# DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of and is incorporated into the existing agreement governing the use of our Products and Services (the "**Agreement**") between [relevant legal MicroStrategy entity] ("**Strategy**" or "we") and _____("**Customer**") (together, the "**Parties**"). This DPA sets forth Customer's instructions for the processing of Personal Data in connection with the services provided under the Agreement (the "**Services**") and the rights and obligations of both Parties. Except as expressly set forth in this DPA, the Agreement shall remain unmodified and in full force and effect. In the event of any conflicts between this DPA and the Agreement, this DPA will govern to the extent of the conflict.

1. **Definitions**. For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalized terms used but not defined in this DPA shall have the meanings given in the Agreement. All other terms in this DPA not otherwise defined in the Agreement shall have the corresponding meanings given to them in Privacy Laws.

    a. "**Customer Group**" means you and any affiliate, 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 third party who is otherwise permitted to use the Hosted Services pursuant to the Agreement, but who has not entered into a separate order form or agreement with Strategy.

    b. "**Data Privacy Framework**" means, as relevant, (i) the EU-US Data Privacy Framework as administered by the US Department of Commerce and approved by the European Commission as ensuring an adequate level of protection for Personal Data for the purposes of Article 45 GDPR; (ii) the UK Extension to the EU-US Data Privacy Framework approved by the competent authority of the United Kingdom as ensuring an adequate level of protection for Personal Data for the purposes of Article 45 UK GDPR; and (iii) the Swiss-US Data Privacy Framework as administered by the US Department of Commerce and approved by the Swiss Federal Administration as ensuring an adequate level of protection for Personal Data for the purposes of applicable Swiss data protection laws, in each case as in force, amended, consolidated, re-enacted or replaced from time to time.

    c. "**EU/UK Privacy Laws**" means, as applicable: (a) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018, the UK General Data Protection Regulation as defined by the UK Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the UK Data Protection Act 2018, the "**UK GDPR**"), and the Privacy and Electronic Communications Regulations 2003; and (d) any relevant law, directive, order, rule, regulation or other binding instrument which implements any of the above, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

    d. "**Personal Data**" means any information Strategy processes on behalf of Customer to provide the Services that is defined as "personal data" or "personal information" under any Privacy Law.

    e. "**Privacy Laws**" means, as applicable, EU/UK Privacy Laws, US Privacy Laws and any similar law of any other jurisdiction which relates to data protection, privacy or the use of Personal

Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

f. "**Security Incident**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Personal Data. For the avoidance of doubt, an unsuccessful attempt that does not result in the unauthorized access to Personal Data or to any of Strategy's or Strategy's sub-processor's equipment or facilities storing Personal Data including, 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 shall not be considered a Security Incident.

g. "**Third Country**" means any country or territory outside of the scope of the data protection laws of the European Economic Area or the UK, as relevant; that has not been approved as providing adequate protection for Personal Data by the relevant competent authority from time to time.

h. "**US Privacy Laws**" means, as applicable, the California Consumer Privacy Act, Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Florida Digital Bill of Rights, Indiana Consumer Data Protection Act, Iowa Consumer Data Protection Act, Montana Consumer Data Privacy Act, Oregon Consumer Privacy Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act, and any similar law of any other state related to the processing of Personal Data.

2. **Amendments**. The Parties agree to negotiate in good faith modifications to this DPA if changes are required for Strategy to continue to process the Personal Data as contemplated by the Agreement or this DPA in compliance with Privacy Laws, or to address the legal interpretation of the Privacy Laws.

3. **Roles of the Parties**. The Parties acknowledge that for purposes of Privacy Laws, Customer is the "controller," "business," or any similar term provided under Privacy Laws, and Strategy is the "service provider," "processor," "contractor," or any similar term provided under Privacy Laws.

4. **Details of Processing**. The Parties agree that the details of processing are as described in Annex 1.

5. **Customer Obligations**. Customer shall comply with all Privacy Laws in providing Personal Data to Strategy in connection with the Services. Customer represents and warrants that: (a) the Privacy Laws applicable to Customer do not prevent Strategy from fulfilling the instructions received from Customer and performing Strategy's obligations under this DPA; (b) all Personal Data was collected and at all times processed and maintained by or on behalf of Customer in compliance with all Privacy Laws, including with respect to any obligations to provide notice to and/or obtain consent from individuals; and (c) Customer has a lawful basis for disclosing the Personal Data to Strategy and enabling Strategy to process the Personal Data as set out in this DPA. Customer shall notify Strategy without undue delay if Customer makes a determination that the processing of Personal Data under the Agreement does not or will not comply with Privacy Laws, in which case, Strategy shall not be required to continue processing such Personal Data.

