DRIP GLOBAL, INC

DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**DPA**") is incorporated into, and forms part of the Agreement (as defined below).

1. DEFINITIONS

1.1 Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. The following capitalized terms used in this DPA will be defined as follows:

"**Adequate Jurisdiction**" means the UK, European Economic Area ("**EEA**") or a country or territory deemed to provide adequate protection for the rights and freedoms of individuals, as set out in: (a) the Data Protection Act 2018 or regulations made by the UK Secretary of State under the Data Protection Act 2018; (b) a decision of the European Commission; or (c) a decision of the Swiss Federal Council as listed in Annex 1 to the Ordinance (as amended from time to time).

"**Administrator Data**" means: (a) contact details relating to, and content of correspondence with the Administrator; and (b) support enquiries submitted by Users of the Subscribing Organization in relation to the Services.

"**Agreement**" means the agreement between the Subscribing Organization and Drip Global on the terms and conditions at https://www.drip.com/terms or such as other terms agreed between the Parties in writing.

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time, including (without limitation) the GDPR and the US Data Protection Laws.

"**Controller Purposes**" means: (a) administering Drip Global relationship with the Subscribing Organization under the Agreement, including maintaining and servicing Drip Accounts; (b) monitoring, investigating, preventing and detecting fraud, security incidents and other misuse of the Services; (c) monitoring the performance of the Services to identify and repair errors; (e) anonymising and aggregating data for the purpose of undertaking internal research for technological development, including testing, improving, developing and altering the functionality of the Services and developing new products and services.

"**Covered Data**" means Personal Data that is: (a) provided by or on behalf of the Subscribing Organization to Drip Global in connection with the Services; or (b) obtained, developed, produced or otherwise Processed by Drip Global, or its agents or subcontractors, for the purposes of providing the Services.

"**Data Subject**" means a natural person whose Personal Data is Processed.

"**Deidentified Data"** means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"**DPF**" means the "DPF", "EU-US Data Privacy Framework" or (where applicable) the "UK Extension to the EU-US Data Privacy Framework", in each case as defined in the relevant US Adequacy Decision.

"**DPF List**" means the "Data Privacy Framework List", "DPF List" or equivalent term in: (a) Commission Implementing Decision C(2023) 4745 on the adequate level of protection of personal data under the EU-US Data Privacy Framework; (b) the UK Data Protection (Adequacy) (United States of America) Regulations 2023; and (c) the Swiss Federal Office of Justice "Assessment of Adequacy – United States" dated 30 April 2024 ((a), (b) and (c), collectively, the "**US Adequacy Decisions**").

"**DPF Principles**" means the "EU-US Data Privacy Framework Principles" or "Principles" as defined in the applicable US Adequacy Decision.

"**DPF Transferred Data**" means Covered Data that is transferred by the Subscribing Organisation to Drip Global and either of the following applies: (a) the GDPR or Swiss Data Protection Laws apply to the Subscribing Organisation when making that transfer; or (b) the Covered Data was received by the Subscribing Organisation from a third party to which the GDPR or Swiss Data Protection Laws applied when making that transfer to the Subscribing Organisation.

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as defined in Section 3 of the UK Data Protection Act 2018.

"**Personal Data**" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Security Incident**" means a confirmed or reasonably suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data.

"**Services**" means the services to be provided by Drip Global pursuant to the Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"**Sub-processor**" means an entity appointed by Drip Global to Process Covered Data on its behalf.

"**Swiss Data Protection Laws**" means the Swiss Federal Act on Data Protection of 25 September 2020 ("FADP") and the Swiss Data Protection Ordinance of 31 August 2022 (the "Ordinance"), and any new or revised version of these laws that may enter into force for time to time.

"**US Data Protection Laws**" means, to the extent applicable, federal and state laws relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States including (without limitation): the CCPA, the Virginia Consumer Data Protection Act, Code of Virginia Title 59.1 Chapter 52 § 59.1-571 et seq., the Colorado Privacy Act, Colorado Revised Statute Title 6 Article 1 Part 13 § 6-1-1301 et seq., the Utah Consumer Privacy Act, Utah Code § 13-6-101 et seq., Connecticut Senate Bill 6, An Act Concerning Personal Data Privacy and Online Monitoring (as such law is chaptered and enrolled).

