EU Data Processing Addendum

This Data Processing Addendum ("DPA") between Peaberry Software Inc. ("Customer.io") and Company forms part of the Agreement and is effective as of the Effective Date.

1. Definitions

All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement. Terms used but not defined in this DPA, such as “controller,” “data subject,” “personal data,” “processing,” and “processor” will have the same meaning as set forth in the EU Data Protection Law.

"Affiliate" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity.

"Agreement" means Customer.io’s Terms of Service, which govern the provision of the Services to Company.

"Company Data" means any personal data that Customer.io processes on behalf of Company as a 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.

"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of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).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 the European Economic Area, United Kingdom and Switzerland.

"Privacy Shield" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"Privacy Shield Principles" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"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 Company Data.

"Services" means any product or service provided by Customer.io to Company pursuant to the Agreement.

“Subprocessors” means the other processors that are used by Customer.io to process Personal Data.

2. Relationship with the Agreement

2.1 The parties agree that the DPA shall replace any existing data processing addendum the parties may have previously entered into in connection with the Services.

2.2 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.

2.3 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.4 Company further agrees that any regulatory penalties incurred by Customer.io in relation to the Company Data that arise as a result of, or in connection with, Company's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Customer.io's liability under the Agreement as if it were liability to the Company under the Agreement.

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

2.6 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 Laws.

3. Scope and Applicability of this DPA

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

Part A: General Data Protection Obligations

4. Roles and Scope of Processing

4.1 Role of the Parties. As between Customer.io and Company, Company is controller of Company Data, and Customer.io shall process Company Data only as a processor acting on behalf of Company.

4.2 Company Processing of Company Data. Company agrees that (i) it shall comply with its obligations as a controller under Data Protection Laws in respect of its processing of Company Data and any processing instructions it issues to Customer.io; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Customer.io to process Company Data and provide the Services pursuant to the Agreement and this DPA.

4.3 Customer.io Processing of Company Data. Customer.io shall process Company Data only for the purposes described in this DPA and only in accordance with Company's documented, lawful instructions. The parties agree that this DPA and the Agreement set out the Company's complete and final instructions to Customer.io in relation to the processing of Company Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Company and Customer.io.

4.4 Details of Data Processing

(a) Subject matter: The subject matter of the data processing under this DPA is the Company Data.

(b) Duration: As between Customer.io and Company, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Company and the performance of Customer.io's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: Customer.io provides email messaging, analytics technology and other related services, as described in the Agreement.

(e) Categories of data subjects: Any individual accessing and/or using the Services through the Company's account ("Users"); and any individual: (i) whose email address is included in the Company'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, "End Users").

(f) Types of Company Data:

(i) Company and Users: identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);

(ii) End Users: identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address), personal interests or preferences (including purchase history, marketing preferences and publically available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

4.5 Company acknowledges that Customer.io shall have a right to use and disclose data relating to the operation, support and use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered personal data under Data Protection Laws, Customer.io is the controller of such data and accordingly shall process such data in accordance with the Customer.io Privacy Policy and Data Protection Laws.

4.6 Tracking Technologies. Company acknowledges that in connection with the performance of the Services, Customer.io employs the use of cookies, unique identifiers, web beacons and similar tracking technologies ("Tracking Technologies"). Company shall maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable Customer.io to deploy Tracking Technologies lawfully on, and collect data from, the devices of End Users (defined below) in accordance with and as described in the Customer.io Cookie Statement.

5. Subprocessing

5.1 Authorized Subprocessors. Company agrees that Customer.io may engage Subprocessors to process Company Data on Company's behalf. The Subprocessors currently engaged by Customer.io and authorized by Company are listed in Attachment A.

5.2 Subprocessor Obligations. Customer.io shall: (i) enter into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Company 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 Subprocessor that cause Customer.io to breach any of its obligations under this DPA.

6. Security

6.1 Security Measures. Customer.io shall implement and maintain appropriate technical and organizational security measures to protect Company Data from Security Incidents and to preserve the security and confidentiality of the Company Data, in accordance with Customer.io's security standards described in this DPA and at https://customer.io/security ("Security Measures").

6.2 Updates to Security Measures. Company is responsible for reviewing the information made available by Customer.io relating to data security and making an independent determination as to whether the Services meet Company's requirements and legal obligations under Data Protection Laws. Company acknowledges that the Security Measures are subject to technical progress and development and that Customer.io may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Company.

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

7. Compliance Verification

7.1 Upon reasonable request, Customer.io will verify its compliance with this DPA, provided that Company shall not exercise this right more than once per year.

8. International Transfers

8.1 Data center locations. Customer.io may transfer and process Company Data anywhere in the world where Customer.io, its Affiliates or its Subprocessors maintain data processing operations. Customer.io shall at all times provide an adequate level of protection for the Company Data collected, transferred, processed, or retained in accordance with the requirements of Data Protection Laws.

8.2 Privacy Shield. To the extent that Customer.io processes any Company Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, to the United States, 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 Customer.io shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Company Data by virtue of having self-certified its compliance with Privacy Shield. Customer.io agrees to protect such personal data in accordance with the requirements of the Privacy Shield Principles. If Customer.io is unable to comply with this requirement, Customer.io shall inform Company.

8.3 Alternative Transfer Mechanism. The parties agree that the data export solution identified in Section 8.2 shall not apply if and to the extent that Customer.io adopts an alternative data export solution with Company for the lawful transfer of personal data (as recognized under EU Data Protection Laws) outside of the EEA ("Alternative Transfer Mechanism"), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which personal data is transferred).

Part B: GDPR Obligations from 25 May 2018

9. Additional Security

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

9.2 Security Incident Response. Upon becoming aware of a Security Incident, Customer.io shall notify Company without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Company.

10. Changes to DPA and Subprocessors.

10.1 Changes to DPA. Customer.io may be required to update this DPA in order to comply with applicable law, and in such case Customer.io will provide reasonable notice of any such updates.

10.1 Changes to Subprocessors. Customer.io shall (i) provide an up-to-date list of the Subprocessors it has appointed upon written request from Company; and (ii) notify Company (for which email shall suffice) if it adds Subprocessors at least 10 days prior to any such changes. Company may object in writing to Customer.io's appointment of a new Subprocessor 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, Company may suspend or terminate the Agreement (without prejudice to any fees incurred by Company prior to suspension or termination).

11. Return or Deletion of Data

11.1 Upon termination or expiration of the Agreement, Customer.io shall (at Company's election) delete (after providing Company the ability to download, pursuant to the Agreement) all Company Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Customer.io is required by applicable law to retain some or all of the Company Data, which Company Data Customer.io shall securely isolate and protect from any further processing, except to the extent required by applicable law.

12. Cooperation

12.1 The Services provide Company with a number of controls that Company may use to retrieve, correct, delete or restrict Company Data, which Company 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 Company is unable to independently access the relevant Company Data within the Services, Customer.io shall (at Company's expense) provide reasonable cooperation to assist Company 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 Customer.io, Customer.io shall not respond to such communication directly without Company's prior

authorization, unless legally compelled to do so. If Customer.io is required to respond to such a request, Customer.io shall promptly notify Company and provide it with a copy of the request unless legally prohibited from doing so.

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

12.3 To the extent Customer.io is required under EU Data Protection Law, Customer.io shall (at Company's expense) provide reasonably requested information regarding the Services to enable the Company to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

Attachment A

List of Customer.io Subprocessors

The list of Subprocessors available at https://customer.io/legal/sub-processors/ 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.