INSTRUCTIONS ON HOW TO EXECUTE THIS DPA IF YOU ARE AN EU CUSTOMER:

1.   This DPA is to be entered into ONLY with EU customers or customers processing personal data of data subjects in the EU.

2.   To complete this DPA, Customer must:
   a. Confirm the email address of clause 10.2.
   b. Complete the information in the signature box and sign on page 9.
   c. Send the signed DPA to Viral Loops at privacy@viral-loops.com using the email address of clause 10.2 within 15 days from their registration to Viral Loops.
   d. Receive the DPA countersigned from Viral Loops

Customer EU Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the Agreement between Viral Loops Technologies Inc. ("**Viral Loops**") and **Customer** for the purchase of referral marketing software and services from Viral Loops (each a "**Party**", collectively the "**Parties**") and shall be effective on the date both parties execute this DPA ("**Effective Date**").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

PREAMBLE

A.   The Parties have entered into an Agreement in relation to the provision of referral marketing software and services by Viral Loops to Customer, in the course of which Viral Loops will be processing Customer Personal Data subject to the General Data Protection Regulation (EU) 2016/ 679 ("GDPR") on behalf of the Customer.

B.   The Parties wish to supplement the terms of the Agreement to ensure that the processing of Personal Data by Viral Loops in connection with the Agreement is pursued in compliance with applicable Data Protection Laws.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**Agreement**" means Viral Loops' [Terms of Service](#), which govern the provision of the Services to Customer, as such terms may be updated by Viral Loops from time to time and any other specific arrangements in place between the parties.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" shall be construed accordingly.

"**Customer Data**" means any Participants' Personal Data that Viral Loops processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"**Group**" means any and all Affiliates that are part of an entity's corporate group.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

"**Services**" means any product or service provided by Viral Loops to Customer pursuant to the Agreement.

"**Sub-processor**" means any Data Processor engaged by Viral Loops or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this   DPA. Sub-processors may include third parties or members of the Viral Loops Group.

Any capitalized terms not otherwise defined in this DPA that have meanings ascribed to them in the applicable Data Protection law shall carry the meanings set forth under applicable Data Protection Laws.

2. Relationship with the Agreement

2.1. This DPA constitutes the entire agreement between the Parties with respect to the subject of this DPA. The Parties agree that DPA shall replace any existing DPA the Parties may have previously entered into in connection with the Services.

2.2. A determination that any provision of this DPA is invalid or unenforceable shall not affect the other provisions of the present.

2.3. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.4. Any claims brought under or in connection with this DPA shall be subject to the Terms of Service, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.5. Any claims against Viral Loops or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. Customer further agrees that, to the extent permitted under applicable law, any regulatory fines incurred by Viral Loops in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Viral Loops' liability under the Agreement as if it were liability to the Customer under the Agreement.

2.6. No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

2.7. This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Law.

2.8. By entering into this DPA you represent and warrant that you are duly authorized and have the legal capacity to execute and deliver this DPA.

2.9. It is the responsibility of the Customer to sign and enter into this DPA. This DPA shall only become legally binding between Customer and Viral Loops when the formalities steps set out in the instructions above have been fully completed, with the responsibility of the Customer.

3. Scope and Applicability of this DPA

3.1. This DPA applies where and only to the extent that Viral Loops processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

4. Roles and Scope of Processing

4.1. **Role of the Parties**. As between Viral Loops and Customer, Customer is the Data Controller of Customer Data, and Viral Loops shall process Customer Data as a Data Processor acting on behalf of Customer.

4.2. **Customer Processing of Customer Data**. Customer determines the scope, purposes and manner by which the Personal Data may be accessed or processed by Viral Loops. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Viral Loops; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Viral Loops to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

4.3. **Viral Loops Processing of Customer Data**. Viral Loops shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions, unless required to do so by applicable law to which Viral Loops is subject, in which case Viral Loops shall (to the extent permitted) inform Customer of that legal requirement before the Processing of that Personal Data. Viral Loops shall immediately notify the Customer if, in its opinion, any instruction infringes the applicable Data Protection Laws. Such notification will not constitute a general obligation on the part of Viral Loops to monitor or interpret the laws applicable to Customer, and such notification will not constitute legal advice to the Customer. Viral Loops shall be allowed to exercise its own discretion in the selection and use of means of Processing, as it considers necessary to pursue those purposes, provided that all such discretion is compatible with the requirements of this DPA, in particular the Customer's written instructions.