"**Usage Data**" means diagnostic, usage and performance information collected by Drip Global in relation to the Subscribing Organization's and its Users' use of the Services.

1.2 The terms "**controller**", "**processor**", "**business**" and "**service provider**" have the meanings given to them in the Applicable Data Protection Laws.

2. INTERACTION WITH THE AGREEMENT

2.1 This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any Processing of Covered Data.

2.2 The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

3. ROLE OF THE PARTIES

3.1 The Parties acknowledge and agree that, save as set out clause 3.2, Dip Global Processes Covered Data as a service provider or processor.

3.2 To the extent that:

(a) the GDPR applies to the Subscribing Organization when it shares Covered Data with Drip Global; or

(b) the transfer of Covered Data by the Subscribing Organization to Drip Global is an "onward transfer" as defined in the SCCs,

Drip Global Processes Covered Data (including Administrator Data and Usage Data) for the Controller Purposes as a controller.

4. DETAILS OF DATA PROCESSING

4.1 The details of the Processing of Personal Data under the Agreement and this DPA (such as subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in **Schedule 1** to this DPA.

4.2 The Subscribing Organization warrants and undertakes that the Covered Data shall not contain any Personal Data prohibited under the Agreement or Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.3 Save as set out in clause 3.2, Drip Global shall only Process Covered Data on behalf of and under the instructions of the Subscribing Organization and in accordance with Applicable Data Protection Laws. The Agreement and this DPA will generally constitute instructions for the Processing of Covered Data. The Subscribing Organization may issue further written instructions in accordance with this DPA. Without limiting the foregoing, Drip Global is prohibited from:

(a) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration;

(b) sharing Covered Data with any third party for cross-context behavioral advertising;

(c) retaining, using, or disclosing Covered Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Applicable Data Protection Laws;

(d) retaining, using, or disclosing Covered Data outside of the direct business relationship between the Parties; and

(e) except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that Drip Global receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

4.4 Drip Global will limit access to Covered Data to personnel who have a business need to have access to such Covered Data, and will ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement.

4.5 Drip Global may (without prejudice to clause 11) Process Covered Data anywhere that Drip Global or its Sub-processors maintain facilities.

4.6 Drip Global will provide the Subscribing Organization with information to enable the Subscribing Organization to conduct and document any data protection assessments required under Applicable Data Protection Laws. In addition, Drip Global will notify the Subscribing Organization promptly if Drip Global determines that it can no longer meet its obligations under Applicable Data Protection Laws.

4.7 The Subscribing Organization will have the right to take reasonable and appropriate steps to ensure that Drip Global uses Covered Data in a manner consistent with the Subscribing Organization's obligations under Applicable Data Protection Laws.

5. SUB-PROCESSORS

5.1 The Subscribing Organization grants Drip Global the general authorisation to engage any of the Sub-processors listed in Schedule 4, as updated in accordance with clause 5.3 ("**Authorized Sub-processors**"), subject to clause 5.2.

5.2 Drip Global will enter into a written agreement with each Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than Drip Global's obligations under this DPA.

5.3 Drip Global will provide the Subscribing Organization with at least fifteen (15) days' notice of any proposed changes to the Authorized Sub-processors. The Subscribing Organization may object to Drip Global's use of a new Sub-processor (including when exercising its right to object under clause 9(a) of the SCCs if applicable) by providing Drip Global with written notice of the objection within ten (10) days after Drip Global has provided notice to the

Subscribing Organization of such proposed change (an "**Objection**"). In the event the Subscribing Organization objects to Drip Global's use of a new Sub-processor, the Subscribing Organization and Drip Global will work together in good faith to find a mutually acceptable resolution to address such Objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, either Party may, as its sole and exclusive remedy, terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to the other Party. During any such Objection period, Drip Global may suspend the affected portion of the Services.

