HOSTED SERVICE DATA PROCESSING ADDENDUM (EU/EEA/UK)

This Data Processing Addendum ("Addendum"), including its Schedules and Appendices, made and entered into by and between MicroStrategy [relevant EU/EEA/UK MicroStrategy entity] ("we," "us," "our", "MicroStrategy"), and the entity identified as "Customer" in the signature block below ("you," "your", "Customer"), supplements and amends the order(s) and, as applicable, the master agreement between you and us (collectively, the "Governing Agreement") that governs your use of our Cloud hosted service ("Hosted Service"). In the event of a conflict between any provision of the Governing Agreement relating to data processing activities (including any existing data processing addendums to the Governing Agreement) and any provision of this Addendum, the provision of this Addendum will prevail. In all other respects the Governing Agreement will remain in full force and effect.

By signing the Addendum, Customer enters into this Addendum on behalf of itself and, to the extent applicable, on behalf of members of its Customer Group. For the purposes of this Addendum only, and except where indicated otherwise, the term "Customer" shall include where applicable Customer Group.

1. Definitions.

"**Applicable Data Protection Law**" means all applicable laws and regulations where these apply to MicroStrategy, its group and third parties who may be utilized in respect of the performance of the Hosted Service relating to the processing of personal data and privacy, including, without limitation, the General Data Protection Regulation (EU) 2016/679, the United Kingdom General Data Protection Regulation and the California Consumer Protection Act (Cal. Civ. Code §§ 1798.100 *et. seq.*) (CCPA), as amended and expanded by the California Privacy Rights Act (CPRA). The terms "**Controller**," "**Commissioner**", **"Business," "Processor**," "**Data Subject,**" **"Service Provider," "Data Protection Supervisory Authority,**" "**process**," "**processing,**" and "**personal data**" shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

"**Customer Group**" means you and any affiliate, subsidiary, subsidiary undertaking and holding company of Customer (acting as a Controller) accessing or using the Hosted Service on Customer's behalf or through Customer's systems or any other third party who is permitted to use the Hosted Services pursuant to the Governing Agreement between Customer and MicroStrategy, but who has not signed its own Order Form with MicroStrategy.

"**International Transfer**" means a transfer of personal data from a country within the European Union (EU), European Economic Area (EEA) or Switzerland or the United Kingdom (UK) (both countries not in the EEA or the EU) to a country or territory not recognized by the European Commission, Switzerland or the United Kingdom as providing an adequate level of protection for personal data or subject to any requirement to take additional steps to adequately protect personal data.

"**EU Standard Contractual Clauses**" means Module 3 of those clauses comprised within the European Commission Decision (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries under Regulation 2016/679, as may be updated, supplemented or replaced from time to time under Applicable Data Protection Law.

"**Sub-Processor**" means any third party appointed by MicroStrategy to process personal data.

"**UK Addendum**" means the addendum to the EU Standard Contractual Clauses for the transfer of personal data to third countries compliant with Applicable Data Protection Laws applicable in the UK, which has Module 3 of the EU Standard Contractual Clauses incorporated and engaged by reference.

2. Data Processing. As a Processor, we will process personal data that is uploaded or transferred to the Hosted Service as instructed by you or provided by you as Controller (collectively, "Customer Data") in accordance with your documented instructions. Customer authorizes MicroStrategy on its own behalf and on behalf of the other members of its Customer Group to process Customer Data during the term of this Agreement as a Processor for the purpose set out in Schedule 1.

The parties agree that this Addendum is your complete and final documented instruction to MicroStrategy in relation to Customer Data. Additional instructions outside the scope of this Addendum (if any) require prior written agreement between MicroStrategy and you, including agreement on any additional fees payable by you to MicroStrategy for carrying out such instructions. You are entitled to terminate this Addendum if MicroStrategy declines to follow reasonable instructions requested by you that are outside the scope of, or changed from, those given or agreed to be given in this Addendum. You shall ensure that your instructions comply with all laws, rules and regulations applicable in relation to Customer Data, and that the processing of Customer Data in accordance with your instructions will not cause MicroStrategy to be in breach of Applicable Data Protection Law and/or this Addendum or applicable agreements with Sub-Processors, including EU Standard Contractual Clauses and UK Addendum. We will not process Customer Data outside the scope of this Addendum.

