DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("**DPA**") is entered into as of the Addendum Effective Date by and between: (1) Trent AI Limited a company incorporated in England and Wales with company number 16213940 and registered office address at 85 Great Portland Street, London, England, W1W 7LT ("**Trent**"); and (2) the entity or other person who is a counterparty to the Agreement (as defined below) into which this DPA is incorporated and forms a part ("**Customer**"), together the "**Parties**" and each a "**Party**".

1. INTERPRETATION

1.1 In this DPA, the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Addendum Effective Date**" means the effective date of the Agreement.

(b) "**Agreement**" means the agreement under which Trent has agreed to provide Services to Customer entered into by and between the Parties.

(c) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to Trent's Processing of Customer Personal Data under the Agreement (including, as and where applicable, the GDPR, the State Privacy Laws, and the Australian Privacy Act 1988 (as amended)).

(d) "**Controller**" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(e) "**Customer Personal Data**" means any Personal Data Processed by Trent or its Sub-Processors on behalf of Customer to perform the Services under the Agreement.

(f) "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

(g) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Customer Personal Data and the Processing thereof.

(h) "**GDPR**" means, as and where applicable to Processing concerned, and each as amended from time to time: (i) the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law ("**UK GDPR**").

(i) "**Personal Data**" means "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws.

(j) "**Personal Data Breach**" means a breach of Trent's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in Trent's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(k) "**Personnel**" means a person's employees, agents, consultants, contractors or other staff.

(l) "**Process**", and grammatical inflections thereof, means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means.

(m) "**Processor**" means a natural or legal person that Processes Personal Data on behalf of a Controller.

(n) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Customer Personal Data to any person located in: (i) in the context of the EU GDPR, any country or territory outside the European Economic Area ("**EEA**") which does not benefit from an adequacy decision from the European Commission (an "**EU Restricted**

Transfer"); and (ii) in the context of the UK GDPR, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "**UK Restricted Transfer**"), which would be prohibited without a legal basis under Chapter V of the GDPR.

(o) "**SCCs**" means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(p) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Trent for Customer pursuant to the Agreement.

(q) "**State Privacy Laws**" means the comprehensive U.S. state-specific data privacy laws currently in effect and, in each case, as may be applicable to Trent's Processing of Customer Personal Data under the Agreement, for example, where so applicable, the California Consumer Privacy Act ("**CCPA**").

(r) "**Sub-Processor**" means any third party appointed by or on behalf of Trent to Process Customer Personal Data.

(s) "**Supervisory Authority**": (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office (or its successor).

(t) "**UK Transfer Addendum**" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Mandatory Clauses included in Part 2 thereof (the "**UK Mandatory Clauses**").

1.2 Unless otherwise defined in this DPA, all capitalised terms in this DPA shall have the meaning given to them in the Agreement.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 Details and roles. The Parties acknowledge and agree that the details of Trent's Processing of Customer Personal Data (including the respective roles of the Parties relating to such Processing) are as described in Annex 1 (Data Processing Details) to this DPA.

2.2 General. Trent shall not Process Customer Personal Data other than: (a) on Customer's instructions set out in the Agreement and this DPA; or (b) as required by applicable laws, provided that in such circumstances, Trent shall inform Customer in advance of the relevant legal requirement requiring such Processing if and to the extent Trent is: (i) required to do so by Applicable Data Protection Laws; and (ii) permitted to do so in the circumstances. Customer instructs and authorises Trent to Process Customer Personal Data for the purposes set out in the Agreement (as further described in Annex 1 (Data Processing Details) to this DPA). The Agreement is a complete expression of such instructions, and Customer's additional instructions will be binding on Trent only pursuant to any written amendment to this DPA signed by both Parties. Where required by Applicable Data Protection Laws, if Trent receives instruction from Customer that, in its reasonable opinion, infringes Applicable Data Protection Laws, Trent shall notify Customer.

3. TECHNICAL AND ORGANISATIONAL MEASURES; ASSISTANCE

3.1 Personnel. Trent shall take commercially reasonable steps designed to ascertain the reliability of any Trent Personnel who Process Customer Personal Data and shall enter into written confidentiality agreements with all Trent Personnel who Process Customer Personal Data that are not subject to professional or statutory obligations of confidentiality.

3.2 Security. Trent shall implement and maintain technical and organisational measures in relation to Customer Personal Data designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access as described in Annex 3 (Security Measures) (the "**Security Measures**"). Trent may modify these Security Measures from time to time to reflect its then-current security standards and practices;

provided that such modifications do not materially decrease the overall security of Services and/or relevant Customer Personal Data.

