Inferact: Data Processing Addendum

Last updated: July 8, 2026

This Data Processing Addendum ("DPA") is entered into as of the Addendum Effective Date by and between: (1) Inferact, Inc., a Delaware corporation with its principal business address at 440 North Barranca Avenue, Suite 8866, Covina, CA 91723, USA and, as applicable, Inferact's Affiliates (together, "Inferact"); and (2) the entity or other person who is a counterparty ("Customer") to the Agreement (as defined below) into which this DPA is incorporated and forms a part, 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(s) under which Inferact has agreed to provide Services to Customer entered into by and between the Parties that provides that this DPA is incorporated therein by reference.

(c) "**Applicable Data Protection Laws**" means all applicable foreign, national, state and local laws and regulations governing the Processing of Customer Personal Data under the Agreement, which are currently in effect and as they become effective, and as amended from time to time, including as and where applicable the GDPR, the FADP and/or State Privacy Laws.

(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 Customer Materials that constitute Personal Data and which Inferact or its Sub-Processors Process 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) "**FADP**" means the Swiss Federal Act on Data Protection in its revised version of 25 September 2020.

(i) "**GDPR**" means, as and where applicable: (i) the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); and/or (ii) the UK General Data Protection Regulation ("**UK GDPR**"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

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

(k) "**Personal Data Breach**" means a breach of Inferact's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in Inferact's possession, custody or control. For clarity, Personal Data Breach does not include (i) 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); or (ii) to the extent this DPA applies in the context of

the BYOC deployment model under the Agreement, compromises to the Customer Environment in which Customer Personal Data is Processed to the extent not caused by Inferact.

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

(m) "**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.

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

(o) "**Restricted Data**" means information that constitutes or contains any of the following: (i) Social Security numbers or other government-issued identification numbers; (ii) health insurance information, "individually identifiable health information" or "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; (iii) genetic, biometric, neural, or biological data; (iv) 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; (v) passwords to any online accounts; (vi) credentials to any financial accounts; (vii) tax return data; (viii) any payment card information subject to the Payment Card Industry Data Security Standard; (ix) Personal Data of minors under 18 years of age; (x) data relating to criminal convictions or offenses; or (xi) any other information that falls within any Special Categories of Personal Data (as defined in the GDPR).

(p) "**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**"); (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**"); and (iii) in respect of the FADP, a country or territory outside of Switzerland which does not benefit from an adequacy decision from the relevant Swiss authorities (a "**Swiss Restricted Transfer**"), in each case which would be prohibited without a legal basis under the EU or UK GDPR or FADP (as applicable).

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

(r) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Inferact for Customer pursuant to the Agreement such as compute and/or token processing capacity, storage, network connectivity, infrastructure, and related services, in each case as further described in the Agreement and the applicable Order Form.

(s) "**State Privacy Laws**" means, collectively, the comprehensive U.S. state-specific data privacy laws currently in effect and applicable to Inferact's Processing of the relevant Customer Personal Data under the Agreement.

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

(u) "**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; (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office ("**ICO**"); and (iii) in the context of Switzerland and the FADP, means the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

(v) "**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 capitalized 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 Inferact'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 the DPA.

2.2 General. Inferact 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, Inferact shall inform Customer in advance of the relevant legal requirement requiring such Processing if and to the extent Inferact is: (i) required to do so by Applicable Data Protection Laws; and (ii) permitted to do so in the circumstances. Customer instructs and authorizes Inferact to Process Customer Personal Data for the purposes set out in the Agreement (as further described in Annex 1 (Data Processing Details) to the DPA). The Agreement is a complete expression of such instructions, and Customer's additional instructions will be binding on Inferact only pursuant to any written amendment to this DPA signed by both Parties. Where required by Applicable Data Protection Laws, if Inferact receives an instruction from Customer that, in its reasonable opinion, infringes Applicable Data Protection Laws, Inferact shall notify Customer.

3. **TECHNICAL AND ORGANIZATIONAL MEASURES; ASSISTANCE**

3.1 Personnel. Inferact shall take commercially reasonable steps designed to ascertain the reliability of any Inferact Personnel who Process Customer Personal Data and shall impose confidentiality obligations on all Inferact Personnel who Process Customer Personal Data that are not subject to professional or statutory obligations of confidentiality.