MicroStrategy will:

a) process Customer Data only on documented instructions from Customer (unless MicroStrategy or the relevant Sub-Processor (see Section 4 below) is required to Process Customer Data to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal requirement prior to such processing unless such applicable laws prohibit notice to Customer on public interest grounds);

b) promptly inform Customer if, in its reasonable opinion, any instruction received from Customer infringes Applicable Data Protection Law;

c) ensure that any individual authorized by MicroStrategy to process Customer Data complies with Section 2a) above; and

d) at the option of Customer, delete or return to Customer all Customer Data after the end of the provision of the Hosted Service relating to processing, and delete any remaining copies. MicroStrategy will be entitled to retain any Customer Data which it has to keep to comply with any applicable law or which it is required to retain for insurance, accounting, taxation or record keeping purposes. Section 3 will continue to apply to retained Customer Data.

MicroStrategy will not "sell" Customer Data as that term is defined in the CCPA, nor will it retain, use, or disclose Customer Data for any purpose other than for the specific purpose of performing the services specified in the Governing Agreement, or as otherwise permitted by the CCPA or its implementing regulations. MicroStrategy certifies that it understands the restrictions and obligations under the CCPA, including the restrictions and obligations in the previous sentence, and will comply with CCPA. In addition, MicroStrategy will comply with any applicable amendments to the CCPA or its regulations.

3. Confidentiality. MicroStrategy will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a government or law enforcement agency (such as a subpoena or court order). If a government or law enforcement agency sends MicroStrategy a demand for Customer Data, MicroStrategy will attempt to redirect the government or law enforcement agency to request that data directly from you. As part of this effort, MicroStrategy may provide your basic contact information to the government or law enforcement agency. If compelled to disclose Customer Data to a government or law enforcement agency, then MicroStrategy will give you reasonable notice of the demand to allow you to seek a protective order or other appropriate remedy, unless MicroStrategy is legally prohibited from doing so. MicroStrategy restricts its personnel from processing Customer Data without authorization by MicroStrategy, and imposes appropriate contractual obligations upon its personnel, including, as appropriate, relevant obligations regarding confidentiality, data protection and data security. If the EU Standard Contractual Clauses or UK Addendum apply, nothing in this section 3 varies or modifies the EU Standard Contractual Clauses or UK Addendum, including without limitation the obligations within clause 5(a).

4. Sub-Processing. Customer provides general authorization to MicroStrategy to engage its own affiliated companies for the purposes of providing the Hosted Service and to use Sub-Processors to fulfill its contractual obligations under this Addendum or to provide certain services on its behalf.

The MicroStrategy website at https://community.microstrategy.com/s/article/GDPR-Cloud-Sub-Processors lists its Sub-Processors appointed by MicroStrategy that are currently engaged to carry out specific processing activities on behalf of Customer. Customer hereby consents to MicroStrategy's use of Sub-Processors as described in this Section 4. Before MicroStrategy engages any new Sub-Processor to carry out specific processing activities on behalf of Customer, MicroStrategy will update the applicable website. If Customer objects to a new Sub-Processor, Customer shall inform MicroStrategy in writing within thirty (30) days following the update of the applicable Sub-Processors list and such objection shall describe Customer's legitimate reasons for objection. If Customer objects to the use of a new Sub-Processor pursuant to the process provided under this Section, MicroStrategy will not engage such Sub-Processor to carry out specific processing activities on behalf of Customer without Customer's written consent. Further, MicroStrategy shall have the right to cure any objection by, in its sole discretion, either choosing to a) take any corrective steps requested by Customer in its objection (which steps will be deemed to resolve Customer's objection) and proceed to use the Sub-Processor or b) suspend and/or terminate any product or service that would involve the use of the Sub-Processor.

If MicroStrategy appoints a Sub-Processor, MicroStrategy will (i) restrict the Sub-Processor's access to Customer Data only to what is necessary to provide the Hosted Service to Customer and will prohibit the Sub-Processor from accessing Customer Data for any other purpose; (ii) will enter into a written agreement with the Sub- Processor; (iii) to the extent the Sub-Processor is performing the same data processing services that are being provided by MicroStrategy under this Addendum, impose on the Sub-Processor substantially similar terms to those imposed on MicroStrategy in this Addendum; and (iv) comply with the EU Standard Contractual Clauses and/or UK Addendum (where applicable) which separately contain obligations in respect of the terms to be imposed in respect of an onward transfer of Personal Data to a Sub-Processor. MicroStrategy will remain responsible to the Customer for performance of the Sub-Processor's obligations.

