Vector AI LTD
Registered in England & Wales
Company number: 11063616
55 Southwark Street
London SE1 1EU, UK

DATA PROCESSING ADDENDUM

1. Preamble. This Data Processing Addendum ("DPA"), forms part of the Software as a Service (SaaS) Agreement (the "SaaS Agreement") between Vector AI LTD, Inc. ("Company") and the entity that has engaged Company to provide the Service (as defined below) ("Customer") and shall be effective as of the date of the applicable SaaS Statement of Work (as defined in the SaaS Agreement). The applicable Saas Statement of Work(s) together with the SaaS Agreement are referred to collectively herein as the "Customer Agreement." This DPA is concluded for the duration of the Customer Agreement between Company and Customer. Terms used and not otherwise defined herein shall have the meanings ascribed to them in the Customer Agreement. In this DPA, "Service" means the services provided to Customer by the Company in accordance with the terms of the Customer Agreement.

2. Subject Matter, Nature, Purpose and Duration. Sections 2 through 6 of this DPA apply to the processing of personal data relating to data subjects located in the European Economic Area or the United Kingdom, or that is otherwise regulated by the GDPR, by the Company solely on behalf of Customer for the purpose of providing the Service ("EU Personal Data"). As between the parties, (i) Customer is a controller and the Company is a processor on behalf of Customer with regard to EU Personal Data or (ii) Customer is a processor and the Company is a sub-processor on behalf of Customer with regard to EU Personal Data. The subject matter and purposes of EU Personal Data processing, type of EU Personal Data, categories of data subjects, nature of the EU Personal Data processing, and Customer's data processing instructions for the Company, are set forth on Exhibit A to this DPA and as otherwise as provided in reasonable written instructions by Customer to the Company from time to time. The Controller is responsible for complying with its applicable data protection laws and for assessing whether the use of the Vector AI LTD Services meets its compliance and contractual obligations.This DPA shall remain in effect, and the duration of the processing under this DPA shall continue, as long as the Company carries out EU Personal Data processing operations on behalf of Customer or until the termination of the Customer Agreement (and all EU Personal Data has been returned or deleted in accordance with Section 3(g)). The following terms have the meanings given in the General Data Protection Regulation (EU) 2016/679 ("GDPR"): "controller", "personal data", "processor", "data subject" and "processing".

3. Processing Covenants. In processing EU Personal Data hereunder, the Company shall:

a. process EU Personal Data only on documented instructions from Customer, unless otherwise required to do so by applicable law, in which case the Company will inform Customer of that legal requirement before processing, unless applicable law prohibits the Company from informing Customer. For the avoidance of doubt, this DPA shall constitute Customer's documented instructions to the Company to process EU Personal Data in connection with the Company's provision of the Service to Customer;

b. use commercially reasonable efforts intended to ensure that persons authorized to process EU Personal Data hereunder have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality or are subject to ethical rules of responsibility that include confidentiality;

c. taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement commercially reasonable technical and organizational measures intended to meet the security requirements described in Article 32 of the GDPR. This does not limit the Controller's responsibility to safeguard its credential information and any components it has control over as well as to assess whether its privacy and security obligations are met when using the Vector AI LTD Services

d. taking into account the nature of the processing, use commercially reasonable efforts to assist Customer, at Customer's expense, by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to requests for exercising the data subjects' rights with respect to their EU Personal Data under the GDPR and any applicable national implementing legislation, regulations and secondary legislation relating to the processing of EU Personal Data (the "Data Protection Laws");

e. taking into account the nature of processing and the information available to the Company, use commercially reasonable efforts to assist Customer, at Customer's expense, in ensuring compliance with Customer's obligations described in Articles 32 through 36 of the GDPR;

f. notify Customer promptly if the Company becomes actually aware of a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, EU Personal Data (an "Incident"), provided that the provision of such notice by the Company shall not be construed as an acknowledgement of fault or liability with respect to any such Incident. In the event the Controller suspects that a potential incident occurred, the Controller shall with undue delay notify the Processor at contact@vector.ai.;

g. at the choice of Customer, delete or return all EU Personal Data to Customer within ninety (90) days after the end of the provision of the Service to Customer and delete existing copies unless applicable law requires retention of EU Personal Data or the Data has been archived on back-up systems due to Service functionalities, which Processor shall securely protect; and

