Information Commissioner's Office ("**ICO**") and/or under applicable UK law (including the UK GDPR), or (ii) the European Commission under the GDPR.

**1.3.** "**Data Subject Request**" means a request from or on behalf of a Data Subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or any objection from or on behalf of a Data Subject to the processing of its Personal Data.

**1.4.** "**Data Protection Impact Assessment"** means an assessment of the impact of the envisaged Processing operations on the protection of Personal Information as required by Article 35 of the EU GDPR or other applicable Data Protection Law.

**1.5.** "**Data Protection Law**" means all applicable provisions of all statutes, laws, rules, regulations, administrative codes, ordinances, decrees, orders, decisions, injunctions, awards judgments or other requirements of any Supervisory Authority (as amended, consolidated or re-enacted from time to time) governing the Processing or protection of Personal Data, including and without limitation, GDPR, UK Data Protection Laws, FADP, The Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), and the California Consumer Privacy Act ("**CCPA**").

**1.6.** "**EU SCCs**" means the standard contractual clauses for the transfer of Personal Data to third counties set out in the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

**1.7.** "**FADP**" means the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded) and related ordinances, and, once effective, the revised FADP version of 25 September 2020, as amended or replaced as applicable.

**1.8.** "**GDPR**" means the General Data Protection Regulation (2016/679) along with any member state derogations, laws implementing the General Data Protection Regulation, and regulator guidance that may be issued from time to time.

**1.9.** **"Personal Data**" means any information relating, directly or indirectly, to an identified or identifiable natural person that is Processed by Loopio or Subprocessors under the Agreement. Without limiting the generality of the foregoing, "Personal Data" includes but is not limited to "Personal Information" and similar terms as defined under Data Protection Law to the extent such data is Processed under the Agreement.

**1.10.** "**Security Breach**" means a breach of security leading to the unauthorized, accidental, or unlawful processing Confidential Information including but not limited to any unauthorized access, acquisition, use, disclosure, loss or modification Confidential Information, or any other event that constitutes a "*Breach*" or "*Personal Data Breach*" or other similar terms as defined under applicable Data Protection Law.

**1.11.** "**Subprocessors**" means a third-party who processes Personal Data on behalf of Loopio in connection with the Services.

**1.12.** "**Supervisory Authority**" means an independent public authority tasked with the regulation and enforcement of applicable Data Protection Law, including supervisory authorities established in

Canada, and supervisory authorities established by an EU Member State or the United Kingdom to monitor the application of the EU GDPR or the UK GDPR respectively.

**1.13.** "**UK Approved Addendum**" means the template Addendum B.1.0, to the EU SCCs issued by the UK Information Commissioner's Office in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Approved Addendum and which together with the applicable modules and the corresponding appendices of the EU SCCs, forms part of this DPA.

**1.14.** "**UK Data Protection Laws**" means the Data Protection Act 2018 (DPA 2018), as amended, and EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into UK law as the UK GDPR, as amended, and any other applicable UK data protection laws, or regulatory Codes of Conduct or other guidance that may be issued from time to time.

## 2. Obligations of Processor

**2.1.** Loopio agrees that it shall:

**(a)** Only use, disclose, transfer, retain, and otherwise Process Personal Data as reasonably necessary for the purposes of rendering the Services and as otherwise instructed by Customer in writing, from time to time;

**(b)** Not Process any Personal Data in any other manner than in accordance with the terms of this DPA including processing Personal Data for Targeted Advertising or for any other Commercial Purpose other than performing the Services, without the express prior written authorization of Customer;

**(c)** Inform Customer, if in Loopio's opinion, or if Loopio reasonably believes, that any instruction received from Customer, infringes applicable Data Protection Law;

**(d)** Limit access to Personal Data only to those employees and authorized agents of Loopio on a need to know basis. Loopio shall not disclose (and not allow any of its personnel, Subprocessors, or permitted agents or representatives to disclose) any Personal Data to any third party without the prior authorization of Customer;

**(e)** Ensure or cause each of Loopio's employees and the authorized agents to agree in writing to keep and to protect the confidentiality and security of the Personal Data in accordance with the terms of this DPA and ensure appropriate security training and awareness of its personnel;

**(f)** Loopio shall not combine any Personal Data with Personal Data that Loopio receives from or on behalf of any other third party or collects from its own interactions with Data Subjects provided that Loopio may combine Personal Data for the business purposes specified in the Agreement or this DPA. Loopio represents and warrants that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Loopio to qualify as "selling personal information" under the CCPA; and

**(g)** Loopio may also Process Personal Data where required by applicable Data Protection Law, in which case Loopio will, to the extent permitted by such applicable law, inform Customer of such legal requirement prior to Processing Personal Data.