5. Transfers of Personal Data by Region. With respect to Customer Data containing personal data that is uploaded or transferred to the Hosted Service, you may specify the geographic region(s) where that Customer Data will be processed within our Sub-Processor's network (*e.g.*, the EU-Dublin region). A Sub-Processor will not transfer that Customer Data from your selected region except as necessary to maintain or provide the Hosted Service, or as necessary to comply with a law or binding order of a law enforcement agency.

To provide the Hosted Service, Customer acknowledges and confirms MicroStrategy may make International Transfers of Customer Data, including onward transfers to its affiliated companies and/or Sub-Processors. MicroStrategy has signed (as data exporter) with its Sub-Processors (as data importers) (i) a copy of the EU Standard Contractual Clauses and where applicable (ii) a copy of the UK Addendum to safeguard those International Transfers which occur.

In the event that the form of the EU Standard Contractual Clauses or UK Addendum is changed or replaced by the relevant authorities under Applicable Data Protection Law, MicroStrategy shall complete the updated form and notify the Customer as Controller of such form. Provided that such form is accurate and applicable to MicroStrategy as Processor, such form shall then be binding upon the parties (which may include the Customer and/ or Sub-Processor dependent on the change/ revised document) when the relevant parties have executed the revised form, subject to the expiration of a grace period, if any, determined by the relevant supervisory authorities. If the Customer does not enter to and execute the EU Standard Contractual Clauses or UK Addendum, where it is required to do so under Applicable Data Protection Law (either out of a failure to provide the appropriate form or because, in MicroStrategy's sole discretion, Customer is unreasonably withholding, delaying or conditioning execution of such form), upon notification from MicroStrategy, MicroStrategy shall in any event have the right to suspend and/or terminate any product or service requiring the International Transfer of Customer Data upon giving 30 (thirty) days of written notice.

For International Transfers which are subject to the Applicable Data Protection Law of Switzerland, MicroStrategy shall include the additional clauses below which shall be added as an annex to the EU Standard Contractual Clauses:

1. "The term EU Member State in this Addendum shall always include the EEA Member Countries and Switzerland";

2. "The data transfer is subject to the provisions of the GDPR. The provisions of the Swiss Data Protection Act are additionally applicable on a secondary basis."

3. "With regard to data transfers of personal data from Switzerland, the Federal Data Protection and Information Commissioner is the competent supervisory authority."

4. "Pursuant to the current Swiss Data Protection Act and until the revised Swiss Data Protection Act enters into force, the term personal data with respect to Switzerland also includes the data of legal entities and not only of natural persons."

Notwithstanding the foregoing, the EU Standard Contractual Clauses and/or UK Addendum (or obligations the same as those under the EU Standard Contractual Clauses or the UK Addendum) will not apply if MicroStrategy has adopted an alternative recognized compliance standard for the lawful transfer of personal data outside the EU, EEA, UK or Switzerland, to protect Customer Data.

In respect of other International Transfers outside of those covered by the EU Standard Contractual Clauses or the UK Addendum, MicroStrategy will only make a transfer of Customer Data if:

a) adequate safeguards are in place for that transfer of Customer Data in accordance with Applicable Data Protection Law, in which case Customer will execute any documents (including without limitation EU Standard Contractual Clauses, the UK Addendum, or other such accepted transfer mechanism) relating to that International Transfer, which MicroStrategy or the relevant Sub-Processor reasonably requires it to execute from time to time; or

b) MicroStrategy or the relevant Sub-Processor is required to make such an International Transfer to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal requirement prior to such International Transfer unless such applicable laws prohibit notice to Customer on public interest grounds; or

c) otherwise lawfully permitted to do so by Applicable Data Protection Law.

6. Security of Data Processing. MicroStrategy has implemented and will maintain appropriate technical and organizational measures, including, as appropriate,

a) security of the MicroStrategy network;

b) physical security of the facilities;

c) measures to control access rights for MicroStrategy employees and contractors in relation to the MicroStrategy network; and

d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by MicroStrategy.

