EMA UNLIMITED DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Appendices, ("**DPA**") forms part of and is subject to the terms and conditions of the Master SaaS Subscription Agreement executed between Ema Unlimited, Inc. ("**Ema**") and the customer signing below ("**Customer**") for the purchase of Ema's proprietary software-as-a-service platform for generative workflow automation solutions (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Commercial Agreement**") to reflect the parties agreement with regard to the Processing of Customer Personal Data defined in Section 1 below. For the purposes of this DPA only, and except as indicated otherwise, the term "Customer" shall include Customer and any Affiliates that are authorized to use the Services. All capitalized terms not defined herein shall have the meaning set forth in the Commercial Agreement.

1. DEFINITIONS

1.1 "**Affiliate**" means, with respect to the identified party, any entity that is directly or indirectly controlled by, controlling or under common control with an entity, where "control" means more than 50% of the voting shares of the subject entity.

1.2 **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

1.3 **"Controller"** means the entity which determines the purposes and means of the Processing of Customer Personal Data.

1.4 **"Customer Personal Data"** means what is defined in the Commercial Agreement as "Customer Data" that is Personal Data, provided that such data is electronic data and information submitted by or for Customer to the Services.

1.5 **"Data Protection Laws and Regulations"** means all applicable laws, rules, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, security and data protection and/or Processing of Customer Personal Data as amended, replaced or superseded from time to time including but not limited to: (a) the CCPA; (b) EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; (c) the Swiss Federal Act on Data Protection; (d) the United Kingdom General Data Protection Regulation, and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time) ("**UK GDPR**").

1.6 **"Data Subject"** means the identified or identifiable natural person to whom Customer Personal Data relates and such terms shall have the same meaning as defined by applicable Data Protection Laws and Regulations.

1.7 **"Personal Data"** means any information relating to (a) an identified or identifiable natural person and, (b) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (a) or (b), such data is Customer Personal Data.

1.8 **"Process or Processing"** means any operation or set of operations that is performed upon Customer Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9 **"Processor"** means the entity which Processes Customer Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

1.10 **"Security Incident(s)"** means the breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or, or access to Customer Personal Data. A "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.11 **"Standard Contractual Clauses" or "SCCs"** means (a) where the GDPR applies the standard contractual clauses adopted by the EU Commission by means of the Implementing Decision EU 2021/914 as of June 4, 2021, and (b) where the United Kingdom General Data Protection Regulation GDPR applies, the standard contractual clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR.

1.12 **"Subprocessor(s)"** means Ema's authorized vendors and third-party service providers that Process Customer Personal Data.

1.13 "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR; and (b) any similar regulatory authority responsible for the enforcement of applicable Data Protection Laws and Regulations.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer is the Controller, Ema is the Processor and that Ema will engage Subprocessors pursuant to the requirements set forth in Section 5 "Subprocessors" below.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Customer Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Ema as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Customer Personal Data to the extent applicable under the CCPA.

2.3 Ema's Processing of Personal Data. Ema shall treat Customer Personal Data as Confidential Information and shall Process Customer Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (a) Processing in accordance with the Commercial Agreement and applicable Order Form(s); (b) Processing initiated by Permitted Users (as defined in the Commercial Agreement) in their use of the Services; and (c) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Commercial Agreement. Ema will Process Customer Personal Data in accordance with the GDPR requirements directly applicable to Ema's provision of its Services.

2.4 Details of the Processing**.** The subject-matter of Processing of Personal Data by Ema is the performance of the Services pursuant to the Commercial Agreement. The nature and purpose of the Processing, duration of the Processing, the categories of Data Subjects and the types of Personal Data Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

2.5 Personal Data Inquiries and Requests. Where required by Data Protection Laws and Regulations, Ema agrees to provide reasonable assistance and comply with reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Data Protection Laws and Regulations.

2.6 Data Protection Impact Assessment and Prior Consultation. Where required by Data Protection Laws and Regulations, Ema agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's reasonable judgement, the type of Processing performed by Ema requires a data protection impact assessment and/or prior consultation with the relevant Supervisory Authorities.

2.7 Aggregation and De-Identification. Ema may: (a) compile aggregated and/or de-identified information in connection with providing the Services provided that such information cannot reasonably be used to identify Customer or any Data Subject to whom Customer Personal Data relates ("**Aggregated and/or De-Identified Data**"); and (b) use Aggregated and/or De-Identified Data for its lawful business purposes.

2.8 Sale of Customer Personal Data Prohibited. Ema shall not sell Customer Personal Data as the term "sell" is defined by the CCPA.

2.9 Verify Compliance. Ema agrees to provide information reasonably necessary to verify its compliance with this DPA upon Customer's reasonable request.

3. RIGHTS OF DATA SUBJECTS. Ema shall, to the extent legally permitted, promptly notify Customer if Ema receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("**Right to be Forgotten**"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**". Taking into account the nature of the Processing, Ema shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Ema shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Ema is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Ema's provision of such assistance.