3.3 Data Subject Rights. Trent, taking into account the nature of the Processing of Customer Personal Data, shall provide Customer with such assistance as may be reasonably necessary and technically feasible to assist Customer in fulfilling its obligations to respond to Data Subject Requests. If Trent receives a Data Subject Request, Customer will be responsible for responding to any such request. Trent shall: (a) promptly notify Customer if it receives a Data Subject Request; and (b) not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Customer, except as required by Applicable Data Protection Laws.

3.4 DPIAs and Consultations. If and to the extent expressly required by Applicable Data Protection Laws (including, where applicable, by the GDPR) in relation to any given Processing of Customer Personal Data, Trent shall, taking into account the nature of the Processing and the information available to it, provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with Supervisory Authorities, which are required by Applicable Data Protection Laws (including, where applicable, Article 35 or Article 36 of the GDPR (as applicable)), in each case solely in relation to such Processing of Customer Personal Data by Trent.

4. PERSONAL DATA BREACHES

4.1 Notifications. Trent shall notify Customer without undue delay upon Trent's confirmation of a Personal Data Breach affecting Customer Personal Data. Trent shall provide Customer with information (insofar as such information is within Trent's possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Trent) to allow Customer to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. To the extent available, this notification will include Trent's then-current assessment of the following, which may be based on incomplete information: (a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (b) the likely consequences of the Personal Data Breach; and (c) measures taken or proposed to be taken by Trent to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects. Trent's notification of or response to a Personal Data Breach shall not be construed as Trent's acknowledgement of any fault or liability with respect to the Personal Data Breach. Nothing in this DPA, the SCCs or the SCCs as varied by the UK Transfer Addendum shall be construed to require Trent to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally. As between the Parties, Customer is solely responsible for complying with applicable laws (including notification laws), and fulfilling any third-party notification obligations, related to any Personal Data Breaches.

4.2 Consultation with Trent. If Customer determines that a Personal Data Breach suffered by Trent or a Sub-Processor affecting Customer Personal Data must be notified to any Supervisory Authority, any other governmental authority, any Data Subject(s), the public or others under Applicable Data Protection Laws or otherwise, to the extent such notice directly or indirectly refers to or identifies Trent, where permitted by applicable laws, Customer agrees to: (a) notify Trent in advance; and (b) in good faith, consult with Trent and consider any clarifications or corrections Trent may reasonably recommend or request to any such notice, which: (i) relate to Trent's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

5. SUB-PROCESSING

5.1 General authorisation. Customer generally authorises Trent to appoint Sub-Processors in accordance with this Section 5. Information about Trent's Sub-Processors, including their functions and locations, is as shown on the Sub-Processor list displayed from time to time at https://trust.trent.ai/subprocessors or any successor webpage (the "**Sub-Processor List**").

Without limitation, Customer authorises Trent engagement of the Sub-Processors listed on the Sub-Processor List as of the Addendum Effective Date.

5.2 Notification. Trent shall give Customer prior written notice of the appointment of any proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor, by updating the Sub-Processor List and providing a means by which Customer may subscribe to receive notice of such updates (or otherwise providing written notice to Customer). Customer agrees that Customer is solely responsible for ensuring that it subscribes to updates to the Sub-Processor List, and it shall do so. If, within ten (10) business days of receipt of that notice, Customer notifies Trent in writing of any objections to the proposed appointment (made in good faith based upon evidenced concerns that the use of that proposed Sub-Processor would cause Customer to be in material and unavoidable breach of Applicable Data Protection Laws): (a) Trent 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) days from Trent'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, then either Party may terminate without penalty the Processing of Customer Personal Data and/or the Agreement with respect only to those services which cannot be provided by Trent without the use of the objected-to new Sub-Processor by providing written notice to the other Party. If Customer does not object to Trent's appointment of a Sub-Processor during the objection period referred to in this Section 5.2, Customer shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

5.3 Trent Responsibilities. With respect to each Sub-Processor, Trent shall maintain a written contract between Trent and the Sub-Processor that includes terms which offer at least an equivalent level of protection for Customer Personal Data as those set out in this DPA (including the Security Measures). As between the Parties, Trent shall remain liable for any breach of this DPA caused by a Sub-Processor.