## 3. Obligations of Controller

**3.1** Customer agrees that it shall:

**(a)** Make and maintain all necessary registrations and notifications as required in order to permit Loopio to perform its obligations and exercise its rights under this DPA;

**(b)** Obtain and provide, all necessary consents and notices, and otherwise has and continues to have all necessary authority to permit Loopio to perform its obligations and exercise its rights under this DPA; and

**(c)** Ensure that there is a valid legal basis to enable Loopio to Process Customer's Personal Data.

## 4. Personal Data Requests

**4.1.** Loopio shall assist Customer, by taking into account the nature of Processing, in the fulfillment of Customer's obligation to respond to Data Subject Requests, including complaints regarding Loopio's or Customer's compliance with any such Data Protection Law. If a Data Subject or authorized individual directly contacts Loopio for the purposes of exercising the Data Subject's right, then Loopio shall:

**(a)** Respond only that it cannot respond to the request because it is a Processor; and

**(b)** Forward the Data Subject's Request to Customer within five (5) business days following receipt of the request. In the event that Customer requests that Loopio assist in connection with any individual rights requests, Loopio shall notify its own Subprocessors to take actions as necessary to comply with such requests.

**4.2.** Loopio will promptly provide reasonable and timely assistance to Customer to enable Customer to respond to any correspondence, inquiry or complaint received from a regulator, attorney general, court, or other party in connection with the processing of Personal Data. If any such communication is made directly to Loopio, Loopio shall within five (5) business days from receipt inform Customer by providing the full details of the communication. Loopio will not respond to the communication directly, unless specifically required by Data Protection Law or authorized by Customer.

**4.3.** Loopio shall, by taking into account the nature of the Processing and Personal Data available to it, provide reasonable assistance to Customer in connection with Customer's obligations under applicable Data Protection Law, including:

**(a)** Obligations relating to ensuring the security and integrity of Personal Data;

**(b)** Undertaking any Data Protection Impact Assessments that are required by applicable Data Protection Law and, where necessary, consulting with the relevant Supervisory Authority in respect of any such Data Protection Impact Assessments; and

**(c)** Notifications to the Supervisory Authority under Data Protection Law and/or communications to Data Subjects by Loopio in response to any Security Breach.

## 5. Subprocessors

**5.1.** Customer grants a general authorisation to Loopio to appoint its Affiliates or third parties as Subprocessors to support the performance of the Services under the Agreement.

**5.2.** A current list of Loopio's Subprocessors is available at: https://loopio.com/subprocessors/. Loopio shall provide Customer with thirty (30) days prior written notice before appointing any new Subprocessor(s). Such notice shall include the details of the Processing to be undertaken by the new Subprocessor(s).

**5.3.** If within thirty (30) days of receipt of that notice, Customer notifies Loopio of any reasonable objections to the proposed appointment, the Parties shall work together in good faith to resolve such objections. If the Parties cannot reach resolution within sixty (60) days of receipt of Customer's objection, either Party may terminate this Agreement, and Customer shall receive a prorated refund of any prepaid fees from the date of termination.

**5.4.** Loopio shall ensure its contracts with Subprocessors contain data protection terms no less protective than those set forth in this DPA. Loopio shall procure the performance by such Subprocessors in accordance with the terms herein and shall remain liable for any breach of this DPA caused by any act, error, or omission of its Subprocessors. Loopio will conduct proper due diligence on all Subprocessors to ensure each Subprocessor can comply with applicable Data Protection Law and this DPA.

## 6. Information Security, Security Breaches, and Audits

**6.1.** Loopio shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against loss, theft, destruction, damage, alteration and unauthorized or unlawful access, use, disclosure or other risks incurred by Processing in pursuit of the Services, as would allow Loopio to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services. Such measures include, without limitation, the security measures set out in Schedule 2 below.

**6.2.** Loopio shall carry out regular reviews of Schedule 2 to ensure its continuing appropriateness and shall not materially lower the standard of the Security Measures.