You may elect to implement appropriate technical and organizational measures in relation to Customer Data, directly from our Sub-Processor. Such appropriate technical and organizational measures include:

a) pseudonymisation and encryption to ensure an appropriate level of security;

b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services provided by you to third parties;

c) measures to allow you to backup and archive appropriately to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

d) processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by you.

7. Security Breach Notification. We will, to the extent permitted by law, notify Customer without undue delay after becoming aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data by us or our Sub-Processor(s) (a "Security Incident"). To the extent such a Security Incident is caused by a violation of the requirements of this Addendum by us, we will make reasonable efforts to identify and remediate the cause of such breach, including steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

You agree that an unsuccessful Security Incident will not be subject to this Section 7. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of MicroStrategy's or MicroStrategy's Sub-Processor's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents; and MicroStrategy's obligation to report or respond to a Security Incident under this Section 7 is not and will not be construed as an acknowledgement by MicroStrategy of any fault or liability of MicroStrategy with respect to the Security Incident.

Notification(s) of Security Incidents, if any, will be delivered to Customer by any means MicroStrategy selects, including via email. It is your sole responsibility to ensure that you provide us with accurate contact information and secure transmission at all times.

The information made available by MicroStrategy is intended to assist you in complying with your obligations under Applicable Data Protection Law in respect of data protection impact assessments and prior consultation.

8. Audit. MicroStrategy will allow for and contribute to audits (including those under the EU Standard Contractual Clauses or UK Addendum where these apply), which may include inspections, conducted by Customer or another auditor mandated by Customer, provided that Customer gives MicroStrategy at least 30 days' reasonable prior written notice of such audit and that each audit is carried out at Customer's cost, during business hours, at MicroStrategy nominated facilities, and so as to cause the minimum disruption to MicroStrategy's business and without Customer or its auditor having any access to any data belonging to a person other than Customer. Any materials disclosed during such audits and the results of and/or outputs from such audits will be kept confidential by Customer. Such audit shall be performed not more than once every 12 months and Customer shall not copy or remove any materials from the premises where the audit is performed.

Customer acknowledges and agrees (having regard to Section 4(iii)) that in respect of our auditing rights of our Sub-Processor providing infrastructure services for the Hosted Service, such Sub-Processor will use external auditors to verify the adequacy of security measures including the security of the physical data centers from which the Sub-Processor provides the Services. This audit: will be performed at least annually, according to ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001, by independent third party security professionals at the Sub- Processor's selection and expense, and will result in the generation of an audit report ("Report"), which will be the Sub-Processor's confidential information or otherwise be made available subject to a mutually agreed upon non-disclosure agreement covering the Report ("NDA"). MicroStrategy will not be able to disclose such Report to Customer without permission from the Sub-Processor. At Customer's written request during the exercise of its audit rights under Section 8, MicroStrategy will request the permission of the Sub-Processor to provide Customer with a copy of the Report so that Customer can reasonably verify the Sub-Processor's compliance with its security obligations. The Report will constitute confidential information and the Sub-Processor may require Customer to enter into an NDA with them before releasing the same.

If the EU Standard Contractual Clauses or UK Addendum apply under Section 5(a), then Customer agrees to exercise its audit and inspection right by instructing MicroStrategy to conduct an audit as described in this Section 8, and the parties agree that notwithstanding the foregoing nothing varies or modifies the EU Standard Contractual Clauses or UK Addendum nor affects any Data Protection Supervisory Authority's, the Commissioner's or data subject's rights under those EU Standard Contractual Clauses or UK Addendum.

9. Independent Determination. You are responsible for reviewing the information made available by MicroStrategy and its Sub-Processor relating to data security and making an independent determination as to whether the Hosted Service meets your requirements and legal obligations as well as your obligations under this Addendum.

10. Data Subject Rights. Taking into account the nature of the Hosted Service, you can utilize certain controls, including security features and functionalities, to retrieve, correct, delete, or restrict Customer Data. MicroStrategy will provide reasonable assistance to Customer (at Customer's cost) in:

a) complying with its obligations under the Applicable Data Protection Law relating to the security of processing Customer Data;

b) responding to requests for exercising Data Subjects' rights under the Applicable Data Protection Law, including without limitation by appropriate technical and organizational measures, insofar as this is possible;

c) documenting any Security Incidents and reporting any Security Incidents to any Data Protection Supervisory Authority (including the Commissioner) and/or Data Subjects;

d) conducting privacy impact assessments of any processing operations and consulting with supervisory authorities, Data Subjects and their representatives accordingly; and

e) making available to Customer information necessary to demonstrate compliance with the obligations set out in this Addendum.

