DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**"), including all schedules and appendices, forms part of the Master Services Agreement ("Agreement") between EasyLlama, Inc., a Delaware corporation ("**Service Provider**" or "**Processor**" or "**Data Importer**") and [entity], a state corporation/LLC] ("**Customer**" or "**Controller**" or "**Data Exporter**"). In this DPA, Customer and Service Provider may also be referred to, singly, as a "**Party**" and, collectively, as the "**Parties**". Unless expressly defined otherwise herein, all capitalized terms used in this DPA shall have the meanings given to them in the Agreement.

(1) DEFINITIONS AND INTERPRETATION

In this DPA, the following terms shall have the following meanings unless expressly stated to the contrary.

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement. "Control," for purposes of this definition, means direct or indirect ownership or control of 50% or more of the voting interests of the subject entity, which (i) is subject to Data Protection Laws and Regulations, and (ii) is permitted to use the Services pursuant to the Agreement between Customer and Service Provider.

(b) "**Customer Data**" means all Personal Data, Customer Confidential Information, products, documents, materials, and any other items that may be supplied to the Processor by or on behalf of the Customer or any Personnel of the Customer pursuant to the Agreement or produced or obtained by the Service Provider wholly or partly at the Customer's expense.

(c) "**Data**" means all reports, documents, data, information, text, drawings, reports, specifications, statistics, analysis and other materials embodied in any form.

(d) "**Data Protection Law(s)**" or "**Applicable Law**" means (i) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); (ii) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("UK GDPR") and the Data Protection Act 2018 (together, "UK Data Protection Laws"), (iii) the Swiss Federal Data Protection Act and its implementing regulations ("Swiss DPA"), and (iv) all applicable U.S. state and federal data protection, data security and data privacy and security laws, including without limitation, the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020) (collectively, the "CCPA"), and the Virginia Consumer Data Protection Act of 2021, as amended, VA Code Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-581 ("VCDPA"); c) the Colorado Privacy Act and its implementing regulations ("CPA"); (d) the Utah Consumer Privacy Act ("UCPA"); (e) Connecticut SB6, An Act Concerning Personal Information Privacy and Online Monitoring ("CTDPA"); and (f) any other applicable laws, rules, orders or regulations related to the protection of Personal Data in the United States that is already in force or that will come into force during the term of this Addendum.

(e) "**Deidentified Information**" means information that cannot reasonably, be used to infer information about, identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or household.

(f) "**Data Controller**", "**Data Processor**", and "**Data Subject**" shall have the meanings ascribed under applicable GDPR and UK Data Protection Laws.

(g) "**Data Security Breach**" means any known potential or actual breach of the Service Provider's minimum information security requirements or any obligations or duties owed by the Service Provider to the Customer relating to the confidentiality, integrity or availability of Confidential Information or Personal Data, including unauthorized access to or disclosure of Personal Data.

(h) "**Personal Data**" means any and all personal data, as defined in the Data Protection Laws; including, without limitation, current or former customer or employee data supplied by Customer or Personnel of Customer in connection with the Services.

(i) "**Personnel**" means the current or former officers, directors, employees, agents and contractors (including subcontractors) of a Party and the members of its Affiliate.

(j) "**Processing**" means obtaining, recording or holding Personal Data or carrying out any operation or set of operations on Personal Data, including:

(i) organization, adaptation, amendment or alteration of Personal Data; or

(ii) retrieval, consultation or use of Personal Data; or

(iii) disclosure of the information or Personal Data by transmission, dissemination or otherwise making available to any third party or the public; or

(iv) alignment, combination, blocking, erasure or destruction of the Personal Data; and/or

(v) any additional meaning given in the Data Protection Laws.

(k) "**Services**" means the services to be delivered by or on behalf of the Service Provider pursuant to the Agreement.

(l) "**EU Standard Contractual Clauses**" means, in relation to the Processing of Personal Data pursuant to this DPA, the Module 2 model clauses for the transfer of Personal Data to Data Processors established in third countries approved by the European Commission, from time to time the approved version of which in force at present is set forth in Schedule 1 of this DPA.

(m) "**UK Standard Contractual Clauses**" means the EU Standard Contractual Clauses, as amended by the addendum published by the U.K. Information Commissioner's Office ("ICO") for use the transfer of data from the U.K. effective March 21, 2022 located at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended or replaced by the ICO from time to time.