**6.3.** Loopio shall notify Customer of any Security Breach without undue delay and in any case within forty-eight (48) hours after becoming aware of such Security Breach. The notification will include the details, if available, of when the Security Breach occurred, when it was detected, the nature and scope of the Personal Data involved, measures taken or planned to mitigate the negative effects of the Security Breach, the name and contact details of a point of contact where more information can be obtained, and any other information available to Loopio regarding the Security

Breach. To the extent Loopio does not have the foregoing information about the Security Breach at the time of initial notification, Loopio will supplement that notification as additional information becomes available. Loopio shall not inform any third party, including Supervisory Authorities or Data Subjects, of any Security Breaches related to Personal Data under this DPA without first obtaining Customer's written consent, unless Loopio is required by applicable Data Protection Law to inform such third party.

**6.4.** Loopio shall support Customer in Customer's relevant duties under applicable Data Protection Law relating to a Security Breach, including but not limited to Loopio's obligation to assist Customer with notifications to a Supervisory Authority, other third parties and Data Subjects. Loopio will take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Breach with respect to Customer, and shall keep Customer promptly informed of all developments in connection with the Security Breach.

**6.5.** At Customer's request, Loopio shall make available all information reasonably necessary to demonstrate compliance with this DPA and applicable Data Protection Law. Loopio shall allow and cooperate with reasonable assessments, audits and inspections by Customer or a Customer designated assessor/auditory, no more than once per calendar year, or in the event of a Security Breach, or as required by a Supervisory Authority. Customer will provide at least thirty (30) days' notice to Loopio when requesting an audit, conduct its audit during regular business hours, and take reasonable measures to prevent unnecessary disruption to Loopio's day to day operations. Loopio shall promptly remediate any material deficiencies discovered through the audit.

## 7. Data Transfers

**7.1.** To the extent that in the course of providing the Services to Customer, Loopio Transfers Personal Data and Processing of Personal Data occurs outside of the UK, Switzerland, and/or the European Economic Area, Loopio will ensure any such Transfer or other processing complies with applicable Data Protection Law.

**7.2.** To the extent any Transfer or Processing of Personal Data takes place and is subject to UK Data Protection Law, GDPR, or the FADP such Transfer shall take place on the basis of the EU SCCs or UK Approved Addendum, as described in Schedule 3 of this DPA.

**7.3.** In case the Parties can no longer rely on the EU SCCs or UK Addendum as an appropriate transfer mechanism, the Parties will conclude an alternative transfer mechanism, as applicable, without undue delay.

## 8. Term and Termination

**8.1.** This DPA shall remain in force for an indefinite period, unless and until terminated in accordance with the provisions of the Agreement. The duties of this DPA shall survive the termination or end of the Agreement to the extent Loopio retains any Personal Data, or any third-party claim arises from actions occurring within the Subscription Term.

**8.2.** Upon termination of the Agreement or upon Customer's request, Loopio shall, at the choice of Customer, delete or return the Personal Data (including all copies of the Personal Data) it processes on behalf of Customer, unless Data Protection Law requires Loopio to retain the

Personal Data, in which case the Personal Data shall remain subject to this DPA and processed solely for the purpose and period required by such Data Protection Law. Loopio shall ensure the erasure or destruction of all Personal Data in the possession, custody or control of any agents, subcontractors, or Subprocessors. Loopio shall confirm the deletion or return of Personal Data without undue delay, upon Customer's written request. Notwithstanding the foregoing, if permitted by applicable Data Protection Law, Loopio may retain Personal Data stored on a backup system that is not technically feasible to immediate deletion, provided that such Personal Data is stored securely, not further processed except as required by Data Protection Law, and deleted as soon as technically feasible and in accordance with Loopio's retention policies.

## 9. General

**9.1.** This DPA is without prejudice to the rights and obligations of the Parties under the Agreement which shall continue to have full force and effect. In the event of a conflict between this DPA and the Agreement, the terms of this DPA shall control and supersede.

**9.2.** This DPA may not be amended or modified except in writing and signed by both Parties. In the event of a change in Data Protection Law, the Parties agree to negotiate in good faith to amend this DPA as is reasonable and appropriate given the change in Data Protection Law.

**9.3.** No person who is not a party to this DPA shall have any rights under the Contracts (Rights of Third Parties) Act 1999 of the United Kingdom (or any equivalent applicable EEA law) or otherwise to enforce any term of this DPA.