6. DATA SUBJECT RIGHTS REQUESTS

6.1 As between the Parties, the Subscribing Organization will have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Covered Data under Applicable Data Protection Laws (each, a "**Data Subject Request**"), other than in relation to any Data Subject Requests relating to Drip Global's Processing of Administrator Data and Usage Data for the Controller Purposes.

6.2 Drip Global will promptly forward to the Subscribing Organization without undue delay any Data Subject Request received by Drip Global or any Sub-processor and may advise the individual to submit their request directly to the Subscribing Organization.

6.3 Drip Global will provide the Subscribing Organization with reasonable assistance as necessary for the Subscribing Organization to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests, including if applicable, the Subscribing Organization's obligation to respond to requests for exercising the rights set out in Applicable Data Protection Laws.

7. SECURITY AND AUDITS

7.1 Drip Global will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure security of Covered Data, including, without limitation, protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage of or to it. When assessing the appropriate level of security, account will be taken in particular of the nature, scope, context and purpose of the Processing as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data.

7.2 Drip Global will implement and maintain as a minimum standard the measures set out in Schedule 2.

7.3 The Subscribing Organization will have the right to audit Drip Global's compliance with this DPA. The Parties agree that all such audits will be conducted:

(i) upon reasonable written notice to Drip Global;

(ii) only once per year; and

(iii) only during Drip Global's normal business hours.

7.4 To conduct such audits, the Subscribing Organization may engage a third-party auditor subject to such auditor complying with the requirements under clause 7.3 and provided that such auditor is suitably qualified and independent.

7.5 To request an audit, the Subscribing Organization must submit a detailed proposed audit plan to Drip Global at least two weeks in advance of the proposed audit date. Drip Global will review the proposed audit plan and work cooperatively with the Subscribing Organization to agree on a final audit plan. All such audits must be conducted subject to the agreed final audit plan and Drip Global's health and safety or other relevant policies.

7.6 The Subscribing Organization will promptly notify Drip Global of any non-compliance discovered during an audit.

7.7 The Subscribing Organization will bear the costs for any audit initiated by the Subscribing Organization, unless the audit reveals material non-compliance with the requirements of this DPA.

7.8 Drip Global shall provide to the Subscribing Organization upon request, or may provide to the Subscribing Organization in response to any audit request submitted by Subscribing Organization to Drip Global, either of the following:

(a) data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company; or

(b) any other documentation reasonably evidencing the implementation of the technical and organizational data security measures in accordance with industry standards.

7.9 If an audit requested by the Subscribing Organization is addressed in the documents or certification provided by Drip Global in accordance with clause 7.8, and:

(a) the certification or documentation is dated within twelve (12) months of the Subscribing Organization's audit request; and

(b) Drip Global confirms there are no known material changes in the controls audited,

the Subscribing Organization agrees to accept those findings in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

8. SECURITY INCIDENTS

8.1 Drip Global will notify the Subscribing Organization in writing without undue delay after becoming aware of any Security Incident, and reasonably cooperate in any obligation of the Subscribing Organization under Applicable Data Protection Laws to make any notifications, such as to individuals or supervisory authorities. Drip Global will take reasonable steps to contain, investigate, and mitigate any Security Incident, and will send the Subscribing Organization timely information about the Security Incident, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation. Drip Global's notification of or response to a Security Incident under this clause 8 will not be construed as an acknowledgement by Drip Global of any fault or liability with respect to the Security Incident.

8.2 Drip Global will provide reasonable assistance with the Subscribing Organization's investigation of the possible Security Incident and any notification obligation of the Subscribing Organization under Applicable Data Protection Laws, including any notification to Data Subjects or supervisory authorities.

9. DELETION AND RETURN

Drip Global will, if requested to do so by the Subscribing Organization within thirty (30) days of the date of termination or expiry of the Agreement (the "**Retention Period**"), return a copy of all Covered Data or provide a self-service functionality allowing the Subscribing Organization to do the same; and (b) on expiry of the Retention Period, delete all other copies of Covered Data Processed by Drip Global or any Sub-processors, other than any Covered Data that Drip Global is required to retain for compliance with applicable law and any Administration Data and Usage Data Processed for the Controller Purposes.

