DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") is incorporated into the agreement pursuant to which Customer obtains the right to use the Services (the "Master Agreement") (collectively, the "Agreement").

1. DEFINITIONS

1.1 "**CCPA**" means the California Consumer Privacy Act of 2018 as amended, including by the California Privacy Rights Act [1798.100 - 1798.199] and regulations adopted thereunder.

1.2 "**Data Protection Law**" means all data protection laws and regulations that apply to the Processing of Personal Data by Informatica under the Agreement, which may include, without limitation, GDPR, CCPA, and LGPD.

1.3 "**Data Subject**" means an identified or identifiable natural person to whom any Personal Data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.4 "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.5 "**Informatica**" means the applicable Informatica Group entity that entered into the Master Agreement.

1.6 "**Informatica Group**" means, collectively, Informatica LLC, Informatica Ireland EMEA UC, and their Affiliates.

1.7 "**LGPD**" means the Brazilian General Data Protection Law, Law No. 13,709, of August 14, 2018.

1.8 "**Personal Data**" means any data that the Customer submits using the Services for Informatica to Process on Customer's behalf that is deemed "personal data" or "personal information" (or other analogous variations of such terms) under Data Protection Law.

1.9 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.10 "**Process**" or "**Processing**" 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, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "**Services**" means any of the following services provided by Informatica pursuant to the Master Agreement: (a) Informatica-branded product offerings made available via the Internet, as described in Annex I ("Scope of Processing"), (b) consulting or training services provided either remotely via the Internet or in person, and (c) any support services, including as applicable to your orders, access to Informatica's help desk and to updates, upgrades, patches and bug fixes.

1.12 "**Standard Contractual Clauses**" means with respect to Switzerland and Brazil, the standard contractual clauses adopted by the European Commission as of June 4, 2021, the text of which is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN ("**EU Standard Contractual Clauses**"), and with respect to the United Kingdom, the EU Standard Contractual Clauses supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, the text of which is available at: https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf ("**International Data Transfer Addendum**") (together with the EU Standard Contractual Clauses, the "**UK Standard Contractual Clauses**"), including any updated, amended, or subsequent version thereof approved by the respective data protection authority.

1.13 **"Swiss DPA"** means the Swiss Data Protection Act, as amended or replaced.

2. DATA PROCESSING AND PROTECTION

This DPA applies when Informatica Processes Customer's data for which Informatica will act as "processor" or "service provider" (or other analogous variations of such terms) under Data Protection Law.

2.1 **Limitations on Use.** Informatica will Process Personal Data only: (a) in a manner consistent with documented instructions from Customer, including (i) to provide the Services, (ii) as permitted under the Agreement, including as specified in Annex I to this DPA, and (iii) consistent with other reasonable instructions of Customer; and (b) with prior notice (unless notice is legally prohibited), as required by applicable law.

2.2 **CCPA Compliance**. Without limiting the foregoing, Informatica will comply with all sections of the CCPA applicable to its role as a service provider and provide the same level of privacy protection as required by the CCPA. Informatica will notify Customer no later than five (5) business days after making a determination that it can no longer meet its obligations under the CCPA. Customer may, upon notice to Informatica, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data. Informatica will not Process the Personal Data for any purpose other than as necessary for the specific purposes of performing the Services or as otherwise expressly permitted for service providers under the CCPA. In particular, Informatica will not sell or share the Personal Data as defined in the CCPA or combine it with any other personal data or information it collects (directly or via any other party) other than as expressly permitted for service providers under the CCPA.

2.3 **Confidentiality.** Informatica will subject persons authorized by Informatica to Process any Personal Data to appropriate confidentiality obligations.

2.4 **Security.** Informatica will protect Personal Data in accordance with requirements under Data Protection Law, including by implementing appropriate technical and organizational measures designed to protect Personal Data against Personal Data Breach per Informatica's Cloud and Support Security Addendum (current copy of which is available here: https://www.informatica.com/content/dam/informatica-com/en/docs/legal/online-cloud-and-support-security-addendum.pdf).

2.5 **Return or Disposal.** At the choice of Customer, Informatica will delete or return (or will enable Customer to delete or retrieve) all Personal Data after the end of the provision of Services (unless applicable law requires Informatica to store any Personal Data, in which case Informatica will continue to protect the Personal Data in accordance with the terms of this DPA).