6. DATA TRANSFERS

6.1 Entry into SCCs. In respect of any Restricted Transfer of Customer Personal Data from Customer to Trent under this DPA that is: (a) an EU Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs; and/or (b) a UK Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs as varied by the UK Transfer Addendum.

6.2 Population of SCCs. In respect of any SCCs entered into pursuant to Section 6.1, the Parties agree as follows: (a) each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs; (b) as applicable: (i) Module Two of the SCCs applies to any relevant Restricted Transfer involving Processing of Customer Personal Data in respect of which Customer is a Controller in its own right; and (ii) Module Three of the SCCs applies to any relevant Restricted Transfer involving Processing of Customer Personal Data in respect of which Customer is itself a Processor; (c) as and where applicable to the relevant Module of the SCCs and the Clauses thereof: (i) in Clause 7: the 'Docking Clause' is not used; (ii) in Clause 9: 'OPTION 2: GENERAL WRITTEN AUTHORISATION' applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Section 5.2; (iii) in Clause 11: the optional language is not used; (iv) in Clause 13: all square brackets are removed and all text therein is retained; (v) in Clause 17: 'OPTION 1' applies, and the Parties agree that the SCCs shall be governed by the laws of Ireland; and (vi) in Clause 18(b): the Parties agree that any dispute arising from the SCCs shall be resolved by the courts of Ireland; and (d) in respect of the Annexes to the Appendix to the SCCs: (i) Annex I is populated with the corresponding information detailed in Annex 1 (Data Processing Details) to the DPA; and (ii) Annex II is populated with reference to the information contained in and determined by Section 3.2 of the DPA (including the Security Measures).

6.3 Population of UK Transfer Addendum. Where relevant in accordance with Section 6.1(b), the SCCs apply to any UK Restricted Transfers as varied by the UK Transfer Addendum in the following manner: (i) 'Part 1 to the UK Transfer Addendum': (A) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Data Processing Details) to the DPA and Section 6.2; and (B) Table 4 to the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked; and (ii) 'Part 2 to the UK Transfer Addendum': the Parties agree to be bound by the UK Mandatory Clauses and that the SCCs shall apply to any UK Restricted Transfers as varied in accordance with those Mandatory Clauses.

6.4 Operational Clarifications. In relation to any SCCs entered into pursuant to Section 6.1, the Parties agree as follows: (a) when complying with its transparency obligations under Clause 8.3 of the SCCs, Customer shall not provide or otherwise make available, and shall take all appropriate steps to protect, Trent's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information; (b) where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Trent to notify any third-party Controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer; (c) for the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required; (d) the terms and conditions of Section 5 apply in relation to Trent's appointment and use of Sub-Processors under the SCCs; (e) any approval by Customer of Trent's appointment of a Sub-Processor that is given expressly or deemed given pursuant to Section 5 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Sub-Processors if and as required under Clause 8.8 of the SCCs; (f) the audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in Section 7; (f) certification of deletion of Customer Personal Data as described in Clauses 8.5 and 16(d) of the SCCs shall be provided only upon Customer's written request; (g) in relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied by Section 6.3; and (h) in respect of any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject or further Controller (where applicable) – on specific written request; accompanied by suitable supporting evidence of the relevant request – Trent shall provide Customer with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with relevant provisions of this DPA in respect of the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage to evidence Customer's compliance with Applicable Data Protection Laws.

7. AUDITS

7.1 Information provision and audits. Trent shall make available to Customer, upon a reasonable request by Customer or its authorised designee, such information as Trent (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA. Subject to Sections 7.2 to 7.4, in the event that Customer (acting reasonably) is able to provide documentary evidence that such information is not sufficient in the circumstances to demonstrate Trent's compliance with this DPA, Trent shall allow for and contribute to audits by Customer or an auditor mandated by Customer in relation to the Processing of Customer Personal Data by Trent.

7.2 Customer responsibilities. Customer shall give Trent reasonable notice of any audit to be conducted under Section 7.1 (which shall in no event be less than thirty (30) days' notice, unless a shorter notice period is specifically required under Applicable Data Protection Laws relevant to the audit concerned) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury or disruption to Trent's premises, equipment, Personnel, data, and business (including any interference with

the confidentiality or security of the data of Trent's other customers or the availability of Trent's services to such other customers).

7.3 Audit plans. Prior to conducting any audit, Customer must submit a detailed proposed audit plan providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Trent will review the proposed audit plan and provide Customer with any feedback, concerns or questions (for example, any request for information that could compromise Trent security, privacy, employment or other relevant policies). Trent will work cooperatively with Customer to agree on a final audit plan.