10. CONTRACT PERIOD

This DPA will commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Drip Global's deletion of all Covered Data as described in this DPA.

11. INTERNATIONAL TRANSFERS

11.1 Drip Global shall not transfer any DPF Transferred Data to a recipient outside the UK or EEA unless:

(a) the recipient is in an Adequate Jurisdiction; or

(b) Drip Global complies with the requirements of the DPF when making such transfer, including taking reasonable and appropriate steps to ensure that the recipient provides the same level of protection as the DPF Principles and notifies Drip Global if it makes a determination that it can no longer meet this obligation; or

(c) the transfer is otherwise not prohibited under Chapter V of the GDPR.

11.2 To the extent that Drip Global collects any Covered Data directly from Data Subjects ("**Directly Collected Data**"), Module Four (Processor to Controller) of the SCCs is hereby incorporated into this DPA and shall, as further specified in Schedule 3 of this DPA, apply to any transfers of Directly Collected Data from Drip Global (as data exporter) to the Subscribing Organization (as data importer) to the extent that:

(a) the GDPR or Swiss Data Protection Laws apply to Drip Global when making that transfer, or the transfer is an "onward transfer" (as defined in the applicable module of the SCCs); and

(b) the Subscribing Organization is not in the UK, EEA, or a country, territory, specified sector which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, as set out in:

(i) with respect to personal data relating to Data Subjects in the EEA or Switzerland, a decision of the European Commission;

(ii) with respect to personal data relating to Data Subjects in the UK, the UK Data Protection Act 2018 or regulations made by the UK Secretary of State under the UK Data Protection Act 2018; or

(iii) with respect to personal data relating to Data Subjects in Switzerland, the Ordinance.

11.3 To the extent that Drip Global ceases to be listed as a participating organisation in the applicable DPF List for the purposes of a US Adequacy Decision, or a US Adequacy Decision is repealed, withdrawn or otherwise does not apply to the transfer of DPF Transferred Data from Subscribing Organisation to Drip Global, the Parties agree that:

(a) Module One (Controller to Controller) and Module Two (Controller to Processor) of the SCCs shall apply to transfers of Covered Data from the Subscribing Organization (as data exporter) to Drip Global (as data importer), in each case as further set out in Schedule 3.

11.4 With respect to any transfers to which clause 11.2 or clause 11.3 apply, signature of this DPA shall have the same effect as signing the SCCs.

12. OTHER INTERNATIONAL TRANSFERS OF PERSONAL DATA

12.1 Subject to the remainder of this clause 12, Module One (Controller to Controller) and Module Two (Controller to Processor) of the SCCs shall apply to transfers of Covered Data from the Subscribing Organization (as data exporter) to Drip Global (as data importer) and Module Four (Processor to Controller) of the SCCs shall apply to transfers of Directly Collected Data from Drip Global (as data exporter) to the Subscribing Organization (as data importer), to the extent that:

(a) the transfer is not covered by clause 11; and

(b) the Applicable Data Protection Laws that apply to the applicable to the data exporter when making that transfer (the "**Exporter Data Protection Laws**") prohibit the transfer of Personal Data to a data importer under this DPA in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of that Personal Data; and

(c) any one or more of the following applies:

(i) the relevant authority with jurisdiction over the data exporter's transfer of Personal Data under this DPA has not formally adopted standard data protection clauses or another transfer mechanism under the Exporter Data Protection Laws; or

(ii) such authority has issued guidance that entering into standard contractual clauses approved by the European Commission would satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(iii) entering into standard contractual clauses approved by the European Commission would otherwise reasonably satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer.

12.2 With respect to any transfers of Personal Data referred to in clause 12.1 (each a "**Global Transfer**"), the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the Exporter Data Protection Laws.

