Customer.io Data Processing Addendum

1. Relationship with the Agreement

1.1. This Data Processing Addendum (this "DPA") is part of the Agreement between Company (defined in the signature block below) and Customer.io, Inc. ("Customer.io"). Customer.io and Company are individually a "party" and, collectively, the "parties."

1.2. This DPA applies only to the extent that Customer.io receives, stores, or Processes Personal Data in connection with the Services. Schedule 1 describes the Processing activities in-scope of this DPA.

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

1.4. 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 will prevail to the extent of that conflict.

1.5. Any claims brought under or in connection with this DPA will be subject to the Agreement.

1.6. No one other than a party to this DPA, its successors and permitted assignees will have any right to enforce any of its terms (except to the extent that individuals are able to enforce their rights through an International Data Transfer Mechanism).

1.7. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by an International Data Transfer Mechanism or applicable Data Protection Laws.

1.8. In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the parties use an International Data Transfer Mechanism and there is a conflict between the obligations in that International Data Transfer Mechanism and this DPA, the International Data Transfer Mechanism will control.

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

2. Definitions

2.1. The following terms have the meanings set forth below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

2.2. The following terms have the definitions given to them in the CCPA: "Business," "Sale," "Service Provider," and "Third Party."

2.3. "Agreement" means the agreement(s) entered into between the parties, which govern the provision of the Services to Company.

2.4. "Company Data" means any Personal Data that Customer.io Processes on behalf of Company as a Processor in the course of providing Services.

2.5. "Consent" means a Data Subject's freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

2.6. "Controller" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Business" or "Third Party," as context requires.

2.7. "Data Protection Law" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including European Data Protection Law, and U.S. Data Protection Law.

2.8. "Data Subject" means an identified or identifiable natural person.

2.9. "De-identified Data" means a data set that does not contain any Personal Data. Aggregated data is De-identified Data. To "De-identify" means to create De-identified Data from Personal Data.

2.10. "EEA" means the European Economic Area.

2.11. "European Data Protection Law" means: (i) 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) ("EU GDPR"); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("UK Data Protection Law"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Act on Data Protection and its implementing regulations ("Swiss GDPR"), in each case as may be amended, superseded or replaced from time to time.

2.12. "Personal Data" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. "Personal Data" includes equivalent terms in Data Protection Law, such as the CCPA-defined term "Personal Information," as context requires.

2.13. "Personal Data Breach" means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Data. For the avoidance of doubt, "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of Company Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

2.14. "Process" or "Processing" any operation or set of operations that a party performs on Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2.15. "Processor" means an entity that processes Personal Data on behalf of another entity. "Processor" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Service Provider," as context requires.

2.16. "Sensitive Data" means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information

governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.

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

2.18. "Standard Contractual Clauses" means, as applicable (a) the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021; or (b) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 ("UK Addendum").

2.19. "Subprocessor" means a Processor engaged by a party who is acting as a Processor.

2.20. "U.S. Data Protection Law" means all state laws in effect in the United States of America that are applicable to the processing of personal data under this DPA, including, but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

3. Description of the Parties' Personal Data Processing Activities and Statuses of the Parties

3.1. Schedule 1 describes the purposes of the parties' Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.

3.2. Schedule 1 lists the parties' statuses under relevant Data Protection Law.

4. International Data Transfer

4.1. Some jurisdictions require that an entity transferring Personal Data to, or accessing Personal Data from, a foreign jurisdiction take extra measures to ensure that the Personal Data has special protections (an "International Data Transfer Mechanism"). The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law, including the Standard Contractual Clauses. Before either party transfers to the other party or permits the other party to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, the transferring party will notify the other party of the relevant requirement and the parties will work together in good faith to fulfill the requirements of that International Data Transfer Mechanism.

4.2. If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find a suitable alternative.

4.3. With respect to Personal Data of Data Subjects located in the EEA, Switzerland, or the United Kingdom that Company transfers to Customer.io or permits Customer.io to access, the parties agree that by executing this DPA they also execute the Standard Contractual Clauses, which will be incorporated by reference and form an integral part of this DPA. The parties agree that,

with respect to the elements of the Standard Contractual Clauses that require the parties' input, Schedules 1 and 2 contain the relevant information.