**9.4.** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

**9.5.** Without prejudice to Section 12 and Section 15 (m) (Incorporation of and changes to the EU SCCs) of the UK Approved Addendum, this DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Agreement and each of the parties agrees to submit to the choice of jurisdiction as stipulated.

**[SIGNATURES ON NEXT PAGE]**

**IN WITNESS WHEREOF,** the Parties have each caused this DPA to be signed and delivered by its duly authorized representative as of the Effective Date set out above.

**EXECUTED** by and on behalf of:

| **Customer.** | **Loopio Inc.** |
|---|---|
| Signature: | Signature: Signed by: Neetu Toor CDE50ABE9220416... |
| Printed Name: | Printed Name: Neetu Toor |
| Title: | Title: General Counsel |
| Date: | Date: 6/26/2025 \| 7:07 PM EDT DS |

# Schedule 1

## Details of Processing

**Part A: List of Parties**

| Role | Controller / data exporter | Processor / data importer |
|---|---|---|
| **Party** | **Customer** | **Loopio Inc.** |
| **Contact person** | **Name:**<br>**Position:**<br>**Contact details:** | **Name:** Loopio Privacy Team<br>**Position:** Data Protection Officer<br>**Contact details:** privacy@loopio.com |
| **Activities / Services provided** | **See Part B below** | **See Part B below** |

**Part B: Description of Processing**

1. **Categories of Data Subjects:**
   Employees, agents, advisors, and personnel of Customer
   Prospects, customers, business partners and suppliers of Customer
   Employees or contact persons of Customer's prospects, customers, business partners and suppliers
   Customer's users authorized by Customer to use the Services
   Other (please specify):

2. **Categories of Personal Data**
   Business contact data
   Device identification data
   Authentication credentials
   Application content (e.g. managing content in a database)
   Other (please specify)

3. **Special Categories of Data (if applicable)**
   - Not Applicable - Customer is prohibited from providing Loopio with any Special Categories of Personal Data

4. **Frequency of the Transfer**

   Data Exporter transfers Personal Data as often as necessary to adequately provide Services in the Agreement.

5. **Subject matter of the Processing**

   Loopio will Process Personal Data as necessary to provide the Services under the Agreement.

6. **Nature and purpose of the Processing**

   The Processor may Process Customer Data to the extent necessary to provide the Services to the Data Controller as more particularly described in the Agreement (including but not limited to, providing services that streamline the way organizations respond to Requests for Proposals (RFPs), Due Diligence Questionnaires (DDQs), and Security Questionnaires).

7. **Duration**

   Personal Data will be retained per the requirements of the Agreement and this DPA, and shall be as long as necessary to perform the Services. The duration of processing shall continue the later of (i) the termination of expiry of the Agreement or (ii) the termination of the last of the Services to be performed by Loopio.

8. **Subprocessors**

   As described at https://loopio.com/subprocessors/.

## Schedule 2

## Technical and Organizational Measures

These Technical and Organization Measures outline the terms and conditions regarding Loopio's information security and data protection program in compliance with applicable data protection laws.

1. **Security Measures.** Loopio will implement and maintain the following technical and organizational security measures to protect all Customer's Confidential Information, which includes Personal Data and Customer Content, against unauthorised access, loss, alteration, disclosure, or destruction.
   - 1.1. **Security Policies & Procedures.** Loopio will maintain a documented approach to information security, referred to as an Information Security Management System ("**ISMS**"). The ISMS includes a comprehensive set of policies, standards, procedures, training and other operational controls designed to implement and maintain the necessary safeguards required to protect Confidential Information in compliance with Applicable Law.
   - 1.2. **Segregation of Duties.** Loopio will ensure the segregation of conflicting duties and areas of responsibility to minimize the risk of any unauthorized or unintentional modification or misuse of Confidential Information. Where segregation is not feasible, alternative mitigating controls - such as monitoring of activities, audit trails and management supervision - will be implemented.
   - 1.3. **Background Checks.** Loopio will conduct background checks on all employees assigned to the Customer under the Agreement, as permitted by Applicable Law. These background checks will include (i) a criminal background investigation, including to identify any unpardoned criminal convictions, (ii) verification of educational credentials, and (iii) verification of employment background.
   - 1.4. **Acceptable Use of Assets.** Loopio will maintain policies governing the acceptable use of company assets that store Confidential Information.
   - 1.5. **Security Breach.** Loopio will provide Customer notice within 48 hours of a Security Breach relating to the Services that impacts Confidential Information. The Customer acknowledges that Loopio may have separate notification obligations under Applicable Law or its contractual obligations.
   - 1.6. **Intrusion Prevention.** Loopio will ensure that its security infrastructure is consistent with industry standards for malware protection, firewalls, and intrusion prevention technologies to prevent any unauthorized access or compromise of Loopio's network, systems, servers, and applications from unauthorized access.
   - 1.7. **Security Awareness Training.** Loopio will implement and maintain appropriate awareness education and training, including regular updates to organizational policies and procedures, as relevant for Loopio employees' job function, regarding the handling and