12.3 For the purposes of any Global Transfers, the SCCs shall be deemed to be amended to the extent necessary so that they operate:

(a) for transfers made by the applicable data exporter to the data importer, to the extent the Exporter Data Protection Laws apply to that data exporter's Processing when making that transfer; and

(b) to provide appropriate safeguards for the transfers in accordance with the Exporter Data Protection Laws.

12.4 The amendments referred to in clause 12.3 include (without limitation) the following:

(a) references to the "GDPR" and to specific Articles of the GDPR are replaced with the equivalent provisions under the Exporter Data Protection Laws;

(b) reference to the "Union", "EU" and "EU Member State" are all replaced with reference to the jurisdiction in which the Exporter Data Protection Laws were issued (the "**Exporter Jurisdiction**");

(c) the "competent supervisory authority" shall be the applicable supervisory in the Exporter Jurisdiction; and

(d) Clauses 17 and 18 of the SCCs shall refer to the laws and courts of the Exporter Jurisdiction respectively.

12.5 With respect to any transfers that, at any time during the term of this DPA, cease being Global Transfers but continue to satisfy the conditions in clauses 11.3 and 12.1(b), the applicable data exporter and data importer shall promptly enter into a supplementary agreement that:

(i) incorporates any standard data protection clauses or another transfer mechanism formally adopted by the relevant authority in the Exporter Jurisdiction;

(ii) incorporates the details of Processing set out in Schedule 1;

(iii) shall, with respect to the transfer of Personal Data subject to the Exporter Data Protection Laws, take precedence over this DPA in the event of any conflict.

12.6 Where required under the Exporter Data Protection Laws, the relevant data exporter shall file a copy of the agreement entered into in accordance with clause 12.5 with the relevant national authority.

13. DEIDENTIFIED DATA

If Drip Global receives Deidentified Data from or on behalf of the Subscribing Organization, then Drip Global will:

(a) take reasonable measures to ensure the information cannot be associated with a Data Subject.

(b) publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information.

(c) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

SCHEDULE 1

DETAILS OF PROCESSING

A. List of Parties

With respect to transfers of Covered Data by the Subscribing Organization to Drip Global

	Subscribing Organization	**Drip Global**
Role	Data exporter (controller)	Data importer (processor or controller, as set out in clause 3)
Contact person	The Administrator	privacy@drip.com
Activities relevant to the transfer	The receipt of the Services under the Agreement.	The performance of the Services under the Agreement.

With respect to transfers of Directly Collected Data from Drip Global to the Subscribing Organization

	Drip Global	**Subscribing Organization**
Role	Data exporter (processor)	Data importer (controller)
Contact person	As above	As above
Activities relevant to the transfer	The performance of the Services under the Agreement.	The receipt of the Services under the Agreement.

B. Description of Processing

With respect to transfers of Covered Data by the Subscribing Organization to Drip Global

Categories of Data Subjects	"**Users**", being individual end users to whom the Subscribing Organization has given access to Drip "**Customers**", being customers of the Subscribing Organization, subscribers to updates from the Subscribing Organization and prospective customers or leads of the Subscribing Organization.
Categories of Personal Data	<u>Users</u> 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) <u>Contacts</u> Identification and contact data (name, date of birth, gender, occupation or other demographic information, address, title, contact details, including email address); personal interests or preferences (including purchase history, marketing preferences and publicly 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).
Special categories of Personal Data	None

Frequency of the transfer	Continuous
Nature of the Processing	The nature of the Processing is: • Collection • Storage • Organization and Structuring (Personal Data collected is stored in a secure environment using industry-standard encryption algorithms); • Disclosure by transmission (transferring of Personal Data to a third- party sub-processor as applicable in connection with the performance of the Services) • Erasure and destruction (Personal Data is erased per the Subscribing Organization's retention requirements) • Anonymisation and aggregation.
Purposes of the data transfer and further Processing	Where Drip acts as a processor, to provide the Drip platform and related services: • Creation and distribution of marketing emails on an automated basis in accordance with the Subscribing Organization's instructions; • Identification of target audiences; • Provision of analytics and feedback on email marketing campaigns. Where Drip acts as a controller, the Controller Purposes.
Retention period	Until termination of the Agreement or earlier deletion by the Subscribing Organization in accordance with the features and functionalities of Drip.
Subprocessors	As set out in Schedule 4