7.4 Limitations. Trent need not give access to its premises for the purposes of any audit under this Section 7: (a) where a third-party audit report or certification (e.g., SOC 2 Type 2, ISO 2700x, NIST or similar audit report or certification) is provided in lieu of such access (acceptance of which for this purpose not to be unreasonably withheld, delayed or conditioned by Customer); (b) to any individual unless they produce reasonable evidence of their identity; (c) to any auditor whom Trent has not approved in advance (acting reasonably); (d) to any individual who has not entered into a non-disclosure agreement with Trent on terms acceptable to Trent (acting reasonably); (e) outside normal business hours at those premises; or (f) on more than one occasion in any calendar year during the term of the Agreement, except for any audits which Customer is required to carry out under Applicable Data Protection Laws or by a Supervisory Authority. Nothing in this DPA shall require Trent to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their customers. Nothing in this Section 7 shall be construed to obligate Trent to breach any duty of confidentiality.

8. RETURN AND DELETION

8.1 General. Upon expiration or earlier termination of the Agreement, Trent shall return and/or delete all Customer Personal Data in Trent's care, custody or control in accordance with Customer's instructions as to the post-termination return and deletion of Customer Personal Data expressed in the Agreement. To the extent that deletion of any Customer Personal Data contained in any back-ups maintained by or on behalf of Trent is not technically feasible within the timeframe set out in Customer's instructions, Trent shall (a) securely delete such Customer Personal Data in accordance with any relevant scheduled back-up deletion routines (e.g., those contained within relevant business continuity and disaster recovery procedures); and (b) pending such deletion, put such Customer Personal Data beyond use.

8.2 Permitted retention. Notwithstanding the foregoing, Trent may retain Customer Personal Data where required by applicable laws, provided that Trent shall (a) maintain the confidentiality of all such Customer Personal Data and (b) Process the Customer Personal Data only as necessary for the purpose(s) and duration specified in the applicable law requiring such retention.

9. CUSTOMER'S RESPONSIBILITIES

9.1 Security. Customer agrees that, without limiting Trent's obligations under Section 3.2 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Trent uses to provide the Services; and (d) backing up Customer Personal Data.

9.2 Compliance. Customer shall ensure: (a) that there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Trent of Customer Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where

applicable)); and (b) that all Data Subjects have (i) been presented with all required notices and statements (including as required by Articles 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Trent of Customer Personal Data.

9.3 Restricted Data. Customer shall not provide or otherwise make available to Trent any data or information that contains any: (a) Social Security numbers or other government-issued identification numbers; (b) health insurance information, Protected Health Information subject to the Health Insurance Portability and Accountability Act (HIPAA), or other information regarding an individual's health, medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) genetic, neural, or biological data; (d) data relating to a person's racial or ethnic origin, religious or philosophical beliefs, political opinions, sexuality or sexual orientation, status as transgender or non-binary, citizenship or immigration status, union membership, or status as a victim of crime; (e) passwords to any online accounts; (f) credentials to any financial accounts; (g) tax return data; (h) payment card information subject to the Payment Card Industry Data Security Standard; (i) any "biometric identifiers", "biometric information", "biometric data" or similar; (j) Personal Data of children under 16 years of age; or (k) other data or information that falls within any Special Categories of Personal Data (as defined in the GDPR) and/or data relating to criminal convictions and offences or related security measures. Sections 9.3(e) and 9.3(f) do not apply to credentials, keys or other secrets that Customer provides to enable the Services, or that are contained in content Customer submits to the Services. Where the Services request credentials, Customer shall use dedicated, least-privilege credentials.

10. VARIOUS

10.1 Incorporation and Application. This DPA shall be incorporated into and form part of the Agreement with effect on and from the Addendum Effective Date. This DPA: (a) applies only if and to the extent Applicable Data Protection Laws govern Trent's Processing of Customer Personal Data in performance of the Service(s) as a 'processor', 'service provider' or similar role defined under Applicable Data Protection Laws; and (b) does not apply to Trent's Processing of any Personal Data for Trent's own business/customer relationship administration purposes, its own marketing or service analytics, its own information and systems security purposes supporting the operation of the Services, nor its own legal, regulatory or compliance purposes.

10.2 State Privacy Laws. Annex 2 (State Privacy Laws Annex) applies if and to the extent Trent's Processing of Customer Personal Data on behalf of Customer under the Agreement is subject to the State Privacy Laws.