(2) **DATA PROCESSING OBLIGATIONS - GENERAL.** In order to provide the Services to Customer, Service Provider will require certain Personal Data to be made available to it by Customer or its Personnel. The rights and obligations of each Party in connection with data Processing activities are set forth in Sections 3 and 4 below.

(3) **DATA PROTECTION OBLIGATIONS – EU/SWISS/UK**

(a) Obligations of the Controller. The Parties acknowledge that for the purposes of Data Protection Laws, Customer acts as a Data Controller ("**Controller**") under the Agreement. The Controller shall provide the Personal Data to the Processor together with such other information as the Processor may reasonably require in order for the Processor to provide the Services to the Controller.

(b) Obligations of the Processor. Service Provider performs as a Data Processor ("**Processor**") in respect of the Personal Data Processed under the Agreement on behalf of the Controller or a member of the Controller's Affiliate. All right, title and interest in the Personal Data shall vest solely in the Controller and the Processor shall not acquire any rights in the Personal Data, except as may be set out in this DPA and the Agreement.

(i) **Instructions**. The Processor shall only, and shall procure that its Personnel only, Process the Personal Data to the extent necessary to perform its obligations in accordance with this DPA, the Agreement, and any other written instructions of the Controller unless required to do so by Union or Member State law to which the Processor is subject and, in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

(ii) **Data Transfers**. The Processor shall not disclose the Controller Data to any third party without the prior written approval of the Controller. The Processor shall not transfer, or otherwise permit access to, any of the Personal Data or other information relating to current or former customers, candidates and Personnel of the Controller and of its Affiliates to a country outside of the European Economic Area ("EEA") or the United Kingdom ("UK") (each an "Exporting Country") except with the prior written consent of the Controller and in accordance with any terms the Controller may reasonably impose on such transfer.

1. **EU SCCs**. The Parties hereby agree to the EU Standard Contractual Clauses (the "SCCs"), Module 2, Transfer Controller to Processor, as set forth in Schedule 1 to this DPA which are incorporated herein by reference. Processor will Process all Personal Data from an Exporting Country in accordance with the EU Standard Contractual Clauses. For purposes of complying with the EU Standard Contractual Clauses, the Parties agree that Service Provider will be the "data importer" and Customer will be the "data exporter".

2. **UK SCCs**. The Parties further agree to apply the provisions of the UK Standard Contractual Clauses to the Processing of Personal Data from an Exporting Country, which is incorporated herein by reference. The SCCs attached hereto as Schedule 1 shall also apply to transfers of such data, and the Parties agree that Annexes I-III of the UK Standard Contractual Clauses shall be deemed completed with the information set forth in Annexes I through III of Schedule 1 of this DPA.

(iii) **Data Subject Rights**. The Processor agrees to assist the Controller, including taking appropriate technical and organisational measures which take into account the nature of the processing, to respond to requests by data

subjects, exercising their rights under Data Protection Laws, within such reasonable timescale as may be specified by the Controller.

(iv) **Assistance**. The Processor shall assist the Controller within such reasonable periods of time that allow the Controller to comply with its obligations pursuant to, Article 32 (Security), Articles 33 and 34 (Data Breach Notification), Article 35 (Data Protection Impact Assessments); and Article 36 (Prior Consultation) of the GDPR and provide all information necessary to demonstrate compliance with such obligations.

(v) **Breach Notification**. The Processor will notify the Controller without undue delay, and where feasible, no later than forty-eight (48) hours of the Processor becoming aware of a Data Security Breach, and shall include in such notification, at least the applicable information referred to in Article 33(3) of the GDPR. The Processor shall not communicate with any data subject with respect to a Data Security Breach without the prior written consent of the Controller, unless required by Applicable Law.

(vi) **Confidentiality**. Processor will ensure that its Personnel who Process Personal Data under this DPA and the Agreement are subject to obligations of confidentiality in relation to such Personal Data. Processor shall ensure that its personnel have received appropriate training regarding their responsibilities have committed themselves to obligations of confidentiality in relation to such Personal Data through executed written confidentiality agreements, and that such confidentiality obligations survive the termination of the Personnel engagement.