With respect to transfers of Directly Collected Data by Drip Global to the Subscribing Organization

Categories of Data Subjects	"**Contacts**", being customers of the Subscribing Organization, subscribers to updates from the Subscribing Organization and prospective customers or leads of the Subscribing Organization.
Categories of Personal Data	IP address, data relating to usage of the Subscribing Organization's service (such as products viewed and placed in shopping carts), online navigation data, location data, browser data
Special categories of Personal Data	None
Frequency of the transfer	Continuous
Nature of the Processing	The nature of the Processing is: • Collection • Storage • Organization and Structuring (Personal Data collected is stored in a secure environment using industry-standard encryption algorithms); • Disclosure by transmission (transferring of Personal Data to a third- party sub-processor as applicable in connection with the performance of the Services) • Erasure and destruction (Personal Data is erased per Subscribing Organization's retention requirements) • Anonymisation and aggregation.
Purposes of the data transfer and further Processing	Collection of information to support the email marketing campaigns the Subscribing Organization undertakes through the Drip platform.

Retention period	Until termination of the Agreement or earlier deletion by the Subscribing Organization in accordance with the features and functionalities of Drip.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

Drip Global has implemented the following technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

1) Organizational management and staff responsible for the development, implementation, and maintenance of Drip Global's information security program.

2) Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Drip Global's organization, monitoring and maintaining compliance with Drip Global's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3) Utilization of commercially available and industry standard encryption technologies for Covered Data that is being transmitted by Drip Global over public networks (i.e., the Internet) or when transmitted wirelessly.

4) Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

5) Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Drip Global's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Drip Global's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6) System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

7) Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Drip Global facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

8) Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Drip Global's possession.

9) Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Drip Global's technology and information assets.

0) Incident / problem management procedures design to allow Drip Global to investigate, respond to, mitigate, and notify of events related to Drip Global's technology and information assets.

10) Network security controls that provide for the use of firewall systems, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

11) Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

12) Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

1. EU SCCS

The Standard Contractual Clauses will apply to any Processing of Covered Data as set out in clauses 11.2, 11.3 or 12. For the purposes of the Standard Contractual Clauses:

1.1 Clause 7 of the Standard Contractual Clauses (*Docking Clause*) does not apply.

1.2 For transfers to which Module Two of the SCCs applies in accordance with clauses **Error! Reference source not found.** or 12, option 2 of Clause 9(a) (*General written authorization*) is selected, and the time period to be specified is determined in clause 5.3 of the DPA.

1.3 The option in Clause 11(a) of the Standard Contractual Clauses (*Independent dispute resolution body*) does not apply.

1.4 With regard to Clause 17 of the Standard Contractual Clauses (*Governing law*), the Parties agree that option 1 will apply and the governing law will be the law of the Republic of Ireland.

1.5 In Clause 18 of the Standard Contractual Clauses (*Choice of forum and jurisdiction*), the Parties submit themselves to the jurisdiction of the courts of the Republic of Ireland.

1.6 For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains details of the Parties, the description of transfer, and the competent supervisory authority

1.7 For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 2 of the DPA contains the technical and organizational measures.

2. UK ADDENDUM

2.1 This paragraph 2 (*UK Addendum*) shall apply to:

(a) any transfer of Covered Data from the Subscribing Organization (as data exporter) to Drip Global (as data importer) referred to in clause 11.3, to the extent that (i) the UK Data Protection Laws apply to the Subscribing Organization when making that transfer; or (ii) the transfer is an "onward transfer" as defined in the Approved Addendum; and

(b) any transfer of Directly Collected Data from Drip Global (as data exporter) to the Subscribing Organization (as data importer) referred to in clause 11.2, to the extent that (i) the UK Data Protection Laws apply to Drip Global when making that transfer; or (ii) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2:

"Approved Addendum" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum.