2.6 **Customer Obligations**. Customer will not instruct Informatica to perform any Processing of Personal Data that violates any Data Protection Law. Informatica may suspend Processing based upon any Customer instructions that Informatica reasonably suspects violate Data Protection Law. Subject to the cooperation of Informatica as specified in this DPA, Customer will be solely responsible for safeguarding the rights of Data Subjects, including determining the adequacy of the security measures in relation to Personal Data and providing any necessary notice to or obtaining any necessary consent from Data Subjects regarding the Processing.

3. DATA PROCESSING ASSISTANCE

3.1 **Data Subject's Rights Assistance.** Taking into account the nature of the Processing of Personal Data by Informatica under the Agreement, Informatica will provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as possible and as necessary, for the fulfilment of Customer's obligations to comply with requests for exercising Data Subject's rights under Data Protection Law with respect to Personal Data solely to the extent Customer does not have the ability to address such Data Subject request without such assistance using functionality provided in the Services. Customer will inform Informatica of any such request and provide any information necessary for Informatica to meet its obligations. Informatica will promptly inform Customer of any Data Subject request relating to Processing of Personal Data that it receives directly from a Data Subject.

3.2 **Security Assistance.** To assist Customer in its efforts to ensure compliance with the security requirements under Data Protection Law, Informatica has made available to Customer its Cloud and Support Security Addendum per section 2.4 above.

3.3 **Data Protection Impact Assessment Assistance**. Taking into account the nature of Informatica's Processing of Personal Data and the information available to Informatica, Informatica will provide reasonable assistance to Customer as required for Customer to comply with its obligations to conduct data protection impact assessments if required under Data Protection Law in connection with Informatica's Processing of Personal Data under the Agreement.

3.4 **Personal Data Breach Notice and Assistance.** Informatica will notify Customer without undue delay after becoming aware of a Personal Data Breach. Taking into account the nature of Processing and the information available to Informatica, Informatica will provide reasonable assistance to Customer as may be necessary for Customer to satisfy any notification obligations required under Data Protection Law related to any Personal Data Breach.

4. AUDITS.

Informatica will make available to Customer all information necessary to demonstrate compliance with its obligations under this DPA and allow for and contribute to audits as follows: (a) once every 12 months, Customer may request to review a summary of Informatica's SOC 2 Type 2 audit report regarding the Processing activities covered by this DPA; (b) Customer or a third party auditor reasonably acceptable to Informatica may take reasonable and appropriate steps to ensure that Informatica uses the Personal Data in a manner consistent with its obligations under Data Protection Law by conducting an on-site audit of Informatica's processing activities as required by a supervisory authority or Data Protection Law. Such on-site audit must (i) be scheduled on at least 45 days advance notice at a mutually agreed date and time; (ii) occur during Informatica's normal business hours; (iii) be permitted only to the extent required to assess Informatica's compliance with this DPA; (iv) comply with the policies, procedures, and other restrictions reasonably imposed by Informatica and, if applicable, the Subprocessor; and (v) not unreasonably interfere with Informatica's business activities. Customer's auditor will not be entitled to access information subject to third-party confidentiality obligations. Customer will provide written communication of any audit findings to Informatica, and the results of the audit will be the confidential information of Informatica.

5. SUBPROCESSORS

Customer authorizes Informatica to use Informatica's Affiliates and third-party subprocessors to Process Personal Data in connection with the provision of Services to Customer ("**Subprocessor**"). Customer may view the list of current Subprocessors at the following link: https://www.informatica.com/legal/informatica-subprocessors.html. Informatica will notify Customer of any intended changes concerning the addition or replacement of its Subprocessors and provide Customer with the opportunity to object to such changes. If Customer reasonably objects to a Subprocessor, Customer must inform Informatica within ten (10) days. If Informatica is unable to resolve Customer's objection, either party may, upon notice and without liability, terminate the Services that use the objected-to Subprocessor. Informatica will impose data protection obligations upon any Subprocessor that are no less protective than those included in this DPA. Informatica shall remain liable to Customer for a Subprocessor's failure to fulfill its data protection obligations.