4. **EMA PERSONNEL.** Ema shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Customer Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Ema shall ensure that such confidentiality obligations survive the termination of the personnel engagement. Ema shall take commercially reasonable steps to ensure the reliability of any Ema personnel engaged in the Processing of Customer Personal Data. Ema shall ensure that Ema's access to Customer Personal Data is limited to those personnel performing Services in accordance with the Commercial Agreement.

5. **SUBPROCESSORS.** Pursuant to the Standard Contractual Clauses, Customer acknowledges and agrees that Ema may engage third party Subprocessors in connection with the provision of the Services. Ema has entered into a written agreement with each Subprocessor containing data protection obligations no less protective than those in this DPA with respect to the protection of Customer Personal Data, to the extent applicable to the nature of the Services provided by such Subprocessor. Ema shall make available to Customer the current list of Subprocessors for the Services identified in Schedule 3 and as otherwise provided upon written request. Ema shall be liable for the acts and omissions of its Subprocessors to the same extent Ema would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Commercial Agreement. **CUSTOMER'S EXECUTION OF THIS DPA CONSTITUTES CUSTOMER'S WRITTEN CONSENT AND AUTHORIZATION FOR EMA TO ENGAGE THE SUBPROCESSORS IDENTIFIED HEREIN.**

6. **SECURITY.** Taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Ema shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Customer Personal Data within Ema's control. Ema will regularly monitor compliance with these measures to ensure a level of security appropriate to the risk, as referred to in Article 32(1) of the GDPR. Ema will not materially decrease the overall security of the Services during a subscription term.

7. **SECURITY INCIDENT NOTIFICATION AND REMEDIATION.** Ema maintains security incident management policies and procedures and shall notify Customer without undue delay within the timeframe required under Data Protection Laws and Regulations. Ema will take all such measures and actions as are reasonably necessary to remediate the effects of the Security Incident to the extent the remediation is within Ema's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or its Permitted Users.

8. **CROSS-BORDER TRANSFERS OF CUSTOMER PERSONAL DATA.**

8.1 Cross-Border Transfers of Customer Personal Data. Customer authorizes Ema and its Subprocessors to transfer Customer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

8.2 EEA, Swiss, and UK Standard Contractual Clauses. If Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Ema in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws and Regulations, the parties agree that the transfer shall be governed by the Standard Contractual Clauses attached hereto as Schedule 2. The parties agree that: (a) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon Customer's written request; (b) the measures Ema is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover Ema's impacted systems; (c) the audit described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 10 of this DPA; (d) Ema may engage Subprocessors using the standard contractual clauses adopted by the European Commission under Implementing Decision (EU) 2021/914, or any other valid adequacy mechanism that complies with applicable Data Protection Laws and Regulations and such use of Subprocessors shall not be considered a breach of Clause 9 of the Standard Contractual Clauses; (e) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses, in which case, the corresponding Processing of Customer Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (f) unless otherwise stated by Ema, Customer will be responsible for communicating with Data Subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (g) the information required under Clause 15.1(c) will be provided upon Customer's written request; (h) notwithstanding anything to the contrary, Customer will reimburse Ema for all costs and expenses incurred by Ema in connection with the performance of Ema's obligations under Clause 15.1(b) and Clause 15.2 of the Standard Contractual Clauses without regard for any limitation of liability set forth in the Commercial Agreement. Each party's signature to the Commercial Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply

hereunder, and (i) in the case of transfers outside of the United Kingdom, (1) the governing law in Clause 9 and Clause 11.3. is the law of England and Wales, (2) references to Data Protection Law are replaced with applicable UK GDPR, (3) references to the EU or Member States are replaced with references to the United Kingdom, and (4) references to the EU authorities are replaced with references to the competent UK authority.

8.2.1 UK Transfers. Where the UK GDPR applies to a transfer of Personal Data, the Parties shall rely on either:
(i) the International Data Transfer Agreement (the 'UK IDTA') issued by the UK's Information Commissioner's Office ('ICO'), or
(ii) the UK Addendum to the EU Commission Standard Contractual Clauses (as issued by the ICO).
The IDTA or UK Addendum, once properly executed or incorporated by reference, shall form part of and supplement these Clauses in respect of such transfers.

8.3 Data Transfer Impact Assessment Outcome. Taking into account the information and obligations set forth in this DPA and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws and Regulations is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws and Regulations.

9. **DELETION OF CUSTOMER PERSONAL DATA.** Upon termination of this DPA or non-renewal of the Commercial Agreement, Ema shall delete Customer Personal Data in accordance with Ema's regular procedures and timeframes and as otherwise set forth in the Commercial Agreement, to the extent allowed by applicable Data Protection Laws and Regulations.