securing of Customer's Confidential Information. Security awareness and training will be conducted pursuant to and in accordance with Applicable Laws, including but not limited to the recent the Digital Operational Resilience Act (DORA).

1.8. **Physical Access Controls.** If applicable, Loopio will implement and maintain physical controls at its corporate offices to restrict access to information systems and facilities, ensuring that access is reasonably limited to authorized individuals.

1.9. **Logical Access Controls.** Loopio will restrict and monitor access to Confidential Information, granting access only to personnel whose roles require it to perform the Services, in accordance with the principles of '*Need to Know*' and '*Least Privilege*'. Loopio will implement and maintain logging and monitoring technologies to detect and prevent unauthorized access attempts to Loopio's networks and production systems. Loopio will conduct periodic reviews to assess changes affecting authentication, authorization, auditing processes, and privileged access to production systems. Upon termination of any personnel, Loopio will immediately revoke the individual's access to all Loopio systems, including but not limited to those which grant access to Confidential Information.

1.10. **Vulnerability Management.** Loopio will perform annual penetration testing of the Loopio Services. The tests are performed externally by a reputable third-party organization. Automated vulnerability scans of the Loopio Services are performed periodically to identify, mitigate and remediate any vulnerabilities.

1.11. **Information Backup.** Loopio will back up Confidential Information daily to a separate online data center. All data is encrypted using PGP keys (RSA 4096) and transmitted over HTTPS. Additionally, customer administrators can back up and export content from the Services. Administrators can set an automatic backup cycle for the library at a preferred frequency or perform manual backups at any time.

1.12. **Encryption.** In accordance with its Encryption Management Policy, Loopio will use strong encryption measures to encrypt Confidential Information while at-rest within Loopio data processing facilities and while in-transit across public networks.

1.13. **Business Continuity & Disaster Recovery.** Loopio will maintain a business continuity plan (BCP) and disaster recovery plan (DRP) in accordance with industry best standards. Each plan is tested at least annually. The adequacy of Loopio's BCP and DRP documentation and procedures is reviewed and validated by independent third-party auditors as part of Loopio's SOC 2 Audit and ISO 27001-9001 certifications.

1.14. **Audit Standards.** Loopio will periodically evaluate its administrative, technical and physical safeguards for Confidential Information. At least annually, Loopio conducts comprehensive assessments to ensure compliance with (i) Standards for Reporting on Controls at a Service Organization (SOC 2) published by the American Institute of CPAs

(AICPA), (ii) ISO 27001 and (iii) ISO 9001. A copy of Loopio's most recent SOC 2 Report is available upon Customer's request.

**1.15.** **Third-Party Vendor Management**. All third-party vendors engaged by Loopio to handle Confidential Information undergo a comprehensive Vendor Request Assessment. Vendor assessments include but are not limited to (i) assessing the scope of vendor's data processing activities, (ii) assessing vendor's information security program and ensuring vendor is audited against applicable standards (e.g. SOC2, ISO 27001), and (iii) assessing the vendor's terms and conditions ensuring compliance with all applicable data protection standards and legal requirements.