6. DATA TRANSFERS

Personal Data may be transferred to any country in which Informatica or its Subprocessors maintain facilities. This Section 6 only applies to the transfer of Personal Data from the Member States of the European Economic Area ("EEA"), the United Kingdom, Switzerland, or Brazil to a third country that has not been deemed adequate by the applicable data protection authority. For each applicable version of the Standard Contractual Clauses between Informatica and Customer contemplated in Sections 6.2 and 6.3: (a) Customer and Informatica are deemed to have executed the Standard Contractual Clauses as of the effective date of this DPA; and (b) Customer is the "data exporter" and Informatica is the "data importer. Upon written notice to Customer, Informatica may substitute the Standard Contractual Clauses with an alternative lawful transfer mechanism.

6.1 **Transfers from the EEA.** Informatica will conduct the transfer of Personal Data from the EEA pursuant to the Informatica Processor Binding Corporate Rules accessible on Informatica's website ("the BCRs") at https://www.informatica.com/binding-corporate-rules.html. The BCRs are incorporated by reference into this DPA and enforceable by Customer with respect to Informatica.

6.2 **Transfers from Switzerland and Brazil.** Informatica will conduct the transfer of Personal Data from Switzerland and Brazil pursuant to the EU Standard Contractual Clauses or any other data transfer mechanism permitted under Data Protection Law of each applicable jurisdiction, such as binding corporate rules. With respect to the EU Standard Contractual Clauses, the following apply if Informatica is an entity outside Switzerland or Brazil: (i) Module Two (controller to processor); (ii) Annexes I and II attached hereto; (iii) "Member State" refers to the country from which the Personal Data originates; (iv) "jurisdiction" and "supervisory authority" refer to the respective data protection authority that enforces Data Protection Law; (v) Clause 7; (vi) in Clause 9, option 2 for general written authorization with a time period of thirty days; (vii) in Clause 11, the optional text is not included; (viii) in Clauses 17 and 18, selecting option 2 and specifying Switzerland or Brazil, respectively, for Personal Data subject to the Swiss DPA or the LGPD; and (vii) references to the GDPR and "that Regulation" will be read as references to the relevant provisions of the Swiss DPA or the LGPD. With respect to a transfer from Informatica to a Subprocessor pursuant to the EU Standard Contractual Clauses, Informatica will conduct the transfer under Module Three (processor to processor) and Informatica shall be the "data exporter" and the Subprocessor shall be the "data importer."

6.3 **Transfers from the United Kingdom.** Informatica will conduct the transfer of Personal Data from the UK pursuant to the UK Standard Contractual Clauses or any other data transfer mechanism permitted under UK Data Protection Law, which may include binding corporate rules. With respect to the International Data Transfer Addendum, the following selections and content shall apply: (i) Table 1 shall consist of the content in Sections A-B of Annex I attached hereto; (ii) for Table 2, the Approved EU SCCs are selected with the following modules, clauses, or optional provisions applied: (a) Module Two (controller to processor); (b) Clause 7; (c) in Clause 9, option 2 for general written authorization with a time period of thirty days; and (d) in Clause 11, the optional text is not included; (iii) Table 3 shall consist of the content in Annex I (Sections A-B) and Annex II of this DPA; and (iv) for purposes of Table 4, neither Party may end the Addendum except by mutual agreement.

7. MISCELLANEOUS

If there is a conflict (a) this DPA will prevail over the Master Agreement and (b) the Standard Contractual Clauses and BCRs as applicable will prevail over this DPA. Except for the matters covered by this DPA, all terms of the Master Agreement, remain in effect. Capitalized terms not defined in this DPA have the same meaning as in the Master Agreement. Except as otherwise stated in the Master Agreement, this DPA and the Standard Contractual Clauses will automatically terminate upon the termination or expiration of the Master Agreement.

Annex I - Scope of Processing

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: As specified in the Master Agreement

Address: As specified in the Master Agreement

Contact person's name, position, and contact details: As specified in the Master Agreement

Activities relevant to the data transferred under these Clauses: Customer utilizes the Services specified in the Master Agreement and is responsible for use of the Services in accordance with applicable documentation.

