HOSTED SERVICE DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum"), made and entered into by and between MicroStrategy [Services Corporation] [or enter relevant EU 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 and any provision of this Addendum, the provision of this Addendum will prevail.

1. Definitions.

"**Applicable Data Protection Law**" shall include and mean 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 terms "**Data Controller**," "**Data Processor**," "**Data Subject,**" "**Supervisory Authority,**" "**process**," "**processing,**" and "**personal data**" shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

"**Customer's Group**" shall include and mean you and any subsidiary, subsidiary undertaking and holding company of Customer.

"**International Transfer**" shall include and mean a transfer from a country within the European Economic Area (EEA) (including the UK following its exit from the European Union) to a country outside the EEA (as it is made up from time to time) of personal data which is undergoing processing or which is intended to be processed after transfer.

"**Sub-Processor**" shall include and mean the processing of personal data in connection with the Hosted Service, and any other third party appointed by MicroStrategy to process personal data shall be referred to as a "Sub-Processor".

2. Data Processing. As a Data Processor, we will process personal data that is uploaded or transferred to the Hosted Service as instructed by you or provided by you as Data 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's Group to process Customer Data during the term of this Agreement as a Data 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. 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) immediately inform Customer in writing if, in its reasonable opinion, any instruction received from Customer infringes any Applicable Data Protection Law;

c) ensure that any individual authorized to process Customer Data complies with Section 2a); 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.

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 law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends MicroStrategy a demand for Customer Data, MicroStrategy will attempt to redirect the law enforcement agency to request that data directly from you. As part of this effort, MicroStrategy may provide your basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a 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.

4. Sub-Processing. Customer authorizes MicroStrategy to engage its own affiliated companies for the purposes of providing the Hosted Service. In addition, Customer agrees that MicroStrategy may 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 that are currently engaged to carry out specific processing activities on behalf of Customer. 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, MicroStrategy will not engage such Sub-Processor to carry out specific processing activities on behalf of Customer without Customer's written consent. Customer hereby consents to MicroStrategy's use of Sub-Processors as described in this Section 4. Except as set forth in this Section 4, or as Customer may otherwise authorize, MicroStrategy will not permit any Sub-Processor to carry out specific processing activities on behalf of Customer. 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 and; (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. MicroStrategy will remain responsible to 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. The adequate safeguard MicroStrategy has in place for transfers from the EU to the US is the EU – US Privacy Shield Framework. MicroStrategy Incorporated and MicroStrategy Services Corporation have certified compliance with the EU – US Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of EU personal information transferred to the United States. Where MicroStrategy makes an International Transfer, it shall do so via the use of the EU-US Privacy Shield Framework, which will apply to all transfers between MicroStrategy EU entities and MicroStrategy U.S. entities and third parties used by MicroStrategy as part of the provision of the Hosted Service. Any transfers from the United States to any third-party countries will be considered an "onward transfer" under the EU – US Privacy Shield Framework. Where MicroStrategy makes an onward transfer to a third party it will ensure a contract is in place with that party which satisfies the onward transfer accountability requirements of the EU – US Privacy Shield Framework.

In respect of other International Transfers, 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 standard contractual clauses) 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 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, (b) will be performed according to ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at the Sub-Processor's selection and expense; and (d) 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 standard contractual clauses 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 standard contractual clauses nor affects any supervisory authority's or data subject's rights under those clauses.

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 supervisory authority and/or Data Subjects as;

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

12. **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 12. 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 EU MicroStrategy entity] (We/Us/Our)	**Customer: _____ (You/Your)**
_____	_____
Name _____	Name: _____
Title _____	Title: _____
Date: _____	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.
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 for processing through the Hosted Service by the Customer.
Categories of Data Subject	Employees of the Customer; and Customer's customers, prospects, business partners and vendors and employees or agents of the Customer, including those who have been authorized to use the Hosted Service.

EXHIBIT A

Terms specific to Personal Information covered under the California Consumer Privacy Act

In the event that you provide us with access to Personal Information as such is defined in Title 1.81.5 California Consumer Privacy Act of 2018 ("CCPA"), the following additional terms of this Data Processing Addendum will apply. The terms "Business," "Personal Information" and "Service Provider" shall be construed in accordance with their meanings as defined in the CCPA. As a Service Provider, we will use Personal Information that is uploaded or transferred to the Hosted Service by you as a Business in accordance with your documented instructions. You authorize us to use Personal Information during the term of this Agreement for the purpose set out in Schedule 1. MicroStrategy will not sell Personal Information, retain, use, or disclose Personal Information 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 hereby certifies that it understands and will comply with the aforementioned restrictions.