10.3 Costs. Except to the extent prohibited by Applicable Data Protection Laws, Customer shall compensate Trent at Trent's then-current professional services rates for, and reimburse any costs reasonably incurred by Trent in the course of providing, cooperation, information, or assistance requested by Customer pursuant to Sections 3.3 (Data Subject Rights), 3.4 (DPIAs and Consultations) and 7 (Audits) of this DPA (provided that Trent shall bear its own costs in the event that any audit or inspection conducted in accordance with that Section 7 reveals any material non-compliance by Trent with this DPA and/or Applicable Data Protection Laws), in each case, beyond providing self-service features included as part of, or in connection with, the Services.

10.4 LIABILITY. THE TOTAL AGGREGATE LIABILITY OF EITHER PARTY TOWARDS THE OTHER PARTY, HOWSOEVER ARISING, UNDER OR IN CONNECTION WITH THIS DPA AND THE SCCS (IF AND AS THEY APPLY) WILL UNDER NO CIRCUMSTANCES EXCEED ANY LIMITATIONS OR CAPS ON, AND SHALL BE SUBJECT TO ANY EXCLUSIONS OF, LIABILITY AND LOSS AGREED BY THE PARTIES IN THE AGREEMENT; PROVIDED THAT, NOTHING IN THIS SECTION 10.4 WILL AFFECT ANY PERSON'S LIABILITY TO DATA SUBJECTS UNDER THE THIRD-PARTY BENEFICIARY PROVISIONS OF THE SCCS (IF AND AS THEY APPLY).

10.5 Required Updates. Each Party shall act in good faith to agree variations to this DPA that are reasonably necessary to address the requirements of Applicable Data Protection Laws from time to time (including to apply a new transfer mechanism to comply with relevant requirements of the GDPR).

10.6 Prevail. This DPA shall be incorporated into and form part of the Agreement with effect on and from the Addendum Effective Date. In the event of any conflict or inconsistency between: (a) this DPA and the Agreement, this DPA shall prevail; (b) the SCCs entered into pursuant to Section 6 and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply; or (c) the UK Transfer Addendum entered into pursuant to Section 6 and this DPA and/or the Agreement, the UK Transfer Addendum shall prevail in respect of the UK Restricted Transfer to which they apply.

Annex 1

Data Processing Details

TRENT / DATA IMPORTER DETAILS

Name:	Trent AI Limited, a company incorporated in England and Wales, with company number 16213940.
Address:	CIC (Attn Trent AI), 22 Station Road, CB1 2JD, Cambridge, Cambridgeshire, United Kingdom
Contact Details for Data Protection:	Name: Maria Paz Klapztein (or other member of the organisation responsible for data protection, from time to time) Email: compliance@trent.ai
Trent Activities:	Trent AI provides an AI-native security platform designed to help organizations securely build, deploy, and operate AI-powered and autonomous software systems. The platform embeds continuous, context-aware security into the software development lifecycle, enabling teams to identify design-level risks, detect emerging threats, and protect AI workflows
Role:	Processor

CUSTOMER / DATA EXPORTER DETAILS

Name:	The entity or other person who is a counterparty to the Agreement
Address:	Customer's address is the address shown in or determined by the Agreement; or if no such address is contained within the Agreement, Customer's principal business trading address – unless otherwise notified to Trent's contact point noted above
Contact Details for Data Protection:	Customer's contact details are: • the contact details shown in the Agreement; or • if the Agreement does not include the contact details, Customer's contact details submitted by Customer and associated with Customers account for the Services
Customer Activities:	Customer's activities relevant to this DPA are the use and receipt of the Services from Trent under and in accordance with, and for the purposes anticipated and permitted in, the Agreement as part of the Customer's ongoing business operations
Role:	• Controller – in respect of any Processing of Customer Personal Data in respect of which Customer is a Controller in its own right; and • Processor – in respect of any Processing of Customer Personal Data in respect of which Customer is itself acting as a Processor on behalf of any other person (including, where applicable, its affiliates or Customer's own customers for whom Customer is a Processor)