(vii) **Security**. Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, from accidental or unlawful destruction, loss, alteration, unauthorised, disclosure of or access to Personal Data including as appropriate: the pseudonymisation and encryption of Personal Data; the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. The Processor shall notify the Controller of any material changes to the technical and organisational measures used by the Processor throughout the Term.

(viii) **Sub-Processing**. Processor shall not engage any third party to Process the Controller's Personal Data without the prior written consent of the Controller. Controller hereby approves all sub processors identified in the list of sub-processors provided in Annex III of the Standard Contractual Clauses attached as Schedule 1 that will perform services necessary for Processor to perform the Services. Changes in sub processors shall be promptly communicated to Controller. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of the other processors. Customer may object to Processor's use of a new Sub-processor by notifying Processor promptly in writing within ten (10) days of receipt of notice. If Customer objects to a new Sub-processor, Processor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Processor without the use of the objected-to new Sub-processor by providing written notice to Processor.

If the Processor engages any third party to Process any Controller Data, Processor shall impose on such third party, by means of a written contract, the same data protection obligations as set forth in this DPA and shall ensure that, if any third-party engaged by Processor in turn engages another person to Process any Controller Data, the third party is required to comply with all of the obligations in respect of Processing Personal Data that are imposed under this DPA. The Processor shall remain fully liable to the Controller for Processing by any third party as if the Processing was being conducted by the Processor.

(ix) **Demonstrating Compliance**. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and this DPA, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor authorized by the

Controller, or any competent authority.

(x) **Infringement**. The Processor will immediately inform the Controller if, in its opinion, an instruction given or request made pursuant to this DPA or the Agreement infringes any Data Protection Law.

(xi) **Termination**. On termination of the Agreement (or at any other time upon request of the Controller), the Processor shall return and/or delete, at the election of the Controller, all copies of Personal Data received and/or processed by Processor under the Agreement unless European Union, Member State, or other applicable law requires retention of the Personal Data. The provisions of this Section 3 shall survive the durational term of the Agreement until the Processor has returned or destroyed all Personal Data.

(4) **DATA PROTECTION OBLIGATIONS – U.S.**

(a) **Definitions.** As used in this Section 4, the following terms have the meanings given them by U.S. Data Protection Laws, as may be amended from time to time: "Business," "Business Purpose," "Commercial", "Commercial Purpose," "Consumer," "Cross-Context Behavioral Advertising," Process," "Sell," and "Service Provider," "Share".

(b) **Service Provider Obligations**. Service Provider shall not collect, retain, use, disclose or otherwise make available Personal Data (and has not collected, retained, used, disclosed or otherwise made available Personal Data) for any purpose other than the limited and specified purpose of performing the Services during the term of the Agreement pursuant to the Agreement, except, where otherwise required by a law that applies to the particular Personal Data. In such a case, unless prohibited by law, Service Provider shall inform Customer of the relevant legal requirement before processing the Personal Data. The parties agree that the nature, purpose, duration, categories, and instructions for processing Personal Data are set forth in Annexes I through III of Schedule 1 of this DPA.

(c) **Service Provider Restrictions**. Without limiting the generality of the foregoing, at all times, Service Provider: (i) shall keep and maintain all Personal Data in strict confidence, using commercially reasonable care to avoid unauthorized collection, receipt, transmission, storage, disposal, use, destruction, disclosure or other processing (i) shall not collect, retain, use, or disclose Personal Data for any purpose other than the Business Purpose specified in the Agreement; (iii) shall not Sell or Share the Personal Data; (iv) shall not collect, retain, use, or disclose Personal Data outside the direct business relationship between Service Provider and Customer; (v) shall not collect more than the minimum Personal Data necessary, nor retain Personal Data longer than necessary, to perform the Services; (vi) shall not use Personal Data to build or modify a profile about a natural person to use in providing services to an entity other than Customer; and (vii) shall not correct or augment Personal Data nor otherwise combine it with Personal Data from or on behalf of another person or persons, or any another source (including from Service Provider itself). This DPA does not authorize Sharing or Processing of Personal Data for cross-context behavioral advertising or targeted advertising. Service Provider hereby certifies that it understands its obligations under this Section 4(c) and shall comply with the obligations set forth herein and as otherwise required under Applicable Law.