h. make available upon Customer's reasonable request information reasonably necessary to demonstrate material compliance with the obligations laid down in this DPA and allow for and contribute to audits (each, an "Audit"), at Customer's expense, including inspections of processing facilities under the Company's control, conducted by Customer or another auditor chosen by Customer (an "Auditor"), during normal business hours, no more frequently than once during any twelve (12) month period, and upon reasonable prior notice at least eight (8) weeks in advance of the proposed audit date, provided that no Auditor shall be a competitor of the Company, and provided further that in no event shall Customer have access to the information of any other Customer of the Company and the disclosures made pursuant to this Section 3(h) ("Audit Information") shall be held in confidence as the Company's Confidential Information and subject to any confidentiality obligations in the Customer Agreement, and

provided further that no Audit shall be undertaken unless or until Customer has requested, and the Company has provided, documentation pursuant to this Section 3(h) and Customer reasonably determines that an Audit remains necessary to demonstrate material compliance with the obligations laid down in this DPA. Without limiting the generality of any provision in the Customer Agreement, Customer shall employ the same degree of care to safeguard Audit Information that it uses to protect its own confidential and proprietary information and in any event, not less than a reasonable degree of care under the circumstances, and Customer shall be liable for any improper disclosure or use of Audit Information by Customer or its agents.

g. The Processor will reasonably support the Controller in carrying out any assessment of the consequences or impact of Processing of Personal Data and in any consultation with the Supervision Authority.

h. The Processor will notify the Controller without delay if a Supervision Authority contacts the Processor directly with respect to the processing activities that fall within the subject matter of this DPA.

4. Sub-processors. Customer hereby grants the Company general authorization to engage another processor to process EU Personal Data on behalf of the Company (each a "sub-processor") to assist the Company in processing EU Personal Data as set out in this DPA. The Company shall enter into contractual arrangements with such sub-processors requiring the same level of data protection compliance and information security as that provided for herein. Customer hereby consents to the processing of EU Personal Data by, and the disclosure and transfer of EU Personal Data to, the sub-processors listed on Exhibit B to this DPA. The Company shall inform Customer of any intended changes concerning the addition or replacement of sub-processors at least ten (10) calendar days before the new sub-processor processes EU Personal Data. Customer may object to such changes in writing within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection (an "Objection"). In the event of an Objection, the parties will discuss such concerns in good faith with the intention of achieving a resolution. If the parties are not able to achieve a resolution as described in the previous sentence, Customer, as its sole and exclusive remedy, may terminate the Customer Agreement for convenience, on the condition that Customer provides written notice to the Company within five (5) calendar days of being informed of the engagement of the sub-processor. Customer shall not be entitled to any refund of fees paid prior to the date of any termination pursuant to this Section 4.

5. Customer Obligations. Customer represents, warrants, and covenants that (i) it shall comply with its obligations as a controller under the GDPR in respect of its processing of EU Personal Data and any processing instructions it issues to the Company as referred to in Section 3(a); (ii) it has provided notice and obtained all consents and rights required by the Data Protection Laws to transfer the EU Personal Data outside the European Economic Area or United Kingdom and for the Company to process EU Personal Data pursuant to the Customer Agreement and this DPA; and (iii) the processing of EU Personal Data by the Company upon the documented instructions of Customer under Section 3(a) shall have a lawful basis of processing pursuant to Articles 6 and 9 of the GDPR. If Customer is a processor, Customer represents and warrants to the Company that Customer's instructions and actions with respect to EU Personal Data, including its appointment of the Company as another processor, have been duly authorized by the relevant controller. Customer shall indemnify, defend and hold the Company harmless against any claims, actions, proceedings, expenses, damages and liabilities (including without limitation any governmental investigations, complaints and actions) and reasonable attorneys'

fees arising out of Customer's violation of this Section 5. Notwithstanding anything to the contrary in the Customer Agreement, Customer's indemnification obligations under this Section 5 shall not be subject to any limitations of liability set forth in the Customer Agreement.

6. Data Transfer. Customer hereby consents to the transfer of EU Personal Data to, and the processing of EU Personal Data in, the United States of America and/or in any other jurisdiction in which Company or its sub-processors have operations. For the avoidance of doubt, the Customer hereby authorizes the Processor to agree on these Standard Clauses on its behalf as data exporter with the relevant Sub-Processors as data importers. The parties hereby enter into the Standard Contractual Clauses for Processors, as approved by the European Commission under Decision 2010/87/EU, attached hereto as Exhibit C (the "SCCs") and made a part of this DPA in their entirety. Unless Processor notifies Customer to the contrary, if the European Commission amends the EU Standard Contractual Clauses at a date following the signature of this DPA, such amended terms will supersede and replace any EU Standard Contractual Clauses executed between the Parties. In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Customer Data to Third Countries, Processor may implement any additional measures or safeguards that may be reasonably required to enable a lawful transfer.