5. Details of Data Processing

5.1. The Parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to Viral Loops in relation to the processing of Customer Data and Processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Viral Loops.

5.2**. Duration**: As between Viral Loops and Customer, the duration of the Data Processing under this DPA is until the termination of the Agreement in accordance with its terms.

5.3. **Subject matter & Nature of the processing**: Viral Loops provides an email service, automation and marketing platform and other related services, as described in the Agreement, in the course of which it collects, uses and stores Customer Data.

5.4. **Categories of data subjects**: Any individual: (i) whose email address is included in the Customer's Distribution List; (ii) whose information is stored on or collected via the Services, or (iii) to whom Users send emails or otherwise engage or communicate with via the Services (collectively, "Participants").

5.5. **Types of Customer Data:**

Participants: e-mail and any type of data requested by the Customer.

5.6. **Purpose:** The purpose of the Data Processing under this DPA is the provision of the Services to the Customer and the performance of Viral Loops' obligations under the Agreement (including this DPA) or as otherwise agreed by the Parties.

In particular, notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Viral Loops shall process Customer Data relating to the operation, support and/or use of the Service, to the extent necessary, for its legitimate business purposes, including:

● To provide, support and improve the Services. For example, this may include sharing your information with third parties in order to support our Services or to make certain features of the Services available to our Users.

● To enforce compliance with our Terms of Service and applicable law. This may include developing tools and algorithms that help us prevent violations.

● To protect the rights and safety of our Users and third parties, as well as our own. For example, sometimes we review the content of our Users' campaigns to make sure they comply with our Terms of Use. Our employees or independent contractors may review those particular campaigns, which may include your participant information. This reduces the amount of spam being sent through our servers and fraudulent behaviour.

● To meet legal requirements, including complying with court orders, valid discovery requests, valid subpoenas, and other appropriate legal mechanisms.

● To provide information to representatives and advisors, including attorneys and accountants, to help us comply with legal, accounting, or security requirements.

● To prosecute and defend a court, arbitration, or similar legal proceeding.

● To respond to lawful requests by public authorities, including to meet national security or law enforcement requirements.

To the extent any such data is considered Personal Data under Data Protection Laws, Viral Loops shall process such data in accordance with the Viral Loops Privacy Policy and Data Protection Laws.

5.7. **Tracking Technologies**. Customer acknowledges that in connection with the performance of the Services, Viral Loops employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Customer shall maintain appropriate notice, consent, opt-in and

opt-out mechanisms as are required by Data Protection Laws to enable Viral Loops to deploy Tracking Technologies lawfully on, and collect data from, the devices of Participants (defined below) in accordance with and as described in the Viral Loops Cookie Statement.

6. Subprocessing

6.1. **Authorized Sub-processors.** Customer hereby grants Viral Loops general written authorisation for the engagement of any Subprocessors.

The Sub-processors currently engaged by Viral Loops and authorized by Customer are listed in Annex A. Viral Loops shall inform Customer in the manner it considers appropriate of any intended changes concerning the addition or replacement of Subprocessors at least ten (10) days in advance. Customer may object in writing to Viral Loops' appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the Parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

6.2. **Sub-processor Obligations.** Viral Loops shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Viral Loops to breach any of its obligations under this DPA.

7.   Security

7.1.   **Security Measures**. Viral Loops shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data. The Security Measures implemented by Viral Loops are listed in Annex B of this DPA.

7.2.   **Updates to Security Measures**. Customer acknowledges that measures implemented by Viral Loops relating to data security meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Viral Loops may update or modify the Security Measures from time to time at its discretion, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer. Where material changes are requested by Customer or required to the security requirements set forth in EU Data Protection Laws or by data protection authorities of competent jurisdiction, the Parties will negotiate in good faith the allocation of the additional cost between them, if any.

7.3. **Customer Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

8.   **Security Reports and Audits**

8.1. Viral Loops shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires, that are necessary to confirm Viral Loops' compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

8.2. Where responses to such requests for information are insufficient, Viral Loops allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, upon at least 30 days' notice, granting the Customer reasonable access to premises and systems which are directly related with the Processing of the Personal Data and are reasonably required to verify Viral Loops' compliance with the DPA.

