HOSTED SERVICE DATA PROCESSING ADDENDUM (UK VERSION)

This Data Processing Addendum ("Addendum"), including its Schedules and Appendices, 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 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 as implemented into UK law ("**UK GDPR"**), the Data Protection Act 2018 and the California Consumer Protection Act (Cal. Civ. Code §§ 1798.100 *et. seq.*) (CCPA). The terms "**Controller**," **"Business," "Processor**," "**Data Subject,**" **"Service Provider,"** "**Foreign Designated 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 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 the United Kingdom to a country or territory to which such transfer is prohibited or subject to any requirement to take additional steps to adequately protect personal data.

"**ICO**" means the Information Commissioner's Office, the regulatory body for Applicable Data Protection Laws, and supervisory authority, for the United Kingdom

"**Standard Contractual Clauses**" means those clauses comprised within the European Commission Decision (C(2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, as may be updated, supplemented or replaced from time to time under Applicable Data Protection Law, and are attached hereto and form part of this Addendum as Schedule 2.

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

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. 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.

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 Standard Contractual Clauses apply, nothing in this section 3 varies or modifies the Standard Contractual Clauses, 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 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 Standard Contractual Clauses, 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. Where those International Transfers occur, the Customer agrees to enter into, complete and execute a copy of the Standard Contractual Clauses contained in Schedule 2 to this Addendum. The Standard Contractual Clauses in Schedule 2 have been pre-signed by MicroStrategy Services Corporation as the data importer. The Customer acknowledges that there may be instances where the contracting MicroStrategy entity or entities executing the Governing Agreement and Addendum may differ from the MicroStrategy entity (data importer) named in the Standard Contractual Clauses. This may occur for example where the MicroStrategy entity signing the Governing Agreement and Addendum is based within the EEA or Switzerland (and is thus not an offshore processor, importing the personal data for the purposes of the Standard Contractual Clauses), and Customer Data is being shared onwards with another MicroStrategy entity who is based outside of the EEA.

In the event that the form of the Standard Contractual Clauses is changed or replaced by the relevant authorities under Applicable Data Protection Law, the Customer as Controller should complete the updated form and notify MicroStrategy as Processor of such form. Provided that such form is accurate and applicable to MicroStrategy as Processor, such form shall then be binding upon the parties when both parties have executed the revised form, subject to the expiration of a grace period, if any, determined by the ICO. If the Customer does not enter into and execute the Standard Contractual Clauses (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.

Notwithstanding the foregoing, the Standard Contractual Clauses in Schedule 2 (or obligations the same as those under the Standard Contractual Clauses) will not apply if MicroStrategy has adopted an alternative recognized compliance standard for the lawful transfer of personal data outside the United Kingdom, to protect Customer Data.

In respect of other International Transfers outside of those covered by the Standard Contractual Clauses contained in Schedule 2, 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 those under the Standard Contractual Clauses where these apply), which shall 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 Standard Contractual Clauses apply under Section 5, 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 Foreign Designated Authority's, the ICO's or data subject's rights under those Standard Contractual 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 the ICO and/or Data Subjects;

d) conducting privacy impact assessments of any processing operations and consulting with the ICO, 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.

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)	**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.

SCHEDULE 2

Standard Contractual Clauses

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 entity identified as “Customer” in the Addendum

(the data exporter)

and

MicroStrategy Services Corporation

(the data importer)

each a “party”; together “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.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '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;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) '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;

(d) '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;

(e) '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;

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

Clause 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.

Clause 3

Third-party beneficiary clause

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.

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. 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.

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.

Clause 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 organisational 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, unauthorised 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).

Clause 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 organisational 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 unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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.

Clause 6

Liability

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.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 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.

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

3. 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.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

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.

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).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely [ENTER]

Clause 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.

Clause 11

Subprocessing

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.

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.

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, namely England & Wales.

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.

Clause 12

Obligation after the termination of personal data processing services

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.