5. Data Protection Generally

5.1. Compliance. The parties will comply with their respective obligations under Data Protection Law and their privacy notices. Specifically, with respect to U.S. Data Protection Law, where Customer.io is a Service Provider, Customer.io agrees that it will not:

5.1.1. retain, use, disclose or otherwise process Company Data other than for the limited and specified purposes identified in this DPA or the Agreement;

5.1.2. retain, use, disclose or otherwise process such Company Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, or as otherwise permitted under U.S. Data Protection Law;

5.1.3. "sell" or "share" such Company Data within the meaning of the U.S. Data Protection Law; and

5.1.4. retain, use, disclose or otherwise process such Company Data outside the direct business relationship with Company and not combine such Company Data with personal information that it receives from other sources, except as permitted under U.S. Data Protection Law.

5.2. Company Processing of Personal Data. Company represents and warrants that it has the Consent or other lawful basis necessary to collect and disclose Personal Data to Customer.io in connection with the Services.

5.3. Cooperation.

5.3.1. Data Subject Requests.

5.3.1.1. *Facilitation of Responses*. 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 Data Protection Law, including its obligations relating to responding to requests from individuals or applicable data protection authorities. To the extent that Company is unable to independently access the relevant Company Data within the Services, Customer.io will (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 Company Data under the Agreement.

5.3.1.2. *Requests Received by Customer.io*. Should Customer.io receive any requests from individuals to exercise their rights, Customer.io will notify the individual of the need to submit the request directly to Company, and will promptly notify Company of the request, unless Customer.io is legally prohibited from providing such notification.

5.3.2. Governmental and Investigatory Requests. If a governmental authority (e.g., the Federal Trade Commission, the Attorney General of a U.S. state, or a European data protection authority) sends Customer.io a demand for Company Data (for example, through a subpoena or court order), Customer.io will 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 governmental authority. If compelled to disclose Company Data to a governmental authority, then Customer.io will 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.

5.3.3. Other Requirements of Data Protection Law. Upon request, the parties will provide relevant information to each other to fulfill their respective obligations (if any) to conduct data protection impact assessments or prior consultations with data protection authorities.

5.4. Confidentiality. The parties will ensure that their employees, independent contractors, and agents are subject to an obligation to keep Personal Data confidential.

5.5. 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 will 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 in accordance with and as described in the Customer.io Cookie Statement.

6. Data Security

6.1. Security Controls. Customer.io will implement and maintain appropriate technical and organizational security measures to protect Company Data from Personal Data Breaches 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. Customer.io's Obligations as a Processor or Subprocessor

7.1. Customer.io will have the obligations set forth in this Section 7 if it Processes Personal Data in its capacity as Company's Processor; for clarity, these obligations do not apply to Customer.io in its capacity as a Controller, Business, or Third Party.

7.2. Scope of Processing. Customer.io will Process Company Data only for the purposes described in this DPA and only in accordance with Company's documented, lawful instructions (as set forth in this DPA, the Agreement, or as otherwise directed by Company or its Authorized Users, including through the Services). Customer.io is prohibited from: (i) Selling Company Data; (ii) retaining, using, or disclosing Company Data for any purpose other than for the specific purpose of performing the Services specified in the Agreement, including retaining, using, or disclosing the Company Data for a commercial purpose other than providing the Services specified in the Agreement; or (iii) retaining, using, or disclosing the Company Data outside of the direct business relationship between Company and Customer.io. Customer.io will promptly inform Company if following Company's instructions would result in a violation of Data Protection Law or where Customer.io must disclose Company Data in response to a legal obligation, unless the legal obligation prohibits Customer.io from making such disclosure. Notwithstanding anything to the contrary in this Section 7.2, Customer.io may Process Company Data as necessary to detect data security incidents or protect against fraudulent or illegal activity and to build or improve the quality of its products and services, provided that in the course of these activities Customer.io will not (i) permit any third party (other than Customer.io's subprocessors or except as instructed by Company) to access Company Data, or (ii) use the Company Data to modify or add to Personal Information it collected from a source that is not Company. **By signing this DPA, Customer.io certifies that it understands and will comply with the obligations herein.**