7. Other Personal Data. Notwithstanding anything to the contrary in the Customer Agreement (including this DPA), Customer acknowledges that the Company shall have a right to use and disclose data relating to the operation, support and/or use of the Service for its legitimate business purposes, such as product development and sales and marketing. To the extent any such data is considered personal data (as defined in, and regulated by the GDPR (as defined in Section 2)), the Company is the controller (as defined in the GDPR) of such data and accordingly shall process (as defined in the GDPR) such data in accordance with the Company's privacy policy and the GDPR.

9. Integration. This DPA, including the SCCs, and the Customer Agreement constitute the parties' entire agreement and understanding with respect to the subject matter hereof. Except as set forth in Sections 5 and 8(d), the obligations contained in this DPA are (i) subject to any limitations of liability set forth in the Customer Agreement and (ii) in addition to the other obligations contained in the Customer Agreement. In the event of a conflict between this DPA and any other terms in the Customer Agreement, the terms of this DPA will govern. For the avoidance of doubt, to the extent that the Customer Agreement excludes any types of information from confidentiality obligations, those exclusions shall not apply to information relating to any identified or identifiable natural person. This DPA shall be interpreted and construed in accordance with the governing laws and jurisdictions specified in the main agreement between the parties, unless otherwise provisioned in the applicable data protection laws.

Exhibit A

Subject Matter, Nature, Purpose and Duration of the Processing

1. Type of EU Personal Data:

Representatives of Customer: Personal data including, but not limited to: First name, last name, title, job title personal address, workplace address, billing address, email address, telephone number(s), payment

card information, password, transaction data, internet protocol address, analytics/audit logging features (logins, file views, modifying data); browser type and version, time zone setting and location, username, account ID, browser plug-in types and versions, operating system and platform and other technology on the devices used to access Vector AI LTDs' software, website, website usage data, website user marketing and communication preferences; and

Individuals whose EU Personal Data is included in files uploaded to the Service by Customer: Any EU Personal Data included in files uploaded to the Service by Customer and/or its representatives, the extent of which is determined and controlled by Customer in its sole discretion, including but not limited to: First name, last name, contact information, email address, date of hire, date of birth, government-issued identification number, bank account information and other financial information, compensation related information, human resources information, performance information, data concerning health, data concerning sexual orientation, ethnicity.

2. Categories of Data Subject:

Representatives of Customer; Individuals whose EU Personal Data is included in files uploaded to Company's platform by Customer.

3. Subject Matter and Purposes EU Personal Data Processing:

Company's provision of the Service to Customer in accordance with the Customer Agreement.

4. Nature of the Processing:

The EU Personal Data will be subject to basic processing, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Service by the Company to Customer in accordance with the terms of the Customer Agreement.

5. Special Categories of Data:

The parties do not anticipate the transfer of special categories of data.

Exhibit B

sub-processors

Apollo.io

Atlassian (Jira, Confluence, Trello)

Functional Software, Inc. d/b/a Sentry

Google, Inc.

Holistics Software Pte Ltd

HubSpot

Notion

PandaDoc, Inc.

SendGrid, Inc.

Slack

Smartsheets

Userpilot, Inc

Velaris Ltd

Exhibit C

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or

access to the data (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 purposes of processing and the risks involved for the data subjects.

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

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended

changes of that list through the addition or replacement of sub-processors at least one week in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

to the Standard Contractual Clauses

This Annex 1 forms part of the Clauses and must be completed and signed by the parties. By signing the signature page to the applicable SaaS Statement of Work, the parties will be deemed to have signed this Annex 1.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is the Service recipient of the data importer, the Customer or its affiliated entities.

Data importer

The data importer is the Service provider for data exporter, Vector AI LTD or Vector AI LTD's affiliated entities or sub-processors.

Data subjects

The personal data transferred concern the following categories of data subjects: Section 2 of Exhibit A to this DPA is incorporated herein by reference.

Categories of data

The personal data transferred concern the following categories of data: Section 1 of Exhibit A to this DPA is incorporated herein by reference.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: Section 5 of Exhibit A to this DPA is incorporated herein by reference.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): Section 4 of Exhibit A to this DPA is incorporated herein by reference.

Annex 2

to the Standard Contractual Clauses

This Annex forms part of the Clauses and must be completed and signed by the parties. By signing the signature page to the applicable SaaS Statement of Work, the parties will be deemed to have signed this Annex 2.

Description of the technical and organisational security measures implemented by the data attached.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data importer has implemented appropriate technical and organizational measures intended to ensure a level of security appropriate to the risk.