DETAILS OF PROCESSING

Categories of Data Subjects:	Relevant Data Subjects include any Data Subjects that Customer causes Trent to process as part of the provision of the Service, including: • Customer's personnel: employees, contractors and other authorized users who access and use the Services; • Customer's end users: individuals who interact with Customer's systems that are protected by the Services, including via the "Prompt Guard" feature; and • other Data Subjects: any individuals whose Personal Data may be contained within the code, documents, prompts or other content uploaded to the Services.
Categories of Personal Data:	Relevant Personal Data includes any Categories of Data Customer causes Trent to process as part of the provision of the Service, including: • name and contact details; • account data (such as username and password); • technical data (such as IP address, device information, and access logs); • usage data; • service content data (Personal Data contained within the code, documents, prompts or other content uploaded to the Services); and • credentials and secrets provided by Customer to enable the Services, or contained in content Customer submits to the Services.
Sensitive Data:	Categories of sensitive data: None anticipated as noted in Section 9.3 of the DPA. Additional safeguards for sensitive data: N/A
Frequency of transfer:	Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.
Nature of the Processing:	Processing operations required in order to provide the Services in accordance with the Agreement.
Purpose of the Processing:	Customer Personal Data will be Processed as necessary to: • Provide the Services as initiated by Customer in its use thereof, and • Comply with any other reasonable instructions provided by Customer in accordance with the terms of this DPA.
Duration of Processing / Retention Period:	For the period determined in accordance with the Agreement and DPA, including Section 8 of the DPA.
Transfers to (sub-)processors:	Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List.

Competent Supervisory Authority:	With respect to the SCCs applicable to EU Restricted Transfers: (i) where Customer is established in an EEA Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EEA Member State in which Customer is established; or (ii) where Customer is not established in an EEA Member State: the competent Supervisory Authority shall be the Supervisory Authority of the EEA Member State in which Customer's Representative for the EU GDPR is based (from time to time), which Customer must notify to Trent in writing.

Annex 2

State Privacy Laws Annex

1. For purposes of this Annex 2, the terms "**business**," "**commercial purpose**," "**sell**," "**share**" and "**service provider**" shall have the respective meanings given thereto in the State Privacy Laws, and "**personal information**" shall mean Personal Data that constitutes personal information governed by the State Privacy Laws.

2. It is the Parties' intent that with respect to any personal information, Trent is a service provider. Trent (a) acknowledges that personal information is disclosed by Customer only for limited and specified purposes described in the Agreement; (b) shall comply with applicable obligations under the State Privacy Laws and shall provide the same level of privacy protection to personal information as is required by the State Privacy Laws; (c) agrees that Customer has the right to take reasonable and appropriate steps to help to ensure that Trent's use of personal information is consistent with Customer's obligations under the State Privacy Laws; (d) shall notify Customer in writing of any determination made by Trent that it can no longer meet its obligations under the State Privacy Laws; and (e) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorised use of personal information.

3. Trent shall not (a) sell or share any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Services, or as otherwise permitted by the State Privacy Laws; (c) retain, use or disclose the personal information outside of the direct business relationship between Trent and Customer; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) collected from Trent's own interaction with any Consumer to whom such personal information pertains, except as and to the extent necessary as a part of Trent's provision of the Services. Trent hereby certifies that it understands its obligations under this Section 3 and will comply with them.

4. Giving Customer notice of Sub-Processor engagements in accordance with Section 5 of the DPA shall satisfy Trent's obligation under the State Privacy Laws to give notice of and an opportunity to object to such engagements.

5. Trent agrees that Customer may conduct audits, in accordance with Section 7 of the DPA, to help ensure that Trent's use of personal information is consistent with Trent's obligations under the State Privacy Laws.

6. The Parties acknowledge that Trent's retention, use and disclosure of personal information authorised by Customer's instructions documented in the DPA are integral to Trent's provision of the Services and the business relationship between the Parties.

Annex 3

Security Measures

Trent agrees to implement and maintain the following security measures:

1. Organisational management and staff responsible for the development, implementation and maintenance of Trent's information security program.

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

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Customer Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

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

7. Physical and environmental security of production resources relevant to the Services is maintained by the relevant Sub-Processor(s) (and their vendors) engaged from time-to-time by Trent to host those resources. Trent takes steps to ensure that such Sub-Processors provide appropriate assurances and certifications that evidence such physical and environmental security – including security of data centre, server room facilities and other areas containing Customer Personal Data designed to:

   (a) protect information assets from unauthorised physical access,

   (b) manage, monitor and log movement into and out of Sub-Processor facilities, and

   (c) guard against environmental hazards such as heat, fire and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Trent's possession.

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

10. Incident management procedures designed to allow Trent to investigate, respond to, mitigate and notify of events related to Trent's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

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

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

Trent may freely update or modify these Security Measures from time to time **provided that** such updates and modifications do not materially decrease the overall security of Services and/or relevant Customer Personal Data.