ALTINITY.CLOUD

Data Processing Addendum

This Data Processing Addendum and its Appendixes ("**DPA**") forms part of, and is subject to, the Altinity.Cloud Terms of Service, or other written or electronic terms of service or subscription agreement between Altinity, Inc., a Delaware corporation, ("**Altinity**") and the legal entity defined therein as the "**Customer**" (the "**Agreement**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

This DPA reflects the parties' agreement with respect to the Processing of Personal Data by Altinity, on Customer's behalf, in connection with the Services provided in the Agreement.

This DPA shall be effective on the effective date of the Agreement, unless this DPA is separately executed, in which case it is effective on the date of the last signature ("**Effective Date**").

In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

1. Definitions.

"**Account**" means Customer's account in the Service in which Customer stores and processes Customer Data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorized Affiliate**" shall mean a Customer Affiliate that is (i) permitted to use the Services pursuant to the Agreement, has not signed its own separate agreement with Altinity and are not a "Customer" as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by Altinity, and (iii) are subject to European Data Protection Laws.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Customer Data**" has the meaning set forth in the Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU & UK Data Protection Law and the CCPA.

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

"**EU & UK Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") and (ii) the United Kingdom's Data Protection Act 2018 (as well as any subsequent data protection law enacted by the United Kingdom, such as a version of GDPR).

"**Services**" means the generally available Altinity software-as-a-service offering described in the Documentation and procured by Customer, and any other services provided by Altinity under the Agreement, including but not limited to support and technical services.

"**Personal Data**" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "personal information" in the CCPA.

"**Processing**" shall mean 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 and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) Altinity's provision of the Services under the Agreement, including Processing initiated by Users in their use of the Services, and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.

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

"Standard Contractual Clauses" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Annex A**.** Appendices 1 and 2 of the Standard Contractual Clauses shall be as set forth in this DPA at Section 3.5 (Details of Data Processing) and 5.1 (Security Measures), respectively.

"**Sub-processor**" means any other Data Processors engaged by Altinity to Process Customer Personal Data.

2. Scope and Applicability of this DPA.

This DPA applies where and only to the extent that Altinity Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing the Services.

3. Roles and Scope of Processing.

3.1 **Role of the Parties**. As between Altinity and Customer, Customer is either the Data Controller of Customer Personal Data, or if Customer is acting on behalf of a third-party Data Controller, then a Data Processor, and Altinity shall Process Customer Personal Data only as a Data Processor acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein. To the extent any Usage Data (as defined in the Agreement) is considered Personal Data under applicable Data Protection Laws, Altinity is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2 **Customer Instructions**. Altinity will Process Customer Personal Data only for the Purposes. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Altinity for the Processing of Customer Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between Customer and Altinity.

3.3 **Customer Affiliates.** Altinity's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to Section 12 (Parties to the DPA), and the following conditions:

(a) Customer must communicate any additional Processing instructions from its Authorized Affiliates directly to Altinity; and

(b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer.

3.4 **Customer Processing of Personal Data**.

(a) Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing and backing- up Customer Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for Altinity to lawfully Process Customer Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Customer Personal Data with third-parties via the Services.

(b) In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (including such as particularly for use by Customer for marketing purposes); (iii) ensuring Customer has the right to transfer, or provide access to, the Personal Data to Altinity for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensuring that Customer instructions to Altinity regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws. Customer will inform Altinity without undue delay if it is not able to comply with its responsibilities under this Section 3.4 or applicable Data Protection Laws.

3.5 **Details of Data Processing.**

(a) Subject matter: The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Duration: Notwithstanding expiry or termination of the Agreement, this DPA and Standard Contractual Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: Altinity shall Process Customer Personal Data only for the Purposes.

(d) Nature of the Processing: Altinity provides Services as described in the Agreement.

(e) Categories of Data Subjects: The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors; and/or

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons).

(f) Types of Personal Data: The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);

(ii) Financial information (credit records, account details, payment information);

(iii) Employment details (employer, job title, geographic location, area of responsibility); and/or

(iv) IT information (IP addresses, usage data, cookies data, location data).