## Schedule 3

## Cross Border Data Transfer Mechanisms

1. Subject to Sections 2 and 3 below, the Parties agree that the Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from a Member State, the UK or Switzerland, either directly or via onward transfer, to any country or recipient outside of a Member State, the UK or Switzerland that is not an Adequate Jurisdiction. The Standard Contractual Clauses will apply to Customer and, to the extent legally required, all of Customer's Affiliates established within a Member State, the UK and/or Switzerland, in their role as Controllers and these entities will be deemed "data exporters". For Personal Data transfers from a Member State, the UK or Switzerland that are subject to the Standard Contractual Clauses, the Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

    a. The Module 2 terms apply to the extent that Customer is a Controller;

    b. In clause 7, the optional docking clause will not apply;

    c. In clause 8.9, any audits will be carried out in accordance with Section 6.5 of this DPA;

    d. In clause 9, Option 2 (*General written authorization*) will apply and the time period for prior notice of subprocessor changes will be as set forth in Section 5 of this DPA;

    e. In clause 11, the optional language will not apply;

    f. In clause 17 (Option 1), the Standard Contractual Clauses will be governed by the laws of the Republic of Ireland;

    g. In clause 18(b), disputes will be resolved before the courts of the Republic of Ireland;

    h. Annex I.A will be deemed to incorporate the information in Schedule 1 Part A (Details of Processing);

    i. Annex I.B (*Description of Transfer*) will be deemed to incorporate the information in Schedule 1 Part B (Details of Processing);

    j. Annex I.C (*Competent Supervisory Authority*) will be deemed to refer to the Irish Data Protection Authority;

    k. Annex II (*Technical and Organizational Measures*) will be deemed to incorporate the information in Schedule 2 (Technical and Organizational Measures).

2. With respect to any transfers of Personal Data falling within the scope of the UK GDPR from Customer (as data exporter) to Loopio (as data importer):

    a. Neither the Standard Contractual Clauses nor the DPA will be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the

Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018;

**b.** The Standard Contractual Clauses are deemed to be amended to the extent necessary so they operate: (i) for transfers made by the Controller to the Processor, to the extent that UK Data Protection Laws apply to the Controller's Processing when making that transfer; and (ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the UK GDPR;

**c.** The amendments referred to in Section 2(b) above include (without limitation) the following:

**i.** References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK GDPR" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article of the UK GDPR;

**ii.** References to Regulation (EU) 2018/1725 are removed;

**iii.** References to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

**iv.** The "competent supervisory authority" will be the Information Commissioner;

**v.** clause 17 of the Standard Contractual Clauses is replaced with the following: "*These Clauses are governed by the laws of England and Wales*";

**vi.** Clause 18 of the Standard Contractual Clauses is replaced with the following:

"*Any dispute arising from these Clauses will be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts*";

**vii.** Any footnotes to the Standard Contractual Clauses are deleted in their entirety.

**3.** With respect to any transfers of Personal Data falling within the scope of the Swiss Federal Act on Data Protection from Loopio (as data exporter) to Loopio (as data importer):

**a.** Neither the Standard Contractual Clauses nor the DPA will be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in Switzerland, including the Swiss Federal Act on Data Protection ("Swiss Data Protection Laws");

**b.** The Standard Contractual Clauses are deemed to be amended to the extent necessary so they operate: (i) for transfers made by the Controller to the Processor, to the extent that Swiss Data Protection Laws apply to the Controller's Processing when making that transfer; and (ii) to provide appropriate safeguards for such transfers;

**c.** The amendments referred to in Section 3(b) above include (without limitation) the following:

**i.** References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "Swiss Data Protection Laws";

**ii.** References to Regulation (EU) 2018/1725 are removed;

**iii.** References to the "Union", "EU" and "EU Member State" are all replaced with the "Switzerland";

**iv.** The "competent supervisory authority" will be the Swiss Federal Data Protection and Information Commissioner;

**v.** Clause 17 of the Standard Contractual Clauses is replaced with the following: "*These Clauses are governed by the laws of Switzerland*";

**vi.** Clause 18 of the Standard Contractual Clauses is replaced with the following:

"*Any dispute arising from these Clauses will 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 any country in Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts*";

**vii.** Any footnotes to the Standard Contractual Clauses are deleted in their entirety.

**4.** Without prejudice to the generality of clause 5 of the Standard Contractual Clauses, in the event of any conflict between the Agreement, this DPA and the Standard Contractual Clauses, the following order of precedence will apply: (1) the Standard Contractual Clauses (or, with respect to transfers of Personal Data subject to the UK GDPR or Swiss Data Protection Laws, the Standard Contractual Clauses as amended by Section 2(c) above and Section 3(c) above respectively); (2) the main body of this DPA; the Agreement.