"**UK Data Protection Laws**" means all 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.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:

(a) the "Addendum EU SCCs" shall refer to the SCCs as they are incorporated into, and applied to transfers of Personal Data between the Parties as set out in clauses **Error! Reference source not found.** and **Error! Reference source not found.** and this Schedule 3;

(b) Table 1 of the Approved Addendum shall be completed with the details in paragraph A of Schedule 1;

(c) the "Appendix Information" shall refer to the information set out in Schedule 1 and Schedule 2

(d) for the purposes of Table 4 of the Approved Addendum, Drip Global (as data importer or data exporter) may end this DPA, to the extent the Approved Addendum applies, in accordance with Section 19 of the Approved Addendum;

(e) Section 16 of the Approved Addendum does not apply.

3. SWISS ADDENDUM

3.1 **Scope**

This Swiss Addendum shall apply to:

(a) any transfer of Covered Data from the Subscribing Organization (as data exporter) to Drip Global (as data importer) referred to in clause 11.3, to the extent that (i) the Processing of such Covered Data is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR; or (ii) the transfer is an "onward transfer" as defined in the Standard Contractual Clauses (as amended by this Swiss Addendum); and

(b) any transfer of Directly Collected Data from Drip Global (as data exporter) to the Subscribing Organization (as data importer) referred to in clause 11.2, to the extent that (i) the Processing of such Covered Data is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR; or (ii) the transfer is an "onward transfer" as defined in the Standard Contractual Clauses (as amended by this Swiss Addendum).

3.2 **Interpretation of this Addendum**

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
Clauses	The Standard Contractual Clauses as further specified in this Schedule
FDPIC	The Federal Data Protection and Information Commissioner

(b) This Addendum will be read and interpreted in a manner that is consistent with Swiss Data Protection Laws and so that it fulfils the Parties' obligations under Article 16(2)(d) of the FADP.

(c) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Swiss Addendum has been entered into.

(e) In relation to any Processing of Personal Data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends and supplements the Clauses to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer; and

(ii) as standard data protection clauses approved, issued or recognised by the FDPIC for the purposes of Article 16(2)(d) of the FADP.

3.3 **Hierarchy**

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 **Changes to the Clauses for transfers exclusively subject to Swiss Data Protection Laws**

To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.4) the following amendments are made to the Clauses:

(i) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(ii) Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer."

(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(iv) References to Regulation (EU) 2018/1725 are removed.

(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

(vii) Clause 17 is replaced to state

"These Clauses are governed by the laws of Switzerland".

(viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws 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 Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

3.5 **Supplementary provisions for transfers of Personal data subject to both the GDPR and Swiss Data Protection Laws**

(a) To the extent that the data exporter's Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" under both the Clauses and the Clauses as amended by this paragraph 3.5, the following amendments are made to the Clauses:

(i) for the purposes of Clause 13(a) and Part C of Annex I:

(A) the FDPIC shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer, or such transfer is an "onward transfer" as defined in the Clauses (as amended by paragraph 3.3 of this Addendum; and

(B) subject to the provisions of paragraph 2 of this Schedule 3 (*UK Addendum*), the supervisory authority identified in Schedule 1 shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent the GDPR applies to the data exporter's processing, or such transfer is an "onward transfer" as defined in the Clauses.

(ii) the terms "European Union", "Union", "EU", and "EU Member State" shall not be interpreted in a way that excludes the ability of Data Subjects in Switzerland bringing a claim in their place of habitual residence in accordance with Clause 18(c) of the Clauses; and

SCHEDULE 4
SUB-PROCESSORS

Name of Sub-processor	Address of Sub-processor	Description of Processing
Amazon Web Services	410 Terry Avenue North, Seattle, WA 98109-5210	Hosting provider
SolarWinds	7171 Southwest Parkway Building 400, Austin, TX 78735	Application performance monitoring.
Twilio	1801 California Street Suite 500, Denver, CO 80202	Email and SMS infrastructure provider
Zendesk	989 Market Street, San Francisco, CA 94103	Support System