(g) Special Categories of Personal Data: The parties do not anticipate the transfer of special categories of data.

4. Sub-processing.

Customer agrees that Altinity may engage Sub-Processors to Process Personal Data on Customer's behalf. Altinity has currently appointed, as Sub-Processors, the third parties listed in Annex B to this DPA. Altinity will notify Customer if it adds or removes Sub-Processors to Annex B prior to any such changes, if Customer opts-in to receive such email notifications by completing the form attached as Annex B-1. Where Altinity engages Sub-Processors, Altinity will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. Altinity will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Altinity to breach any of its obligations under this DPA.

5. Security.

5.1 **Security Measures**. Altinity shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with the Security Measures described in Annex C (the "Security Measures"). Altinity may review and update its Security Measures from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

5.2 **Confidentiality of Processing**. Altinity shall ensure that any person who is authorized by Altinity to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3 **No Assessment of Customer Personal Data by Altinity**. Altinity shall have no obligation to assess the contents of Customer Personal Data to identify information subject to any specific legal requirements. Customer is responsible for reviewing the information made available by Altinity relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6. Customer Audit Rights.

Altinity will make all information reasonably necessary to demonstrate compliance with this DPA available to Customer and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it will exercise its audit rights under this DPA by instructing Altinity to comply with the audit measures described in this Section 6.1. Customer acknowledges that the Service is hosted by Altinity's data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that Altinity's systems are regularly tested by independent third party penetration testing firms. Upon request, Altinity will supply (on a confidential basis) a summary copy of its penetration testing report(s) to Customer so that it can verify Altinity's compliance with this DPA. Further, at Customer's written request, Altinity will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer necessary to confirm Altinity's compliance with this DPA, provided that Customer will not exercise this right more than once per calendar year.

7. Data Transfers

7.1 **Hosting and Processing Locations.** Customer acknowledges and agrees that Altinity may access and Process Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement, and in particular that Personal Data will be transferred to and Processed by Altinity, Inc. in the United States and to other jurisdictions where Altinity, its Affiliates and Sub-Processors have operations. Altinity will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

7.2 **Transfer Mechanisms.** For any transfers by Customer of Customer Personal Data from the European Economic Area and/or its member states, United Kingdom and/or Switzerland (collectively, "**Restricted Countries**") to Altinity in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by a valid mechanism for the lawful transfer of Customer Personal Data recognized under Data Protection Laws, such as those directly below:

(a) **Standard Contractual Clauses (processors):** Altinity agrees to abide by, and Process Customer Personal Data from the Restricted Countries in compliance with the Standard Contractual Clauses which are incorporated into this DPA by reference, and for these purposes Altinity shall be the "data importer" and Customer is the "data exporter" under the Standard Contractual Clauses (notwithstanding that Customer may be an entity located outside of a Restricted Country).

(b) **BCRS.** Notwithstanding the foregoing, if Altinity has adopted Binding Corporate Rules (BCRs) for Processors that cover the transfer of Customer Personal Data to a Third Country, then such BCRs shall govern the transfer of Customer Personal Data.

8. Return or Deletion of Data. Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the Agreement as set forth in the Agreement. Subject to 10.3, any Customer Personal Data not deleted by Customer shall be deleted by Altinity promptly upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement.

9. Security Incident Response.

9.1 **Security Incident Reporting.** If Altinity becomes aware of a Security Incident, Altinity shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware. Altinity shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2 **Security Incident Communications.** Altinity shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Altinity to mitigate or contain the Security Incident, the status of Altinity's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Altinity personnel do not have visibility to the content of Customer Personal Data, it will be unlikely that Altinity can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of Altinity with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Altinity of any fault or liability with respect to the Security Incident.