3.2 Security.

(a) Inferact shall implement and maintain technical, administrative, physical, and organizational measures in relation to Customer Personal Data to the extent such measures are within Inferact's control designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access as described in Annex 3 (Security Measures) (the "Security Measures"). Inferact 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 protection of the relevant Customer Personal Data.

(b) Without prejudice to Inferact's security obligations, to the extent this DPA applies to Personal Data Processed in the Customer Environment, the following provisions apply:

(i) Customer shall implement and maintain technical, administrative, physical and organizational measures in relation to Personal Data designed to (i) protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access; (ii) prevent Inferact from unauthorizedly Processing Personal Data within the Customer Environment (excluding Customer Personal Data Processed in performance of the Services); and (iii) protect the Customer Environment.

(ii) Customer shall promptly notify Inferact in the event that Customer discovers or becomes aware that Inferact has Processed Personal Data in a manner that exceeds or does not comply with the DPA. Promptly following receipt of such notice, Customer and Inferact shall meet and confer, in good faith, in an effort to remediate such Processing.

3.3 Data Subject Rights. Inferact, 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, including access, deletion, and cessation of Processing of Customer Personal Data. If Inferact receives a Data Subject Request, Customer will be responsible for responding to any such request. Inferact 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 the given Processing of Customer Personal Data, Inferact 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), in each case solely in relation to such Processing of Customer Personal Data by Inferact.

4. PERSONAL DATA BREACHES

4.1 Inferact Notification to Customer. Inferact shall notify Customer without undue delay upon Inferact's confirmation of a Personal Data Breach affecting Customer Personal Data. Inferact shall provide Customer with information (insofar as such information is within Inferact's possession and knowledge and does not otherwise compromise the security of Inferact's information technology systems or practices or any Personal Data Processed by Inferact) designed 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 Inferact'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 approximate categories and 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 Inferact to address the Personal Data Breach, including, where applicable, measures designed to mitigate its possible adverse effects. Inferact's notification of or response to a Personal Data Breach shall not be construed as Inferact's acknowledgment of any fault or liability with respect to the Personal Data Breach. Nothing in this DPA or in the SCCs shall be construed to require Inferact 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 Inferact. If Customer determines that a Personal Data Breach 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 Inferact, where permitted by applicable laws, Customer agrees to: (a) notify Inferact in advance; and (b) in good faith, consult with Inferact and consider any clarifications or corrections Inferact may reasonably recommend or request to any such notice, which: (i) relate to Inferact's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

5. SUB-PROCESSING

5.1 General authorization. Customer generally authorizes Inferact to appoint Sub-Processors in accordance with this Section 5. Information about Inferact's Sub-Processors, including their functions and locations, is available at https://trust.inferact.ai/subprocessors (the **"Sub-Processor List**"). Customer authorizes Inferact's engagement of (a) the Sub-Processors listed on the Sub-Processor List as of the Addendum Effective Date; and (b) all of Inferact's Affiliates as Sub-Processors.

5.2 Notification. Inferact shall give Customer prior written notice of the appointment of any proposed new Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor by updating the Sub-Processor List. Customer agrees that Customer is solely responsible for ensuring that it subscribes to such updates, and it shall do so. If, within ten (10) business days of receipt of that notice, Customer notifies Inferact 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) Inferact 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 Inferact'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 Inferact without the use of the objected-to new Sub-Processor by providing written notice to the other Party. If Customer does not object to Inferact'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 Inferact Responsibilities. With respect to each Sub-Processor, Inferact shall maintain a written contract between Inferact and the Sub-Processor that includes terms which are designed to 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, Inferact 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 Inferact under this DPA: (a) that is an EU Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs; (b) that is 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 in accordance with Section 6.3; and/or (c) that is a Swiss Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs as varied in accordance with Section 6.4.