7.3. Data Subjects' Requests to Exercise Rights. Customer.io will promptly inform Company if Customer.io receives a request from a Data Subject to exercise their rights with respect to their Personal Data under applicable Data Protection Law. Company will be responsible for responding to such requests. Customer.io will not respond to such Data Subjects except to acknowledge their requests. Customer.io will provide Company with commercially reasonable assistance, upon request, to help Company to respond to a Data Subject's request.

7.4. Customer.io's Subprocessors**.**

7.4.1. Existing Subprocessors. Company agrees that Customer.io may use the Subprocessors listed at Schedule 1.

7.4.2. Use of Subprocessors. Company grants Customer.io general authorization to engage Subprocessors if Customer.io and those Subprocessors enter into an agreement that requires the Subprocessor to meet obligations that are no less protective than this DPA.

7.4.3. Notification of Additions or Changes to Subprocessors. Customer.io will (i) provide an up-to-date list of the Subprocessors it has appointed upon written request from Company at https://Customer.io/legal/sub-Processors/; and (ii) notify Company (for which email will suffice) if it adds or changes Subprocessors at least ten (10) calendar days prior to any such changes. Company may object in writing to Customer.io's appointment of a new or changed 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 will 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).

7.4.4. Liability for Subprocessors. Customer.io will be liable for the acts or omissions of its Subprocessors to the same extent as Customer.io would be liable if performing the services of the Subprocessor directly under the DPA, except as otherwise set forth in the Agreement.

7.5. Personal Data Breach. Customer.io will notify Company without undue delay, but in any event within the time frame required by applicable Data Protection Law, of a Personal Data Breach affecting Personal Data Customer.io Processes in connection with the Services. Upon request, Customer.io will provide information to Company about the Personal Data Breach to the extent necessary for Company to fulfill any obligations it has to investigate or notify authorities, except that Customer.io reserves the right to redact information that is confidential or competitively sensitive. Company agrees that email notification of a Personal Data Breach is sufficient and Company will notify Customer.io if it changes its contact information. Company agrees that Customer.io may not notify Company of security-related events that do not result in a Personal Data Breach or affect Personal Data Customer.io Processes in connection with the Services.

7.6. Deletion and Return of Personal Data. Upon termination or expiration of the Agreement, Customer.io will (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 will 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 will securely isolate and protect from any further Processing, except to the extent required by applicable law.

7.7. Compliance Verification. Upon reasonable request, Customer.io will verify its compliance with this DPA by providing summary copies of independent audit reports or such other written responses to requests for information. Only to the extent Company cannot reasonably satisfy Customer.io's compliance with this DPA through the exercise of its rights under this Section 7.7, or where required by applicable Data Protection Law or a regulatory authority, Company, or its authorized representatives, may conduct audits (including inspections) during the term of the Agreement to assess Customer.io's compliance with the terms of this DPA. Any audit must (i) be conducted during Customer.io's regular business hours, with reasonable advance notice of at least 45 calendar days; (ii) be subject to reasonable confidentiality controls; (iii) occur no more than once annually; (iv) restrict its findings to only data and information relevant to Company; and (v) obligate Company, to the extent permitted by law or regulation, to keep confidential any information disclosed that, by its nature, should be confidential.