11. Customer Group Authorization. Where the Customer is entering into and executing the Addendum on behalf of members of its Customer Group, the Customer warrants that it has it has full capacity and authority to do so and shall indemnify, and keep indemnified, MicroStrategy against any and all claims, costs, damages and expenses (including, without limitation, legal costs on a full indemnity basis) incurred by MicroStrategy arising out of and/or in connection with a breach of the warranties contained in this Section 11. The terms of this Addendum shall apply as between MicroStrategy and relevant members of the Customer Group subject to the provisions of the Governing Agreement.

The parties agree that the Customer that is the contracting party to the Governing Agreement and this Addendum shall, to the fullest extent permissible under applicable law, have the sole right to exercise any rights or remedies available under this Addendum for itself and/or jointly on behalf of any or all of the members of its Customer Group – acting as their single nominated representative and the Customer warrants on behalf of the Customer Group that the Customer Group shall only exercise their respective rights through the Customer as their single nominated representative.

12. Limitation of Liability. The cumulative aggregate liability of us and all of our affiliates and licensors to you the Customer and all of your Customer Group related under the Governing Agreement whether in contract tort or otherwise, will not exceed the amount of the fees paid or payable to us in the twelve (12) months immediately preceding the claim. In no event will we or any of our affiliates or licensors be liable to you or any of your Customer Group for any indirect, special, incidental, punitive, consequential, or exemplary damages, whether in contract, tort or otherwise, even if we or any of our affiliates or licensors have been advised of the possibility of such damages and even if an agreed remedy fails of its essential purpose or is held unenforceable for any other reason. Subject to the foregoing, our maximum liability for each claim made by you to the extent the claim arises from or is based upon the use of a third party solution, will not exceed the amount of the applicable third party solution provider's liability to us related in the claim. The parties agree that if MicroStrategy as Processor is held liable for damages for breaches of Applicable Data Protection Law, and/or this Addendum or applicable agreements with Sub-Processors, including EU Standard Contractual Clauses and UK Addendum, MicroStrategy shall be entitled to claim back from the Customer that part of the compensation corresponding to the Customer's responsibility for the damage.

13. Termination of the Addendum. This Addendum shall continue in force until the termination of the Governing Agreement (the "Termination Date").

14. Return or Deletion of Customer Data. Due to the nature of the Hosted Service, our Sub-Processor provides you with controls that you may use to retrieve or delete Customer Data. Up to the Termination Date, you will continue to have the ability to retrieve or delete Customer Data in accordance with this Section 14. For 90 days following the Termination Date, you may retrieve or delete any remaining Customer Data from the Hosted Service, subject to the terms and conditions set out in the Governing Agreement, unless (i) it is prohibited by law or the order of a governmental or regulatory body, (ii) it could subject MicroStrategy or its Sub-Processors to liability, or (iii) you have not paid all amounts due under the Governing Agreement. No later than the end of this 90-day period, you will close all MicroStrategy accounts. MicroStrategy will delete Customer Data when requested by you through the Hosted Service controls provided for this purpose.

Except as amended by this Addendum, the Governing Agreement will remain in full force and effect.

ACCEPTED AND AGREED TO BY:

MicroStrategy [enter relevant MicroStrategy entity] (We/Us/Our)

_____

Name _____
Title _____
Date: _____

Customer: _____ (You/Your)

_____

Name: _____
Title: _____
Date: _____

SCHEDULE 1

Customer Data in relation to Hosted Service

Subject matter of Processing	Storage of data, including without limitation Personal Data, provided by the Customer for its business purposes.
Duration of Processing	Subscription Term and 90 days following expiry of such term.
Nature of Processing	Storage, back-up and recovery and processing in connection with the provision of the Hosted Service.
Purpose of Processing	Provision of the Hosted Service.
Type of Personal Data	The Customer Data uploaded or transferred for processing through the Hosted Service by the Customer.
Categories of Data Subject	Employees or agents of the Customer; and Customer's customers, prospects, business partners and vendors and those individuals who have been authorized to use the Hosted Service by the Customer.