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 AUTHORIZATION' 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 law of: (A) Ireland in relation to any EU Restricted Transfer; (B) England and Wales in relation to any UK Restricted Transfer; and (C) Switzerland in relation to any Swiss Restricted Transfer; and (vi) in Clause 18(b): the Parties agree that any dispute arising from the SCCs shall be resolved by: (A) in relation to any EU Restricted Transfer, the courts of Ireland; (B) in relation to any UK Restricted Transfer, the courts of England and Wales; and (C) in relation to any Swiss Restricted Transfer, the courts of Switzerland; 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 labeled '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 Swiss Restricted Transfers. To the extent that any Processing of Customer Personal Data under this DPA involves a Swiss Restricted Transfer from Customer to Inferact, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (a) populated in accordance with Section 6.2; (b) varied in the following manner: (i) the FDPIC shall be the sole Supervisory Authority for Swiss Restricted Transfers exclusively subject to the FADP (including for the purposes of Annex I.C to the Appendix to the SCCs and the competent Supervisory Authority referenced therein); (ii) the terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the SCCs shall be interpreted to include the FADP with respect to Swiss Restricted Transfers; (iii) references to Regulation (EU) 2018/1725 are removed; (iv) references to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs; (v) where Swiss Restricted Transfers are exclusively subject to the FADP, all references to the GDPR in the SCCs are to be understood to be references to the FADP; and (vi) where Swiss Restricted Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the SCCs are to be understood to be references to the FADP only insofar as the Swiss Restricted Transfers are subject to the FADP; and (c) entered into by the Parties and incorporated by reference into this DPA.

6.5 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, Inferact'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 Inferact 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 Inferact's appointment and use of Sub-Processors under the SCCs; (e) any approval by Customer of Inferact'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; (g) 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; (h) in relation to any: (i) 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 (ii) Swiss 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 6.4; and (i) 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 – Inferact 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. Inferact shall make available to Customer, upon reasonable request by Customer or its designee, such information as Inferact (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 Inferact's compliance with this DPA, Inferact shall, subject to the provisions in this Section 7, allow for and contribute to audits by Customer or an auditor mandated by Customer in relation to the Processing of Customer Personal Data by Inferact.

7.2 Customer responsibilities. Customer shall: (a) give Inferact reasonable notice of any audit to be conducted under Section 7.1 (which shall in no event be less than fourteen (14) days' notice, unless a shorter notice period is specifically required under Applicable Data Protection Laws relevant to the audit concerned); (b) where appropriate (as determined at Inferact's discretion), conduct all audits remotely via means made available by Inferact for that purpose; (c) 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 Inferact's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Inferact's other customers or the availability of Inferact's services to such other customers); and (d) except to the extent prohibited by applicable law, reimburse Inferact for all of its costs incurred with such audits and the provision of any cooperation and assistance (excluding any costs incurred in the procurement, preparation, or delivery of Audit Reports to Customer).

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 as Inferact's Confidential Information. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Inferact will review the proposed audit plan and provide Customer with any feedback, concerns or questions (for example, any request for information that could compromise Inferact security, privacy, employment or other relevant policies). Inferact will work cooperatively with Customer to agree on a final audit plan.

7.4 Limitations. Inferact 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 Inferact has not approved in advance (acting reasonably); (d) to any individual who has not entered into a nondisclosure agreement with Inferact on terms acceptable to Inferact (acting reasonably); (e) outside normal business hours at those premises; (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; or (g) in relation to Personal Data Processed in the Customer Environment. Nothing in this DPA shall require Inferact 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 Inferact to breach any duty of confidentiality.

8. **RETURN AND DELETION**

8.1 General. Promptly following expiration or earlier termination of the Agreement, Inferact shall return and/or delete all Customer Personal Data in Inferact's possession, 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 backups' maintained by or on behalf of Inferact is not technically feasible within the timeframe set out in Customer's instructions, Inferact shall (a) securely delete such Customer Personal Data in accordance with any relevant scheduled backup deletion routines (e.g., those contained within Inferact's relevant business continuity and disaster recovery procedures); and (b) pending such deletion, put such Customer Personal Data beyond use other than for storage within such backups.

8.2 Permitted retention. Notwithstanding the foregoing, Inferact may retain Customer Personal Data where required by applicable laws, provided that Inferact shall 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 Inferact'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 Inferact uses to provide the Services; and (d) backing up Customer Personal Data.

9.2 Customer's Security Assessment. Customer has determined that the Services, the Security Measures and Inferact's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Customer Personal Data.

9.3 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 Inferact 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 Article 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Inferact of Customer Personal Data.

