ANNEX A

Privacy and Information Security Addendum

I. General

Pursuant to an Order Form (the "**Order Form**") and the applicable General Terms and Conditions (collectively the "**Agreement**"), Rupert, Inc. or one of its affiliated companies (collectively referred to herein as "**Rupert**" or "**Service Provider**") provides certain Services, as defined in the Order Form. This Privacy and Information Security Addendum (the "**Addendum**") is specific to the Services, where Rupert processes any Personal Information on behalf of Customer. This Addendum is entered into between Rupert and the Customer. Rupert retains the right to utilize its affiliated companies in pursuing any of its rights and fulfilling any of its obligations under this Addendum. Therefore, the term "Rupert" as used herein may also refer to affiliated companies that are directly or indirectly owned or controlled by the ultimate parent company of Rupert and who have been authorized by Rupert to distribute the Services.

This Addendum is additional to the terms in the Agreement and, to the extent that the terms in this Addendum are in conflict with the terms of the Agreement, the terms in this Addendum will take precedence and supersede the terms of the Agreement.

Capitalized terms shall have the meaning given to them above and otherwise shall have the meaning given to them in the Agreement and/or the Requirements.

II. Definitions

In this Addendum the following terms shall have the following meanings:

(A) "**Personnel**" means any employees, agents, consultants or contractors of Service Provider or Customer, as appropriate.

(B) "**Personal Information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a natural personal or household.

(C) "**Requirements**" means all applicable laws, statutes, rules, regulations, orders, decisions, interpretations, opinions, industry self-regulatory principles and guidelines, and other requirements, whether promulgated by the United States or any other applicable jurisdiction including, not by way of limitation, (i) the EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. ("**CCPA**"); (iv) the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("**CAN-SPAM**"); (v) information security breach notification laws (such as Cal. Civ. Code §§ 1798.29, 1798.82 - 1798.84); (vi) laws imposing minimum information security requirements (such as Cal. Civ. Code § 1798.81.5 and (vii) any federal or national data protection laws made under, pursuant to, replacing or succeeding (i), (ii), (iii), (iv), (v), (vi) related or applicable to Personal Information Processed by Service Provider; and successors of the foregoing, as they may be supplemented, revised or amended from time to time.

Terms that have been capitalized but not defined in this Addendum shall have the same meaning as in the Agreement.

III. Customer Obligations

Customer shall be responsible for compliance with any Requirements applicable to Customer (especially laws and regulations applicable to Controllers and/or Businesses) and shall ensure that Rupert and its Sub-Processors are allowed to provide the Services as Processor, Service Provider, or Sub-Processor.

IV. Privacy and Information Security

A. Service Provider represents, warrants and covenants as follows:

(1) **Authority to Process Personal Information**

(a) Service Provider is acting solely as a Service Provider and Data Processor with respect to Personal Information. Customer is acting as the Data Controller and the Business with respect to Personal Information and shall have the exclusive authority to determine the purposes for and means of Processing Personal Information.

(b) Service Provider shall Process Personal Information (i) on behalf of Customer; (ii) as necessary to perform the services specified in the Agreement for Customer's Business Purposes; and (iii) as otherwise permitted by the Requirements, including using Customer Data for a Business Purpose of developing the Services by means of machine learning that supports certain product features and functionality within the Services, and Service Provider shall not further collect, retain, use, disclose or otherwise Process Personal Information for any other purpose.

(c) Service Provider shall not retain, use, disclose or otherwise Process Personal Information outside of the direct business relationship between Customer and Service Provider and only to the extent necessary for the purposes set out under Section II(A)(1)(b).

(d) Service Provider shall not sell Personal Information.

(2) **Disclosure of and Access to Personal Information**

(a) Service Provider shall limit access to Personal Information to its Personnel who have a need to know the Personal Information as a condition to Service Provider's performance of the Services and who have explicitly agreed in writing to comply with legally-enforceable privacy, confidentiality and security obligations that are substantially similar to those required by this Addendum.

(b) Customer authorizes Service Provider to appoint Sub-processors in accordance with this Section II (2) (b). Service Provider may continue to use those Sub-processors already engaged by Service Provider as at the date of this Addendum, as enlisted in Appendix 1 to this Addendum. Service Provider shall give Customer prior written notice of the appointment of any new Sub-processor, including reasonable details of the Processing to be undertaken by the Sub-processor. If, within five (5) Business Days of receipt of that notice, Customer notifies Service Provider in writing of any objections (on reasonable grounds) to the proposed appointment: (a) Service Provider shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services which avoids the use

of that proposed Sub-processor; and (b) where: (i) such a change cannot be made within thirty (30) business days from Service Provider's receipt of Customer's notice; (ii) no commercially reasonable change is available; and/or (iii) Customer declines to bear the cost of the proposed change, notwithstanding anything in the Agreement, either Party may by written notice to the other Party with immediate effect terminate the Agreement either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-processor. With respect to each Sub-processor, Service Provider shall: (a) before the Sub-processor first Processes Customer Personal Data (or, as soon as reasonably practicable), carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Customer Personal Information required by this Addendum; and (b) ensure that the arrangement between Service Provider and the Sub-processor is governed by a written contract including terms which offer at least an equivalent level of protection for Customer Personal Information as those set out in this Addendum.