6. **Processing of Personal Data**. In processing Personal Data under the Agreement, Strategy shall:

a. only process Personal Data on documented instructions from Customer which the Parties agree that this DPA is Customer's complete and final documented instruction to Strategy in relation

to Personal Data (which the parties agree are reflected in full in this DPA), for the limited and specific purpose described in Annex 1, and at all times in compliance with Privacy Laws, unless required to process such Personal Data by applicable law to which Strategy is subject; in such a case, Strategy shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b. notify Customer without undue delay if it: (i) makes a determination that it can no longer meet its obligations under applicable US Privacy Laws or (ii) believes that instruction of Customer, infringes applicable Privacy Laws;

c. to the extent required by Privacy Laws, and upon reasonable written notice that Customer reasonably believes Strategy is using Personal Data in violation of Privacy Laws or this DPA, grant Customer the right to take reasonable and appropriate steps to help ensure that Strategy uses the Personal Data in a manner consistent with Customer's obligations under Privacy Laws, and stop and remediate any unauthorized use of the Personal Data; and

d. require that each employee or other person processing Personal Data is subject to an appropriate duty of confidentiality with respect to such Personal Data.

7. **Anonymized Data**. Strategy may aggregate and/or anonymize Personal Data such that it no longer constitutes Personal Data under Privacy Laws and process such data for its own purposes. To the extent Strategy receives de-identified data (as such term is defined under applicable US Privacy Laws) from Customer, Strategy shall: (i) take commercially reasonable measures to ensure that the data cannot be associated with an identified or identifiable individual; (ii) publicly commit to maintain and use the data only in a de-identified form and not attempt to re-identify the data; and (iii) otherwise comply with applicable US Privacy Laws with respect to such de-identified data. Customer will take all measures possible to avoid transferring or providing us any access to any Personal Data to the extent possible while continuing using the Services.

8. **Prohibitions**. To the extent required by applicable US Privacy Laws, and except to the extent permitted by such US Privacy Laws, Strategy is prohibited from:

a. selling the Personal Data or sharing the Personal Data for cross-context behavioral advertising purposes;

b. retaining, using, or disclosing the Personal Data outside of the direct business relationship between Strategy and Customer and for any purpose other than for the specific purpose of performing the Services; and

c. combining the Personal Data received from, or on behalf of, Customer with any Personal Data that may be collected from Strategy's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Privacy Laws.

9. **Use of Sub-processors**. To the extent Strategy engages any subcontractors to process Personal Data on its behalf:

a. Customer hereby grants Strategy general written authorization to engage the sub-processors set out on the Strategy's website, currently at: https://community.microstrategy.com/s/article/GDPR-Cloud-Sub-Processors, https://community.microstrategy.com/s/article/GDPR-Technical-Support-Sub-Processors and

https://community.microstrategy.com/s/article/GDPR-Consulting-Sub-Processors (as such website addresses may be amended or replaced from time to time), subject to the requirements of this Section 9.

b. If Strategy appoints a new sub-processor or intends to make any changes concerning the addition or replacement of any sub-processor which will process Personal Data that Strategy is processing on behalf of Customer, Strategy shall update the websites set out in Section 9(a) above and inform Customer of such update via e-mail if the new or replacement sub-processor will process any Personal Data. If Customer fails to object to the appointment or replacement within thirty (30) days' of its posting on reasonable and documented grounds related to the confidentiality or security of Personal Data or the subcontractor's compliance with Privacy Laws, Strategy may proceed with the appointment or replacement. If Customer reasonably objects to a new sub-processor, Customer shall inform Strategy in writing within thirty (30) days following the update of the applicable sub-processor list and such objection shall describe Customer's legitimate reasons for objection. Strategy shall have the right to cure any objection by, in its sole discretion, either choosing to (i) 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 (ii) suspend and/or terminate any product or service that would involve the use of the sub-processor.

c. Strategy shall engage subcontractors only pursuant to a written agreement that contains obligations on the subcontractor which are no less onerous on the relevant subcontractor than the obligations on Strategy under this DPA.

d. In the event Strategy engages a subcontractor to carry out specific processing activities on behalf of Customer pursuant to EU/UK Privacy Laws, where that subcontractor fails to fulfil its obligations, Strategy shall remain fully liable under applicable EU/UK Privacy Laws to Customer for the performance of that subcontractor's obligations.

10. **Assistance**. To the extent required by Privacy Laws, and taking into account the nature of the processing, Strategy shall, in relation to the processing of Personal Data and to enable Customer to comply with its obligations which arise as a result thereof, provide reasonable assistance to Customer, through appropriate technical and organizational measures, in:

a. responding to requests from individuals pursuant to their rights under Privacy Laws, including by providing, deleting or correcting the relevant Personal Data, or by enabling Customer to do the same, insofar as this is possible;

b. implementing reasonable security procedures and practices appropriate to the nature of the Personal Data to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure;

c. notifying relevant competent authorities and/or affected individuals of any Security Incident;

d. conducting data protection impact assessments and, if required, prior consultation with relevant competent authorities; and

e. entering into this DPA.