9.4 Restricted Data. Unless otherwise agreed by the Parties in writing, Customer represents and warrants that it will not provide or otherwise make accessible to Inferact any Restricted Data. Prior to Customer providing or otherwise making accessible to Inferact any "individually identifiable health information" or "protected health information" subject to HIPAA, the Parties must enter into a business associate agreement or similar agreement governing the Processing of such data.

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 Inferact'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 Inferact's Processing of any Personal Data for its 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 Inferact's Processing of the relevant 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 Inferact at Inferact's then-current professional services rates for, and reimburse any costs reasonably incurred by Inferact 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 Inferact shall bear its own costs in the event that any audit or inspection conducted in accordance with that Section 7 reveals any material noncompliance by Inferact 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 Updates. Each Party shall act in good faith to agree to variations to this DPA that are reasonably necessary to address the requirements of Applicable Data Protection Laws from time to time. Without limiting the foregoing, Inferact may on notice vary this DPA including to replace the relevant SCCs with any other transfer mechanism (including the EU-U.S. Data Privacy Framework or the UK Extension to the EU-U.S. Data Privacy Framework, or the Swiss-U.S. Data Privacy Framework) that enables the lawful transfer of Customer Personal Data by Customer to Inferact under this DPA in compliance with Chapter V 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; or (b) any 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.

Annex 1

Data Processing Details

INFERACT DETAILS

Name:	Inferact, Inc.
Address:	440 North Barranca Avenue, Suite 8866, Covina, CA 91723
Contact Details for Data Protection:	Email: privacy@inferact.ai
Inferact Activities:	Inferact provides a platform designed to run AI inference models for customers
Role:	Processor

CUSTOMER DETAILS

Name:	The entity who is a counterparty to the Agreement.
Address:	Customer's address is the address shown in the Order Form; or if no such address is contained within the Order Form, Customer's principal business trading address.
Contact Details for Data Protection:	As set forth in the Order Form or elsewhere in the Agreement between Customer and Inferact. Customer agrees that it is solely responsible for ensuring that such contact details are valid and up to date, and direct relevant communications to the appropriate individual within its organization.
Customer Activities:	Customer's activities relevant to this DPA are the use and receipt of the Services as part of its ongoing business operations under and in accordance with the Agreement.
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.

DETAILS OF PROCESSING

Categories of Data Subjects:	Any individuals whose Personal Data is comprised within Customer Data based upon Customer's use of the Services, which will be as determined by Customer in its sole discretion through its use of the Services – but may include: • Staff (as defined below). • Marketing prospects. • Customers. • Website visitors. • End-users and other users of Customer's products and services • Suppliers, service providers, vendors and other providers of goods or services. • Direct or indirect distributors, resellers, sales agents, introducers, sales representatives, collaborators, joint-venturers and other commercial partners. • Shareholders, investors, partners, members and supporters. • Advisers, consultants and other professionals and experts. Where any of the above is a business or organization, it includes their staff, namely, employees and non-employee workers; students, interns, apprentices and volunteers; directors and officers; advisers, consultants, independent contractors, agents and autonomous, temporary or casual workers, together with applicants and candidates for any one or more of the foregoing roles or positions (collectively, "**Staff**"). Each category includes current, past and prospective Data Subjects.
Categories of Personal Data:	Any Personal Data comprised within Customer Data based upon Customer's use of the Services, which will be as determined by Customer in its sole discretion through its use of the Services – but may (subject to the exclusion for Restricted Data unless otherwise agreed in writing by the Parties) include: • **Personal details** – for example any information that identifies the Data Subject and their personal characteristics, name, age, date of birth, sex, and physical description. • **Contact details** – for example home and/or business address, email address, telephone details and other contact information such as social media identifiers/handles. • **Public authority personal details** – for example, identifiers issued by a public authority, such as passport details, national insurance numbers, identity card numbers, driving licence details. • **Authentication details** – for example username, password or PIN code, security questions and other access protocols. • **Biometric details** – for example fingerprints, retinal/iris scans, which may be used for unique identification purposes. • **Family, lifestyle and social circumstance details** – for example any information relating to the family of the Data Subject and the Data Subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household