(c) Service Provider shall immediately inform Customer in writing of any requests with respect to Personal Information received from individuals whose Personal Information are Processed. Service Provider shall respond to such requests only in accordance with Customer's instructions. Service Provider shall reasonably assist Customer in fulfilling Customer's obligation to respond to individuals' requests to exercise their rights under the Requirements with respect to their Personal Information.

(d) Upon Customer's request, Service Provider shall delete a particular individual's Personal Information from Service Provider's records and direct any relevant Personnel to delete such Personal Information from their records as soon as reasonably possible. In the event Service Provider is unable to delete the Personal Information for reasons permitted under the Requirements, Service Provider shall (i) promptly inform Customer of the reason(s) for its refusal of the deletion request, (ii) ensure the privacy, confidentiality, and security of the Personal Information, and (iii) delete the Personal Information promptly after the reason for Service Provider's refusal has expired.

(e) Subject to applicable law, Service Provider shall notify Customer immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Information and comply and fully cooperate with all instructions of Customer relating thereto. Customer shall have the right to defend such action in lieu of and/or on behalf of Service Provider. Service Provider shall reasonably cooperate with Customer in such defense.

(3) **Compliance with Privacy and Information Security Requirements**

(a) Service Provider shall comply with applicable Requirements;

(b) No applicable Requirement, other laws, or privacy or information security enforcement action, investigation, litigation or claim prohibits Service Provider from (i) fulfilling its obligations under this Addendum or (ii) complying with instructions it receives from Customer concerning Personal Information. In the event a law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim, or any other circumstance, is reasonably likely to adversely affect Service Provider's ability to fulfill its obligations under this Addendum, Service Provider shall promptly notify Customer in writing and Customer may, in its sole discretion and without penalty of any

kind to Customer, suspend the (i) transfer or disclosure of Personal Information to Service Provider or (ii) access to Personal Information by Service Provider, terminate any further Processing of Personal Information by Service Provider, and terminate the Agreement, if doing so is necessary to comply with the Requirements.

(4) **Transfers of Personal Information**

To the extent that Service Provider transfers Personal Information and such transfer requires additional safeguards in accordance with Chapter V of the GDPR, the parties enter into and agree to abide by the Standard Contractual Clauses (the "**SCCs**") incorporated herein as Appendix 2, which form an integral part of this Addendum. For the purpose of the SCCs, the parties agree that the Customer is the "data exporter" and Service Provider is the "data importer".

(5) **Personal Information Safeguards**

(a) Taking into account the nature of the Processing, Service Provider has in place a written information security policy that complies with applicable Requirements. Service Provider's information security program includes appropriate administrative, technical and physical safeguards and other technical and organizational security measures designed to (i) ensure the security and confidentiality of Personal Information; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Information; and (iii) protect against any actual or suspected unauthorized Processing, loss, use, disclosure or acquisition of or access to any Personal Information (hereinafter "**Information Security Incident**").

(b) Service Provider shall inform Customer of any Information Security Incident of which Service Provider becomes aware as soon as reasonably possible, by providing notice via email using an email designated by Customer. Such notice shall summarize in reasonable detail the effect on Customer, if known, the nature and cause of the Information Security Incident (including, if known, a description of the Personal Information involved and approximate number of individuals and Personal Information records affected, and the likely consequences of the Information Security Incident), the date and/or time period during which the Information Security Incident is believed to have occurred, and the corrective actions taken or to be taken by Service Provider. Service Provider shall provide regular updates to Customer as additional information becomes available. Service Provider shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Information Security Incident. Service Provider shall keep and maintain a record of every Information Security Incident in connection with the services provided by Service Provider under the Agreement, and provide a copy of such records to Customer promptly upon request.

(c) Service Provider shall exercise the necessary and appropriate supervision over its relevant Personnel to maintain appropriate privacy, confidentiality and security of Personal Information. Service Provider shall provide training, as appropriate, regarding the privacy, confidentiality, and information security requirements set forth in this Addendum to relevant Personnel who have access to Personal Information.

(d) Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as Customer requests, Service Provider shall return to Customer or its designee, or at Customer's request, securely destroy or render unreadable or undecipherable if the return to Customer is not reasonably feasible or desirable Personal Information in Service Provider's possession, custody or control. In the event applicable law does not permit Service Provider to comply with the delivery or destruction of the Personal Information, Service Provider warrants that it shall ensure the privacy, confidentiality and security of the Personal Information in accordance with this Addendum and that it shall not use or disclose any Personal Information after termination of the Agreement.