11. **Security Measures and Incidents**. Strategy shall, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purpose of the processing, implement

appropriate technical and organizational measures designed to provide a level of security appropriate to the risk. To the extent required by Privacy Laws, Strategy shall without undue delay notify Customer of any Security Incident, with further information about the Security Incident provided in phases as more details become available. For the avoidance of doubt, Strategy's obligation to report or respond to a Security Incident, including without limitation, under this Section 11 is not and will not be construed as an acknowledgement by Strategy of any fault or liability of Strategy with respect to the Security Incident.

12. **Access and Audits**.

a. Customer Audits of Strategy. Upon reasonable request of Customer, Strategy shall make available to Customer such information in its possession as is reasonably necessary to demonstrate Strategy's compliance with its obligations under this DPA, and allow for and contribute to audits by providing written responses to questionnaires and copies of relevant documents. Customer shall be permitted to conduct such an assessment no more than once every 12 months, upon 30 days' advance written notice to Strategy, and only after the Parties come to agreement on the scope of the audit and any auditor reviewing the provided materials is bound by a duty of confidentiality. As an alternative to an audit performed by the Customer, to the extent permitted by Privacy Laws, Strategy may arrange for a qualified and independent auditor to conduct, at Customer's expense, an assessment of Strategy's policies and technical and organizational measures in support of its obligations under Privacy Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessment, and will provide a report of such assessment to Customer upon reasonable request. Notwithstanding the foregoing, in no event shall Strategy be required to give Customer access to information, facilities, documents or systems to the extent doing so would cause Strategy to be in violation of confidentiality obligations owed to other customers or its legal obligations.

b. Strategy Audits of sub-processors. Customer acknowledges and agrees that our rights to audit our sub-processors referred to in Section 9 above will be subject to the terms we have in place with each such sub-processor and will likely involve: (i) using 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; (ii) ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001; and (iii) 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**"). Strategy may not be able to disclose such Report to Customer without permission from the sub-processor. At Customer's reasonable written request during the exercise of its audit rights under Section 12, Strategy will request the permission to provide Customer with a copy of such Report so that Customer can reasonably verify the sub-processor's compliance with its security obligations, provided that Customer acknowledges that the sub-processor may require Customer to enter into an NDA with such sub-processor before releasing the same.

13. **Deletion of Personal Data**. At Customer's written direction, Strategy shall delete or return all Personal Data to Customer as requested at the end of the provision of the Services, unless retention of the Personal Data is required by law.

14. **Data Transfers**.

Customer acknowledges and agrees that Strategy may appoint an affiliate or third-party sub-processor to process the Personal Data in a Third Country, in which case, Strategy shall ensure that any Personal

Data transferred to such affiliate or third-party shall be done so pursuant to a valid data transfer mechanism under EU/UK Privacy Laws, such as the Data Privacy Framework (if applicable) or the standard contractual clauses for the transfer of Personal Data to third countries.

15. **Customer Group Authorization**.

Where the Customer is entering into and executing the DPA 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, Strategy against any and all claims, costs, damages and expenses (including, without limitation, legal costs on a full indemnity basis) incurred by Strategy arising out of and/or in connection with a breach of the warranties contained in this Section 15. The terms of this DPA shall apply as between Strategy and relevant members of the Customer Group subject to the provisions of the Agreement.

The parties agree that the Customer that is the contracting party to the Agreement and this DPA shall, to the fullest extent permissible under applicable law, have the sole right to exercise any rights or remedies available under this DPA 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.

**IN WITNESS WHEREOF**, the Parties have executed this DPA as of the dates listed below.

| **Strategy** | **Customer** |
|---|---|
| By: _____ | By: _____ |
| Name: _____ | Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |

## ANNEX 1

## Details of Processing

### Personal 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 Services. |
| **Purpose of Processing** | Provision of the Services |
| **Type of Personal Data** | The Personal Data uploaded or transferred for processing through the Services 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 Services by the Customer |

### Personal Data in relation to Consulting Services

| | |
|---|---|
| **Subject matter of Processing** | Provision of Services as described in the Agreement, statement of work and/or other ordering document |
| **Duration of Processing** | Term of Services engagement or contract |
| **Nature of Processing** | Access, storage and processing of Personal Data in the course of the provision of Services |
| **Purpose of Processing** | Provision of Services |
| **Type of Personal Data** | Personal Data that may be provided during the course of the engagement or contract |
| **Categories of Data Subject** | Personal Data, which may include, employees of the Customer or Customer's customers, prospects, business partners and vendors and employees of agents of the Customer |

## Personal Data in relation to Technical Support

| | |
|---|---|
| **Subject matter of Processing** | Provision of Services to the Customer in connection with the resolution of a technical support case |
| **Duration of Processing** | Term of Services engagement or contract |
| **Nature of Processing** | Storage, back-up, recovery and processing of Personal Data in connection with a Technical Support case |
| **Purpose of Processing** | Provision of technical support |
| **Type of Personal Data** | The Personal Data that is uploaded or transferred in connection with the resolution of a technical support case |
| **Categories of Data Subject** | Employees of the Customer or Customer's customers, prospects, business partners and vendors and employees of agents of the Customer |