	members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organizations. • **Education and training details** – for example information which relates to the education and any professional training of the Data Subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records. • **Employment-/engagement-related details** – for example position, job title, corporate status, management category, job code, salary plan, pay grade or level, job function and sub-function, department, primary location for role, employment status and type, full-time/part-time, terms of employment/engagement, employment contract, contract of engagement, work history, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information, and attendance records, health and safety records, performance appraisals, training records, and security records. • **Financial details** – for example information relating to the financial affairs of the Data Subject, including income, salary, assets and investments, payments, loans, benefits, grants, insurance details, and pension information. • **Commercial details** – for example Personal Data relating to goods, services or other intellectual property licensed, developed provided and related information, including details of the goods or services supplied, licences issued and contracts, by or to Data Subjects. • **Technological details** – for example internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.
Sensitive Categories of Data, and associated additional restrictions/safeguards:	Categories of sensitive data: None absent prior written agreement between the Parties. To the extent the Parties agree to Process through the Services any Restricted Data, any such data submitted to Services by or on behalf of Customer under the Agreement will be as determined by Customer in its sole discretion through its use of the Services. Additional safeguards: Customer acknowledges that Inferact is unable to distinguish between the various categories of data which Customer may cause Inferact to Process in its provision of the Services. Inferact provides uniform standards of information and data security across the board to all relevant systems and data types in the manner determined by and set out in Section 3.2 of the DPA and the Security Measures
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, including collection, recording, organization, structuring, storage, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure and/or destruction.

Purpose of the Processing:	Processing necessary to provide the Services.
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 (as may be updated from time to time in accordance with Section 5 of the DPA).
Competent Supervisory Authority:	If and where applicable, having regard to Section 6 of the DPA: • **EU Restricted Transfers**: the competent Supervisory Authority shall be determined as follows: (i) where Customer is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which Customer is established; and (ii) where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EU Representative under Article 27 of the GDPR: the competent Supervisory Authority shall be the Supervisory Authority of the EU Member State in which Customer's EU Representative relevant to the Processing hereunder is based (from time-to-time), which Customer shall notify to Inferact in writing. • **UK Restricted Transfers**: the ICO. • **Swiss Restricted Transfers**: the FDPIC

Annex 2

State Privacy Laws Annex

1. For purposes of this Annex 2, the terms "business," "commercial purpose," "sell," "share," "targeted advertising" 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, Inferact is a service provider. Inferact (a) acknowledges that personal information is disclosed by Customer only for the 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 Inferact'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 Inferact 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 unauthorized use of personal information.

3. Inferact shall not (a) sell or share any personal information or use it for targeted advertising; (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 Inferact 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 Inferact's own interaction with any Consumer to whom such personal information pertains, except as and to the extent necessary as a part of Inferact's provision of the Services. Inferact hereby certifies that it understands its obligations under this Annex 2 and will comply with them.

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

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

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

Annex 3

Security Measures

- **Data Security Controls**. Data security controls such as logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Customer Personal Data as and where appropriate to the data concerned.
- **Logical Access Controls**. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.
- **Password Controls**. Password controls designed to manage and control password strength, expiration and usage.
- **Physical and Environmental Security**. Physical and environmental security of production resources relevant to the Services, which are maintained by the relevant Sub-Processor(s) (and their vendors) engaged from time-to-time by Inferact to host those resources. Inferact takes reasonable steps to ensure that such Sub-Processors provide appropriate assurances and certifications that evidence such physical and environmental security – including security of data center, server room facilities and other areas containing Customer Personal Data designed to: (a) protect information assets from unauthorized 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.
- **Operational Procedures**. Operational procedures and controls designed to provide for configuration, monitoring and maintenance of technology and information systems.
- **Change Management**. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to technology and information assets applicable to the Services and Customer Personal Data.
- **Incident Management**. Incident management procedures designed to allow Inferact to investigate, respond to, mitigate and notify of events related to technology and information assets applicable to the Services and Customer Personal Data. Notification procedure for timely disclosure in case of events affecting information assets applicable to the Services and Customer Personal Data or the systems processing them.
- **Network Security**. Network security controls that provide for the use of enterprise firewalls designed to protect systems from intrusion and limit the scope of any successful attack.
- **Vulnerability Assessment and Threat Protection**. Vulnerability assessment and threat protection technologies designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
- **BC/DR**. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.