(d) **Cooperation.** Service Provider shall, upon reasonable request, make available all information reasonably necessary in Service Provider's possession to demonstrate Service Provider's compliance with its obligations under this Section. Service Provider shall reasonably cooperate with Customer as necessary for Customer to fulfill its responsibilities pursuant to Applicable Law with respect to Personal Data. Without limiting the generality of the foregoing, as Customer may direct, Service Provider shall promptly: (i) provide Customer copies of any or all Personal Data in a structured, commonly used, machine-readable format easily rendered into text an average consumer/data subject can read and understand; (ii) correct any or all Personal Data; (iii) delete any or all Personal Data; (iv) assist Customer as it reasonably requests to comply with requests by Consumers/Data Subjects or their agents pursuant to Applicable Law, including without limitation, requests to "know;" to "delete," to "correct", to "opt out," or to not "opt in"; and (v) assist Customer as it reasonably requests to facilitate its compliance with Applicable Law, including without limitation through Service Provider cooperation with audits and data protection assessments. For the avoidance of doubt, Service Provider shall not respond to requests from consumers or their agents as to Personal Data, except where and to the extent directed by Customer or required by Applicable Law. For the avoidance of doubt, neither the Agreement nor this DPA authorizes or permits Service Provider to respond to requests from consumers, their agents or other third parties relating to Personal Data unless Customer directs

Service Provider to respond in writing, in which case, Service Provider shall respond to the extent and in accordance with such written direction from Customer.

(e) **De-Identified Information.** Service Provider shall not reidentify or attempt to reidentify any Deidentified Information provided by, or obtained on behalf of, Customer. Service Provider shall not use Deidentified Information unless expressly authorized by the Agreement. If the Agreement authorizes such use and Service Provider intends to make such use, Service Provider represents and warrants, at all times, that it has implemented and that it shall maintain the following: (i) technical safeguards that prohibit reidentification of any individual or household to whom the information may pertain; (ii) business processes that specifically prohibit reidentification of the information; (iii) business processes to prevent inadvertent release of Deidentified Information; (iv) publicly commit to maintain and use Deidentified Information only in deidentified form, and make no attempt to reidentify Deidentified Information; (v) permit and facilitate reasonable Customer oversight of Service Provider's compliance with this paragraph; and (vi) process Deidentified Information only if, to the extent, and for the purposes permitted by Applicable Law and the Agreement.

(f) **Sub-Processors**. Service Provider shall not permit any third party, including any affiliate, to process Personal Data, except as authorized under this DPA. Prior to engaging any Sub-processor to process Personal Data, Service Provider shall notify Customer in advance of such engagement and provide Customer an opportunity to object to such Sub-processor's processing of Personal Data. If Customer objects to such Sub-processor, Service Provider shall not permit such Sup-processor to process Personal Data. If Customer does not object to such Sup-processor, Service Provider shall execute a written agreement with such Sub-processor imposing binding confidentiality and data processing obligations no less protective of the Personal Data than those imposed on Service Provider in this DPA and the Agreement. Service Provider remains fully liable to Customer for each Sub-processor's acts or omissions and performance of its obligations. Any Sub-processor used in accordance with this Section must qualify as a service provider or processor under the Applicable Law and Service Provider cannot make any disclosures of Personal Data to the Sub-processor that the Applicable Law would treat as a "Sale" or "Sharing". Upon the Customer's written request, Service Provider will audit a Sub-processor's compliance with its obligations relating to Personal Data and provide Customer with the audit results.

(g) **Non-Compliance Notice**. Service Provider shall promptly notify Customer if Service Provider determines it can no longer meet its obligations under this DPA or Applicable Law.

(h) **Remediation**. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

(5) **ENTIRE AGREEMENT; CONFLICT.** This DPA includes any applicable DPA Schedules incorporated by reference. Except as supplemented by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of the DPA will control, except that an applicable DPA Schedule will control over this DPA and the Agreement.

SERVICE PROVIDER:

Signature:_____

Name: _____

Title:_____

Date: _____

CUSTOMER:

Signature:_____

Name:_____

Title:_____

Date: _____

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES - MODULE 2

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.

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 –Clause 9(a), (c), (d);
(iv) Clause 12 –Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 –: 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: N/A

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 organizational measures, to satisfy its obligations under these Clauses.

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

(a) SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(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

(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.

(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

(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 that part of the compensation corresponding to 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

(a) 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.

(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, submits 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

(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

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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(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 the Republic 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.