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.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:
Name (written out in full): Phong Le
Position: President and Treasurer
Address: 1850 Towers Crescent Plaza, Tysons Corner, VA 22182, U.S.A.
Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is the entity identified as "Customer" in the Addendum. The data exporter is using the personal data which is being transferred for the following purposes or activities:

[data exporter to complete with activities]

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

MicroStrategy is a provider of business intelligence, mobile software, and cloud-based services. For the purposes of the Hosted Service Addendum, MicroStrategy provides business intelligence as a service including reporting, analysis, and mobile analytics capabilities through the cloud and processes personal data upon the instruction of the data exporter in accordance with the terms of the Governing Agreement

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit personal data to the Hosted Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data concerning the following categories of data subjects (please specify):

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of the data exporter's prospects, customers, business partners and vendors
- Employees or agents of the data exporter, including those who have been authorized to use the Hosted Service
- Data exporter's users authorized by data expoerter to use the Hosted Service

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit personal data to the Hosted Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data concerning the following categories of data (please specify):

[Data exporter to complete.]

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of personal data to the Hosted Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which includes for the sake of clarity, personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniqely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (please specify):

[Data exporter to complete. Select special categories or state "None"]

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of processing of personal data by the data importer is the performance of the Hosted Services pursuant to the Governing Agreement and includes:

- Storage and processing through the Hosted Service
- Processing in connection with a technical support case related to the Hosted Service

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

The technical and organisational security measures implemented by the data importer are as described in and will be implemented in accordance with the terms of a master agreement currently in effect between the data exporter and the data importer or if one does not exist, by the MicroStrategy Cloud Environment Service Guide and Terms and Conditions listed at https://www.microstrategy.com/licensing on the effective date.

This Appendix further provides MicroStrategy's current technical and organizational security measures to protect the confidentiality, integrity and availability of personal data with MicroStrategy's products and services. MicroStrategy may change these measures at any time without notice so long as it maintains a comparable or better level of security.

- Measures of pseudonymisation and encryption of personal data
    - MicroStrategy requires that personal data is encrypted at rest and in transit. This can be achieved through application-level encryption, filesystem encryption or hardware-based encryption at a storage media level.
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
    - MicroStrategy has established processes that incorporate security into the evaluation of a vendor, system, or service to ensure the confidentiality, integrity and availability of its data.
    - MicroStrategy has established rules of behaviour that are documented in its Acceptable Use Policy. The MicroStrategy Acceptable Use Policy provides common rules on the appropriate use of all MicroStrategy information technology resources for all users, including employees, interns, and contractors.
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
    - MicroStrategy has taken steps to ensure its business continue to operate, even during a disaster disrupting normal mode of operation. Critical systems and services have been identified and regular exercises are being held to ensure that personnel are prepared in the event that disaster recovery procedures must be invoked.
    - Backups are completed nightly, ensuring that critical systems can be restored with minimal data loss.
    - MicroStrategy has established incident response procedures, allowing for handling of incidents in a timely and controlled manner and in accordance with applicable law and obligations.
    - MicroStrategy has defined contingency plan(s) for its critical systems. Those plan(s) are tested at least annually and updated as needed.
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
    - Independent third-party audits/certifications:
        - SOC-2: MicroStrategy has an independent accountant firm conduct an annual SOC-2 compliance audit of its Hosted Service, which is available to customers upon request.
        - ISO27001:2013: MicroStrategy has an independent accountant firm conduct an annual ISO27001 recertification of its Hosted Service. The certification letter is available to customers upon request.
    - MicroStrategy has contracted with an independent third party to conduct an annual risk assessment of its Hosted Service.
    - Vulnerability Scans

        - MicroStrategy has established weekly internal scans of its systems, identifying security vulnerabilities that need to be addressed.

        - Quarterly external scans are part of the PCI-DSS compliance efforts, to identify if there are any remotely exploitable vulnerabilities, in the Hosted Service, accessible from the Internet.

    - Independent third-party pen-test: Semi-annual pen-tests are performed as part of the PCI-DSS compliance efforts of the Hosted Service.

    - Internal Security Assessments

        - MicroStrategy conducts Health Insurance Portability and Accountability Act (HIPAA) self-assessments at least annually.

        - MicroStrategy performs an annual self-assessment for PCI-DSS compliance of its Hosted Service.