(6) **Right to Monitor**

(a) During the term of this Agreement and not more than once per year (unless circumstances warrant additional audits as described below), Customer may, at Customer's expense, during regular business hours and without unreasonable interference with Service Provider's operations, audit Service Provider's policies, procedures and records that relate only to the performance of the Agreement upon at least 10 business days' written notice to Service Provider. Notwithstanding the foregoing, the parties agree that Customer may, at Customer's expense, during regular business hours and without unreasonable interference with Service Provider's operations, conduct an audit at any time, in the event of (i) audits required by governmental or regulatory authorities or (ii) Customer reasonably believes that an audit is necessary to address a material operational problem or issue that poses a threat to Customer's business.

(b) Service Provider shall deal promptly and appropriately with any reasonable inquiries from Customer relating to the Processing of Personal Information subject to this Addendum.

(B) The Parties acknowledge and agree that Customer does not sell Personal Information to Service Provider in connection with the Agreement.

(C) The Parties acknowledge and agree that Customer has no knowledge or reason to believe that Service Provider is unable to comply with the provisions of this Addendum.

V. **Miscellaneous**

All notices to be provided by Company to Service Provider under this Addendum may be delivered in writing (i) by nationally recognized overnight delivery service ("**Courier**") or US mail to the contact mailing address provided herein by Service Provider: 39 Clover St. Tenafly, NJ 07670, USA; or (ii) electronic mail to the following e-mail address: ziv@hirupert.com. All notices to be provided to Company by Service Provider in writing by Courier or US Mail, or via e-mail to the address provided by Customer to Rupert. All notices shall be deemed to have been given immediately upon delivery by electronic mail, or if otherwise delivered upon receipt or, if earlier, two (2) business days after being deposited in the mail or with a Courier as permitted above.

This Addendum is binding upon successors and assigns of the parties.

A waiver by either party of any term or condition of the Addendum in one or more instances shall not constitute a permanent waiver of the term or condition or any other term or condition of the addendum

or a general waiver.

APPENDIX I TO THE PRIVACY AND INFORMATION SECURITY ADDENDUM

SUB-PROCESSORS

Name	Processing Activity
Google Cloud	Cloud computing services (e.g. storage, data model processing, model training)
Intercom	Communication platform for messages and conversational support
Heap	Product analytics
Jumpcloud	Management of user identity, devices, and access.
Hotjar	Product analytics
FullStory	Product analytics
Sendgrid	Customer communication platform
Amplitude	Product analytics

APPENDIX II TO THE PRIVACY AND INFORMATION SECURITY 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)1 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 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

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 the 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 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 Union4 (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.

8.8 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) 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 five (5) business 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 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.

(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

(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.

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 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 _____ (*specify Member State*).

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 _____ (*specify Member State*).

(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.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
1. Name: [INSERT]
Address: [INSERT]
Contact person's name, position and contact details: [INSERT]
Activities relevant to the data transferred under these Clauses: As described in the Master Services Agreement.
Signature and date: [INSERT]
Role (controller/processor): Controller.

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Rupert, Inc.
Address: 39 Clover St. Tenafly, NJ 07670, USA
Contact person's name, position and contact details: Ziv Wangenheim, President, ziv@hirupert.com
Activities relevant to the data transferred under these Clauses: As described in the Master Services Agreement.
Signature and date: [INSERT]
Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Customer employees
Customers' customers
Individuals whose data is included in the Customer Data
……..
Categories of personal data transferred
Customer may submit Personal Information to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Information:

- *Name*
- *Title*
- *Position*
- *Employer*
- *Contact information (company, email, phone, physical business address)*
- *ID data*
- *Professional data*

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation,

access restrictions (including access only for staff having followed specialised 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
Nature of the processing
Data analysis and other activities included in the Service

Purpose(s) of the data transfer and further processing
Providing the Service.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the subscription period of the Service.
……..
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
……..

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with ____ (specify Member State)
……

ANNEX II

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

The technical and organizational measures that the data importer has implemented to protect the confidentiality, integrity, and availability of personal data include, not by way of limitation:

- Forcing HTTPS on all connections, so data in-transit is encrypted with TLS;
- Encrypting all database data at-rest with AES-256;
- Hosting all servers on Google Cloud in the US, in data centers that are SOC 1, SOC 2 and ISO 27001 certified, protected with strong passwords and two-factor authentication;
- Regularly conducting external penetration tests from third-party vendors;
- Regularly conducting security awareness training sessions with all employees;
- Maintaining detailed audit logs of all internal systems; and
- Implementing access control protocols to restrict data availability to those parties who need it.

ANNEX III – LIST OF SUB-PROCESSORS

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

Name	Processing Activity
Google Cloud	Cloud computing services (e.g. storage, data model processing, model training)
Intercom	Communication platform for messages and conversational support
Heap	Product analytics
Jumpcloud	Management of user identity, devices, and access.
Hotjar	Product analytics
FullStory	Product analytics
Sendgrid	Customer communication platform
Amplitude	Product analytics