9.   **International Transfers**

9.1. **Data center locations**. Customer hereby agrees that Viral Loops may transfer and process Customer Data anywhere in the world where Viral Loops, its Affiliates or its Sub-processors maintain data processing operations, without prior explicit authorization from Customer. Viral Loops shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

9.2. **Transfer Mechanism**. To the extent that Viral Loops processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the Parties acknowledge that Viral Loops shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data, by using any appropriate alternative transfer mechanisms set forth by the GDPR.

10.   **Additional Security**

10.1. **Confidentiality of processing.** Viral Loops shall ensure that any person who is authorized by Viral Loops to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

10.2. **Notifications**. Viral Loops shall notify Customer at the email address provided in the Registration Information without undue delay, in any case within 48 hours of any actual or suspected Personal Data Breach involving Customer's Personal Data. Customer authorizes Viral Loops to take all reasonable remedial measures as required to mitigate any Personal Data Breach.

10.3. **Demonstration of Compliance**. Viral Loops shall make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and in Article 28 of the GDPR. Viral Loops' adherence to either an approved code of conduct or to an approved certification mechanism recognized under EU Data Protection Laws may be used as an element by which Viral Loops may demonstrate such compliance.

10.4. **Data Subject Requests**. Viral Loops shall assist Customer by appropriate Technical and Organizational Measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to requests for exercising Data Subjects' rights according to the conditions of Articles 15-22 of the GDPR.

In addition, with regard to data subject rights, the Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Viral Loops shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Viral Loops, Viral Loops shall have the right to respond to such communication directly without Customer's prior authorization.

10.5. **Assistance.** Viral Loops shall provide all cooperation and assistance to Customer, at customer's expense, as may be reasonably required, to allow Customer to comply with its obligations under Data Protection Laws, including in relation to data security, data breach notifications, data protection impact assessments, prior consultation with Supervisory Authorities.

If a law enforcement agency sends Viral Loops a demand for Customer Data (for example, through a subpoena or court order), Viral Loops shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Viral Loops may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Viral Loops shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Viral Loops is legally prohibited from doing so.

11. Return or Deletion of Data

11.1. Upon termination or expiration of the Agreement, Viral Loops shall delete all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Viral

Loops is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Viral Loops shall securely isolate and protect from any further processing, except to the extent required by applicable law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative(s):

For and on behalf of Viral Loops Technologies Inc.

Signature:

Name of legal representative: Dimitrios Tzortzis

Title of legal representative: General Manager

Date:

For and on behalf of Customer

Signature:

Legal Name:

Full Name and title of legal representative:

Date:

Annex A - List of Viral Loops Sub-processors

Viral Loops uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors set out below provide cloud hosting and storage services; content delivery and review services; assist in providing customer support; as well as incident tracking, response, diagnosis and resolution services.

- Amazon
- Heroku
- Kickbox
- Mailchimp
- Papertrail
- Rollbar

ANNEX B - Technical and Organisational Measures

Application Level Security

- Viral Loops account passwords are hashed and even our own engineers can't view them. If you lose your password, it can't be retrieved—it can only be reset.
- The entire Viral Loops application is encrypted with TLS, including data transmission.
- Login pages have brute force protection.
- We use rate limiting and services from Cloudflare to protect the Viral Loops app and API from abuse and DDoS attacks.
- We run a Bug Bounty Program so that skilled researchers from around the world can help us identify potential security weaknesses which can then be addressed by our Product Team or by the application of a new policy.

Information Security

- We have implemented a Data Retention Policy to ensure that unnecessary data is deleted from our systems and databases regularly.
- All team members are required to sign a confidentiality agreement before getting hired.
- Access to our infrastructure (including databases) is allowed only to skilled engineers required to support and maintain these systems.
- We sign Data Processing Agreements with all our sub-processors to ensure their processing of data is in accordance with our own standards and relevant regulation.
- We retain a law firm in the EU to consult on EU privacy issues and improve our policies and practices.

Data Storage & Processing

- For our data storage we use Amazon Web Services infrastructure, on the eu-west-1 data centers. AWS employs world-leading cloud security practices. You can find out more about security on AWS [here](#).
- We use Heroku for our servers on the Europe region. Heroku employs best practices for the security of their infrastructure. You can find out more about security on Heroku [here](#).