    - Risk Assessment: MicroStrategy conducts independent third-party risk assessments at least annually for its Hosted Service.

- Measures for user identification and authorisation

    - MicroStrategy has established Identification and Authentication Policy and Procedures for its critical systems.

    - MicroStrategy has implemented physical access controls at all of our offices, requiring employees and onsite contractors to authenticate before entering the premises or special sections in the office. Third party hosting providers are required to provide evidence that physical access control requirements are met.

    - MicroStrategy has implemented system access control for all systems that are not for public access. Access control includes the usage of a username and a complex password and, with critical systems, multifactor authentication leveraging one-time credentials.

    - MicroStrategy has implemented network access control at all the ingress and egress network points. All network traffic is denied by default. Only traffic that meets an access control rule is allowed into the corporate network.

- Measures for the protection of data during transmission

    - MicroStrategy requires that data is encrypted during transit by leveraging common industry protocols as Transport Layer Security (TLS) or Virtual Private Networks (VPN).

    - Encrypted communication is used for all sensitive communication between systems.

- Measures for the protection of data during storage

    - MicroStrategy requires that data is encrypted during storage by leveraging common industry protocols such as AES-256bit level of encryption.

    - Encrypted storage of sensitive information is available for customers of the Hosted Service, ensuring the confidentiality of their data.

- Measures for ensuring physical security of locations at which personal data are processed

    - MicroStrategy requires that its data center hosting providers meet at a minimum SOC-2 and ISO27001 requirements. Hosting providers that host systems storing or processing regulated customer data (e.g., Protected Health Information (PHI) or card holder data) are required to have additional attestations in place, ensuring compliance and alignment with laws, regulations and business needs.

    - MicroStrategy uses Public Cloud service providers, e.g Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, as Sub-Processors providing the Hosted Service. The Public Cloud service providers meet SOC-2, ISO27001, HIPAA and PCI-DSS requirements. Each year MicroStrategy requests the Public

Cloud service providers to provide updated documentation that demonstrate their compliance with those security standards/frameworks.

- Measures for ensuring events logging
    - Critical log events have been identified for all critical systems. These critical log events include information that is meaningful in identifying security incidents.
    - A third-party 24x7 monitoring services conducts log reviews, analysis and reporting and notifies MicroStrategy in case suspicious events are identified.
    - MicroStrategy has installed file integrity monitoring on critical systems. Any unauthorized change of files monitored would be detected and investigated.
    - Logs for critical systems are maintained according to the retention time required by law, regulation, business need or standard best practice.
- Measures for ensuring system configuration, including default configuration
    - MicroStrategy has established secure baseline configuration for its critical systems. Baselines are reviewed and updated as new security threats or needs are identified.
    - Hardening of systems is part of the deployment of new critical systems.
    - MicroStrategy has established a configuration management plan that identifies tools, methods, and processes on how changes are being implemented with its critical systems.
- Measures for internal IT and IT security governance and management
    - MicroStrategy has defined an IT governance program that addresses security. It establishes “security gates” with projects, ensuring that requirements and design address potential security threats.
- Measures for certification/assurance of processes and products
    - MicroStrategy has established change control processes for its critical systems. Every change request must be reviewed for impact, back-out procedure and approved by the Change Control Board (CCB).
- Measures for ensuring data minimisation
    - Data minimisation is conducted on a regular basis with systems or when deemed necessary to ensure only the minimum amount of necessary data is retained.
- Measures for ensuring data quality
    - File integrity monitoring is used to ensure that critical systems are protected from unauthorized changes by users or malicious code.
    - Malicious code protection uses a next generation based third party vendor solution that identifies malicious behaviour and allows roll-back of any actions taken.
- Measures for ensuring limited data retention
    - Data is retained on systems only for as long as deemed necessary to ensure system operability or as determined by contractual agreement.
- Measures for ensuring accountability
    - MicroStrategy adjusts access rights of personnel whenever they are transferred or assume different responsibilities.
    - MicroStrategy revokes all access of employees upon termination.

- Measures for allowing data portability and ensuring erasure
    - MicroStrategy has established Digital Media Handling Procedures addressing media access, media marking, media storage, media transport and media sanitization.