Schedule 1: Description of the Processing and Subprocessors

Processing Activity	Status of the Parties	Categories of Personal Data Processed	Categories of Sensitive Data Processed	Applicable SCCs Module
Company discloses Personal Data to Customer.io in connection with the Services.	Company is a Controller. Customer.io is a Processor.	Any Personal Data Company discloses to Customer.io.	None	Module 2 Module 3, if Company acts as a Processor to another Controller.
Customer.io provides Tracking Technologies for Company's use.	Customer.io is a Controller. Company is a Controller.	Device and browser identifiers (e.g., IP address, MAC address, identifiers stored in cookies) and information connected to such identifiers	None	Module 2 Module 3, if Company acts as a Processor to another Controller.
Customer.io provides professional services to Company.	Customer.io is a Controller. Company is a Controller.	Name, email address, user ID.	None	Module 1
Customer.io creates account information for Company's end-users and collects usage information from them.	Customer.io is a Controller. Company is a Controller.	User ID. Usage/telemetry data about the end-user's device, e.g., device and browser identifiers (e.g., IP address, MAC address, identifiers stored in cookies) and information connected to such identifiers	None	Module 1
Company contacts Customer.io for support.	Company is a Controller. Customer.io is a Controller.	Name, email address, user ID.	None	Module 1
The parties Process Personal Data of their representatives to, e.g., (a) administer and provide the Services; (b) manage invoices;	Customer.io is a Controller. Company is a Controller.	Name, title, and contact information.	None	Module 1

(c) manage the Agreement and resolve any disputes relating to it; (d) respond and/or raise general queries; and (e) comply with their respective regulatory obligations.				

Subprocessors

Customer.io uses the Subprocessors listed here: https://customer.io/legal/sub-processors/. Company authorizes Customer.io to use these Subprocessors consistent with Section 7.4.

Information for International Transfers

Frequency of Transfer

Continuous for all Personal Data.

Retention Periods

Customer.io retains Personal Data it collects as a Controller for as long as Customer.io has a business purpose for it or for the longest time allowable by applicable law.

Customer.io retains Personal Data it collects or receives from Company as a Processor for the duration of the Agreement and consistent with its obligations in this DPA.

Standard Contractual Clauses

In relation to transfers of Customer Personal Data governed by the EU GDPR:

- Clause 7: The parties do not permit docking.
- Clause 9, Module 2(a): The parties select Option 2. The time period is 5 days.
- Clause 9, Module 3(a): The parties select Option 2. The time period is 5 days.
- Clause 11(a): The parties do **not** select the independent dispute resolution option.
- Clause 17: The parties agree that the governing jurisdiction is Irish law.
- Clause 18: For Modules 1-3, the parties agree that the forum is before the courts of Ireland.
- Annex I(A): The data exporter is Company. The data importer is Customer.io. Contact details for the parties are part of the Agreement.
- Annex I(B): The parties agree that Schedule 1 describes the transfer.
- Annex I(C): The competent supervisory authority is the supervisory authority that has primary jurisdiction over the data exporter.
- Annex II: The parties agree that Schedule 2 describes the technical and organizational measures applicable to the transfer.

Localizing the Standard Contractual Clauses

- For Switzerland
    - The parties adopt the GDPR standard for all data transfers.

    - Any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP;
    - references to "EU", "Union", "Member State" and "Member State law" will be interpreted as references to Switzerland and Swiss law, as the case may be, and will not be interpreted in such a way as to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs;
    - Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.
    - Clause 17: The parties agree that the governing jurisdiction is the laws of Switzerland.
    - Clause 18: For Modules 1-3, the parties agree that the forum is Switzerland. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).
    - The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.
- For the United Kingdom
    - The parties agree that the Standard Contractual Clauses are deemed amended to the extent necessary that they operate for transfers from the United Kingdom to a Third Country and provide appropriate safeguards for transfers according to Article 46 of the United Kingdom General Data Protection Regulation ("UK GDPR"). Such amendments include changing references to the GDPR to the UK GDPR and changing references to EU Member States to the United Kingdom. Tables 1 to 3 in Part 1 of the UK Addendum is deemed completed respectively with the information set out in Section 7.4 and this Schedule 1. Table 4 in Part 1 is deemed completed by selecting "neither party." Any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum
    - Clause 17: The parties agree that the governing jurisdiction is the United Kingdom.
    - Clause 18: For Modules 1-3, the parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.
- It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses prevail to the extent of such conflict

Schedule 2: Technical and Organizational Security Measures

Customer.io implements the security measures described here: https://customer.io/legal/security/.