Signature and date: As specified in the Master Agreement

Role (controller/processor): Controller

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

Name: Informatica LLC

Address: 2100 Seaport Blvd., Redwood City, CA 94063

Contact person's name, position and contact details: Joseph Bracken, VP, jbracken@informatica.com for Informatica

Activities relevant to the data transferred under these Clauses: Informatica Processes Personal Data for the subject matter specified under the Master Agreement and until the Master Agreement terminates or expires, unless otherwise agreed upon by the parties in writing. In particular, the subject matter is determined by the Service(s) to which Customer subscribes and the data which Customer uploads to the Service.

Signature and date: As specified in the Master Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer controls the categories of Data Subjects to which the Personal Data relates. For instance, Customer may Process via the Services Personal Data that relates to its current or prospective customers, employees or business partners.

Categories of personal data transferred

Other than in connection with Data-as-a-Service Address Content and Web Services, Customer controls the types of Personal Data uploaded via the Services for Processing. Data-as-a-Service Address Content and Web Services may Process postal addresses, email addresses, and/or telephone numbers, in accordance with the specific Service to which Customer subscribes.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None anticipated, but Customer controls the types of Personal Data processed via the Services.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Customer will determine the frequency of Personal Data transferred but such transfers are anticipated on a continuous basis during the term of the Services provided under the Master Agreement.

Nature of the processing

The nature and purpose of Processing is determined by the Service(s) to which Customer subscribes and the data which Customer uploads to the Service. For instance, the Services constitute providing and improving one or more of the following:

1. Data Integration Cloud Services Process data uploaded to the Service, including Personal Data if uploaded, to connect, transform, and integrate data, applications, and processes across on-premise and cloud systems.

2. Data Management, Quality, and Governance Cloud Services Process data uploaded to the Service, including Personal Data if uploaded, to help Customer understand and enrich data, to help ensure that data are relevant and trustworthy, and to help optimize compliance and business value from data.

3. Infrastructure Hosting Services Process data uploaded to the Service, including Personal Data if uploaded, in accordance with the function performed by the Informatica software product that Informatica is hosting for Customer.

4. Data-as-a-Service Address Content and Web Services (including Address Verification, Email Verification, Global Phone Number Validation, and SMS Alerts and Notifications) Process data uploaded to the Service, including Personal Data if uploaded, to help verify and enrich contact data.

Purpose(s) of the data transfer and further processing

The purpose of Processing is determined by the Service(s) to which Customer subscribes and the data which Customer uploads to the Service.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data exporter will determine the period required for Personal Data to be retained depending on the purpose of Processing. Data importer will return or destroy Personal Data within sixty (60) days after the expiration or termination of Services, unless otherwise required to be retained by applicable law or legal order.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of processing involving Informatica's sub-processors is dependent upon the Service to which the Customer Subscribes. For instance:

- For Cloud Services and Infrastructure Hosting Services, Informatica's sub-processors provide infrastructure services (such as cloud hosted data storage) and process encrypted Personal Data that the Customer uploads for the duration of the Services under the Master Agreement.

- For Data-as-a-Service Address Content and Web Services, Informatica's sub-processors Process Personal Data uploaded by the Customer in order to provide the Services for the duration of the Services under the Master Agreement.

- For professional and support Services, Informatica's sub-processors Process Personal Data if provided by the Customer in order to provide the professional or support Services under the Master Agreement and for the duration of the particular engagement. Personal Data will be deleted from Informatica systems upon termination or expiration of Customer's engagement, as applicable.

C.COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

For Personal Data subject to the Swiss DPA or the LGPD, the competent supervisory authority will be the supervisory authority in Switzerland or Brazil, respectively.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO SECURE THE DATA

Technical and organisational measures to secure the data are described for each Service to which the data exporter subscribes at: https://www.informatica.com/content/dam/informatica-com/en/docs/legal/online-cloud-and-support-security-addendum.pdf.

In addition: (i) Informatica will encrypt all Personal Data in transit; (ii) Informatica represents that it has not, as of the effective date of this DPA, received any requests under Section 702 of the U.S. Foreign Intelligence Surveillance Act that may enable access to the personal data of individuals located within a country in the European Economic Area, and (iii) if Informatica receives a request for any such personal data from any government or law enforcement authority, Informatica will make commercially reasonable efforts to assert available defenses against making the disclosure and will minimize the scope of any legally required disclosure to only that which is necessary to meet the disclosure obligation.