10. Cooperation.

10.1 **Data Subject Requests.** To the extent legally permitted, Altinity shall promptly notify Customer if Altinity receives a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Customer Personal Data, or to restrict the Processing of Customer Personal Data ("**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to a Data Subject Request and Customer will be responsible for responding to any such Data Subject

Request. To the extent Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, taking into account the nature of the Processing, Altinity shall (upon Customer's written request) provide commercially reasonable cooperation to assist Customer in responding to any Data Subject Requests.

10.2 **Data Protection Impact Assessments.** Altinity shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

10.3 **Government, Law Enforcement, and/or Third Party Inquiries.** If Altinity receives a demand to retain, disclose, or otherwise Process Customer Personal Data for any third party, including, but not limited to law enforcement or a government authority ("**Third-Party Demand**"), then Altinity shall attempt to redirect the Third-Party Demand to Customer. Customer agrees that Altinity can provide information to such third party as reasonably necessary to redirect the Third-Party Demand. If Altinity cannot redirect the Third-Party Demand to Customer, then Altinity shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy.

11. Relationship with the Agreement.

11.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment or exhibit (including the Standard Contractual Clauses (as applicable)) that Altinity and Customer may have previously entered into in connection with the Services.

11.2 Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state health care laws, rules or regulations ("**HIPAA Data**"), if there is any conflict between this DPA and a business associate agreement between Customer and Altinity ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

11.3 Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, the Standard Contractual Clauses, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by the one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

11.4 In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

11.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

12. Parties to this DPA

12.1 **Permitted Affiliates.** By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of Customer's Authorized Affiliates, thereby establishing a separate DPA between Altinity and each such Authorized Affiliates subject to the Agreement and the 'General Provisions' and 'Parties to this DPA' sections of this DPA. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the purposes

of this DPA only, and except where indicated otherwise, the terms "Customer" will include Customer and such Authorized Affiliates.

12.2 **Authorization**. The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Authorized Affiliates.

12.3 **Remedies**. Except where applicable Data Protection Laws require an Authorized Affiliates to exercise a right or seek any remedy under this DPA against Altinity directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Authorized Affiliates may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Customer together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Altinity under the DPA and will be entitled to make and receive any communication related to this DPA on behalf of its Authorized Affiliates.

12.4 **Other Rights.** The parties agree that Customer will, when reviewing Altinity's compliance with this DPA pursuant to the Section 6 (Customer Audit Rights), take all reasonable measures to limit any impact on Altinity and its Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Authorized Affiliates in one single audit.

Annex A
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

THE PARTIES HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to

exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal

data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities

covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("**DPA**").

Data importer*:* The data importer is Altinity, as defined in the DPA. Altinity provides enterprise cloud computing solutions, which process Customer Personal Data upon the instruction of the Customer in accordance with the terms of the Agreement.

Description of Data Processing: Please see Section 3.5 (Details of Processing) of the DPA for a description of the categories of data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Annex C of the DPA, which describes the technical and organizational security measures implemented by Altinity.

Annex B
List of Sub-processors

Sub-Processor	Purpose	Location
Amazon Web Services, Inc.	Hosting & Infrastructure for management plane (Altinity Cluster Manager)	United States
Amazon Web Services, Inc	Hosting & Infrastructure of data plane used for Processing (Customer data warehouses)	Determined by location of Amazon selected by user.
Auth0, Inc	Authentication for access to management plane	United States
Google, Inc	Email to users as well as authentication to management plane	United States

Annex B-1

Request for notification of changes to List of Sub-processors

Annex C

Security Measures

This Annex forms part of the DPA.

Altinity currently observe the Security Measures described in this Annex C. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Master Terms.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems hosted by infrastructure provider(s) and accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

Data isolation: Customer data warehouses (data plane) are located in isolated environments for each Customer with dedicated storage, compute, and network resources.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

b) Transmission Control

In-transit: We apply HTTPS encryption (also referred to as TLS) available on all interfaces and for free on every customer site hosted on the Altinity products. Our HTTPS implementation uses industry standard encryption protocols and valid certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We provide the option for users to select at rest encryption for all data warehouse data. Users must select this option at cluster launch time.

c) Input Control
Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to Customer will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is replicated across availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 2 replicas. All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.