10. **AUDITS.** Any audits, including those described in the Standard Contractual Clauses shall be permitted after reasonable prior written notice, during Ema's normal business hours and at Customer's sole cost and expense. Ema may reject any requests for audits that are not made pursuant to a regulatory requirement or mandated by a Supervisory Authority. Before the commencement of any on-site audit, Customer and Ema shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible.

11. **TERMINATION OF THE DPA.** This DPA will continue in force until the termination of the Commercial Agreement (the "**Termination Date**"), provided that the data protection obligations of this DPA and the Standard Contractual Clauses shall continue to apply for so long as Ema Processes Customer Personal Data.

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

13. **ENTIRE AGREEMENT ORDER OR PRECEDENCE.** Except as supplemented by this DPA, the Commercial Agreement will remain in full force and effect. Any conflict between the terms of the Commercial Agreement and this DPA related to the processing of Customer Personal Data are resolved in the following order of priority: (1) the Standard Contractual Clauses, where applicable; (2) the DPA; and (3) the Commercial Agreement.

IN WITNESS WHEREOF, each party has caused to be signed and delivered by its duly authorized representatives with effect from the date of the last signature below.

Ema Unlimited, Inc.	**[Customer]**
Signature:_____	Signature:_____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

SCHEDULE 1 TO THE DATA PROCESSING ADDENDUM

DETAILS OF THE PROCESSING

- **Subject Matter**

The subject matter of the data Processing under this DPA is Customer Personal Data

- **Nature and Purpose of Processing**

Ema will Process Customer Personal Data as necessary to perform the Services pursuant to the Commercial Agreement.

- **Duration of Processing**

The duration of the Processing under this DPA is term of the Commercial Agreement.

- **Categories of Data Subjects**

Data Subjects whose Customer Personal Data will be Processed pursuant to the Commercial Agreement.

- **Special Categories of Personal Data**

Ema does not process any special categories of Personal Data

SCHEDULE 2 TO THE DATA PROCESSING ADDENDUM

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(f) To the extent applicable hereunder, these Clauses, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

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 specified in Annex I.B.

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of

implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State, the following section applies: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annexes to the Standard Contractual Clauses

ANNEX 1

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s):

Name: The entity identified as "Customer" in the Commercial Agreement.
Address: The address for Customer specified in the Commercial Agreement.
Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the DPA, or the Commercial Agreement.
Activities relevant to the data transferred under these Clauses: The Services as described in the Commercial Agreement
Role (controller/processor): Controller.

Data importer(s):

Name: Ema Unlimited, Inc.
Address: 139 Townsend Street, Suite 150, San Francisco, CA, 94107
privacy@ema.co.
Activities relevant to the data transferred under these Clauses: The Services as described in the Commercial Agreement
Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

- **Categories of Data Subjects whose Personal Data is transferred/Processed**

  The Personal Data transferred/Processed under the Commercial Agreement may concern the following categories of Data Subjects: Personnel of Customer who utilize the Services; individuals whose data may be contained in the Customer Personal Data provided by Customer

- **Categories of Personal Data transferred/Processed**

  The Personal Data transferred/Processed concern the following Categories of Personal Data:

  - Identification data (first and last name)
  - Title and position
  - Email address
  - Usage data related the Services
  - Any Customer Personal Data

- **Sensitive Data transferred.**

  Not Applicable

  Where Sensitive data is transferred (if applicable), the following restrictions or safeguards are applied: strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- **The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)**

  Continuous basis as need for performance of the Services

- **Nature of the Processing**

Personal Data is Processed by Ema in connection with its performance of the Services as set forth in the Commercial Agreement.

- **Purpose(s) of the data transfer and further Processing**

  Ema will Process Personal Data as necessary to perform the Services pursuant to the Commercial Agreement or as further specified by Controller's lawful documented instructions.

- **The period for which the Personal Data will be retained**

  For the duration of the Commercial Agreement, pursuant to the terms stated in the DPA, unless otherwise required by applicable Data Protection Laws and Regulations.

- **For transfers to (Subprocessors, also specify subject matter, nature and duration of the processing**

  Ema will use Subprocessors to assist in providing the Services for the duration of the Commercial Agreement, unless otherwise required in accordance with this DPA and/or applicable Data Protection Laws and Regulations. The list of Subprocessors is set forth in Schedule 3 of this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer shall implement and maintain appropriate technical and organizational measures designed to protect personal data as set forth at: https://app.vanta.com/ema/trust/1842i1jo9g53d8v89ohwb in accordance with the Addendum.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPA.

SCHEDULE 3 TO THE DATA PROCESSING ADDENDUM
LIST OF CURRENT SUBPROCESSOR

SUBPROCESSOR	COUNTRY	PURPOSE
Merge.dev	United States	API access to SAAS apps
Google Cloud Platform	United States	Cloud Service Provider
Azure Cloud Platform	United States	Cloud Service Provider
Hubspot	United States	CRM tool
Vercel.com	United States	API Libraries for Frontend Development
WorkOS	United States	Login Screen
Sentry	United States	Used for logging