SERVICE PROVIDER:	**CUSTOMER:**
Signature:_____	**Signature:**_____
Name:_____	**Name:**_____
Title:_____	**Title:**_____

ANNEX 1: DESCRIPTION OF THE TRANSFER

Annex 1(A): List of parties	
Data exporter	Name of the data exporter: _____ Address: Contact person's name, position and contact details: _____ _____ _____ _____ _____ Email: _____ Activities relevant to the data transferred: Transfer of Personal Data to Vendor for the purposes of providing the Services as more particular described in the Agreement. Role (Controller/Processor): Controller and/or Processor
Data importer	Name of the data importer: EasyLlama, Inc. Address: 440 N Barranca Ave #3753, Covina, CA 91723 Contact person's name, position and contact details: Michael Devyver, CTO, michael@easyllama.com Activities relevant to the data transferred: Performance of Services pursuant to the Agreement Role (Controller/Processor): Processor
Annex 1(B): Description of the transfer	
Description of transfer	*Categories of Data Subjects whose Personal Data is transferred*: Customer's employees and independent contractors authorized by Controller to use the Services. *Categories of Personal Data transferred*: name, email, work address, employee id, phone, employment title, employment type, employment department. *Sensitive Data transferred (if appropriate) and applied restrictions or safeguards*: N/A *Frequency of the transfer* (e.g. whether the data is transferred on a one-off or continuous basis): Continuous *Nature and subject matter of the Processing*: Vendor will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Data Exporter in its use of the Services. *Duration of the Processing*: Vendor will Process Personal Data for the duration of the Services and in accordance with the Agreement. *Purpose of the data transfer and further Processing:* Compliance with contractual obligations and related administration authenticating accounts and activity.
Annex 1(C): Competent supervisory authority	
Competent supervisory authority	The data protection authority of the EEA member state in which the Data exporter legal entity that has entered into the Agreement is established or, if such legal entity is not established in the EEA, the Irish Data Protection Commissioner. For the purposes of UK and Swiss transfers, the competent supervisory authority is the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable).

ANNEX 2: SECURITY MEASURES

ANNEX II

This Annex forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational measures implemented by Vendor (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:	
Measures of pseudonymisation and encryption of personal data	Customer Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to easyllama.com is encrypted with 128-bit encryption and supports TLS 1.2 and above. Logins and sensitive data transfer are performed over encrypted protocols such as TLS or ssh.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	EasyLlama maintains an information security program, which includes: (a) having a formal risk management program; (b) conducting periodic risk assessments of all systems and networks that process Customer Data on at least an annual basis; (c) monitoring for security incidents and maintaining a tiered remediation plan to ensure timely fixes to any discovered vulnerabilities; (d) a written information security policy and incident response plan that explicitly addresses and provides guidance to its personnel in furtherance of the security, confidentiality, integrity, and availability of Customer Data; (e) penetration testing performed by a qualified third party on an annual basis
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	EasyLlama takes daily snapshots of its databases and securely copies them to a separate data center for restoration purposes in the event of a regional AWS failure. Backups are encrypted and have the same protection in place as production.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	On an annual basis, EasyLlama performs on its own and engages third-parties to perform a variety of testing to protect against unauthorized access to Customer Data and to assess the security, reliability, and integrity of the Service. To the extent EasyLlama determines, in its sole discretion, that any remediation is required based on the results of such testing, it will perform such remediation within a reasonable period of time taking into account the nature and severity of the identified issue As of the Effective Date, EasyLlama undergoes a SOC 2 Type II audit on an annual basis with respect to the suitability of its controls to meet the criteria related to security, availability, and confidentiality set forth in the 2016 edition of TSP section 100A, Trust Services Principles and Criteria for Security (AICPA, Trust Services Principles and Criteria).
Measures for user identification and authorisation	Access to manage EasyLlama's AWS environment requires multi-factor authentication, ssh access to the Service is logged, and access to Customer Data is restricted to a limited set of approved EasyLlama employees. AWS networking features such as security groups are leveraged to restrict access to AWS instances and resources and are configured to restrict access using the principle of least privilege. Employees are trained on documented information security and privacy procedures. Every EasyLlama employee signs a data access policy that binds them to the terms of EasyLlama's data confidentiality policies and access to EasyLlama systems is promptly revoked upon termination of employment.
Measures for the protection of data during transmission	Customer Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to easyllama.com is encrypted with 128-bit encryption and supports TLS 1.2 and above. Logins and sensitive data transfer are performed over encrypted protocols such as TLS or ssh.

