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 legal entity identified as "Customer" on an order for MicroStrategy Products or Services pursuant to the Software License and Services Agreement

(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.

Appendix 1 to the Standard Contractual Clauses

Data exporter

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

The data exporter is the legal entity identified as "Customer" on an order for MicroStrategy Products or Services pursuant to the Software License and Services Agreement.

Data importer

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

MicroStrategy Services Corporation, a subsidiary of MicroStrategy Inc., a provider of business intelligence, mobile software, and cloud-based services. 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 cloud hosted service or in connection with the provision of technical support or consulting services, 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 cloud hosted service
- Data exporter's users authorized by data exporter to use the cloud 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 cloud hosted service or in connection with the provision of technical support or consulting services, 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):

- Personal life data
- Employment and professional life data
- Financial data
- Education and training data
- Contact information (company, email, phone, business address)
- ID data
- Localisation data

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 cloud hosted service or in connection with the provision of technical support or consulting services, 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):

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 cloud hosted service or in connection with the provision of technical support or consulting services pursuant to a governing agreement and includes:

- Storage and processing through the cloud hosted service
- Processing in connection with a technical support case related to the cloud hosted service
- Processing in connection with providing consulting services related to cloud hosted service

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and 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, Technical Support Policy and Procedures, and/or the Terms and Conditions listed at https://www.microstrategy.com/licensing on the effective date.

In addition, below are generally 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.