Measures for the protection of data during storage	Customer Data is stored cross-regionally with AWS. Data backups are encrypted. Customer data is encrypted at rest with AES 256 bit secret keys.
Measures for ensuring physical security of locations at which personal data are processed	EasyLlama uses Amazon Web Services (AWS) to provide management and hosting of production servers and databases in the United States and the European Union. AWS employs a robust physical security program with multiple certifications, including SSAE 16 and ISO 27001 certification.
Measures for ensuring events logging	All access to information security management systems at EasyLlama are restricted, monitored, and logged. At a minimum, log entries include date, timestamp, action performed, and the user ID or device ID of the action performed. The level of additional detail to be recorded by each audit log will be proportional to the amount and sensitivity of the information stored and/or processed on that system. All logs are protected from change.
Measures for ensuring system configuration, including default configuration	To prevent and minimize the potential for threats to EasyLlama's systems, baseline configurations are required prior to deployment of any user, network, or production equipment. Baseline configurations are in place for wireless security settings in order to ensure strong encryption and replace vendor default settings as part of deployment of network devices. Systems are centrally managed and configured to detect and alert on suspicious activity.
Measures for internal IT and IT security governance and management	IT Security Governance and Management structures and processes are designed to ensure compliance with data protection principles at their effective implementation.
Measures for certification/assurance of processes and products	As of the Effective Date, EasyLlama undergoes a SOC 2 Type II audit on an annual basis with respect to the suitability of its controls to meet the criteria related to security set forth in the 2016 edition of TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria).

Measures for ensuring data minimisation	EasyLlama only collects information that is necessary in order to provide the Services outlined in our Terms of Service or applicable Agreement. Our employees are directed to access only the minimum amount of information necessary to perform the task at hand.
Measures for ensuring data quality	EasyLlama maintains web Server and application log details that include any changes to sensitive configuration settings and files. At minimum, log entries include date, timestamp, action performed, and the user ID or the device ID of the action performed. Logs are protected from change. Users who would like to exercise their rights under applicable law to update information which is out of date or incorrect may do so at any time using this form. More information on data subject rights can be found at https://www.easyllama.com/privacy
Measures for ensuring limited data retention	EasyLlama will retain information for the period necessary to fulfill the purposes outlined in our Privacy Policy, unless a longer retention period is required or permitted by law, or where the Customer Agreement requires or permits specific retention or deletion periods. Customer may request deletion of data at any time and Customer Personal Data is deleted or anonymized upon termination of the Agreement.

Measures for ensuring accountability	EasyLlama has established a comprehensive GDPR compliance program and is committed to partnering with its customers and vendors on GDPR compliance efforts. Some significant steps EasyLlama has taken to align its practices with the GDPR include: Revisions to our policies and contracts with our partners, vendors, and users Enhancements to our security practices and procedures Closely reviewing and mapping the data we collect, use, and share Creating more robust internal privacy and security documentation Training employees on GDPR requirements and privacy and security best practices generally Carefully evaluating and building a data subject rights' policy and response process. Below, we provide additional details about the core areas of EasyLlama's GDPR compliance program and how customers can use EasyLlama to support their own GDPR compliance initiatives. EasyLlama offers its customers who are controllers of EU personal data the option to enter into a robust data processing addendum ("DPA") under which EasyLlama commits to process and safeguard personal data in accordance with GDPR requirements. This includes current Standard Contractual Clauses and EasyLlama's commitment to process personal data consistent with the instructions of the data controller.
Measures for allowing data portability and ensuring erasure	EasyLlama provides a mechanism for individuals to exercise their privacy rights in accordance with applicable law. Individuals may contact EasyLlama at any time using this form.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name	Description	Duration
Amazon Web Services	Hosting and storage systems provider	Continuous
Bugsnag	Application logging	Continuous
Hightouch	Data pipeline for connecting systems to our data warehouse	Continuous
Postmark	Transactional messaging	Continuous
Segment	Event logging for analytics	Continuous
Twilio	Transactional messaging	When text option is enabled
Front	Customer support communications	When contacting support
New Relic	Application Performance Analytics	Continuous
PostHog	Analytics	Continuous