riverbed

DATA PROCESSING ADDENDUM

Riverbed offers its customers and partners a data processing addendum (DPA) that provides key GDPR-related assurances about our products and services. Customers and partners may review the terms of the applicable DPA below (pp. 2-17 for customers; pp. 18-33 for partners).

HOW TO EXECUTE RIVERBED'S DPA:

- **CUSTOMERS**: To execute the DPA, please click here to complete the form fields and sign electronically.
- **PARTNERS**: To execute the DPA, please click here to complete the form fields and sign electronically.

Data Processing Addendum – Customers

This DPA forms part of the Master Purchase Agreement, End User License Agreement (EULA), Cloud Services Agreement or other written agreement between Riverbed and the Customer for the purchase or license of Riverbed products and services from Riverbed (hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

DATA PROCESSING TERMS

1. **Definitions**.

    a. "**Affiliate**" means any legal entity that controls, is controlled by, or is under common control with a party.

    b. "**Controller**" means the entity which determines the purposes and means of the processing of Personal Data.

    c. "**Customer Personal Data**" means Personal Data provided by or on behalf of the Customer to Riverbed as part of the Services.

    d. "**Data Breach** means any breach of Riverbed's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data on systems managed by or otherwise controlled by Riverbed. "Data Breaches" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

    e. "**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

    f. "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

    g. "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

    h. "**Personal Data**" means any information relating to an identified or identifiable natural person.

    i. "**Privacy and Security Documentation**" means the Privacy and Security Documentation applicable to the specific Services purchased by Customer, as may be updated from time to time, and accessible via Riverbed's Privacy Resource Center at www.riverbed.com/privacy (available under the "Privacy and Security Documentation" tab), or otherwise made generally available by Riverbed.

    j. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

    k. "**Processor**" means the entity which processes Personal Data on behalf of the Controller.

    l. "**Standard Contractual Clauses**" mean the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection within the meaning of the applicable Data Protection Laws and Regulations.

    m. "**Subprocessor**" means any Processor engaged by Riverbed.

    n. "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

    o. "**Users**" means the individuals Customer authorizes to use the Services.

2. **Processing of Personal Data**.

    a. **Roles of the Parties**. In order to perform the Services, Riverbed may be required to process Customer Personal Data during the term of the Agreement. In that case and with respect to the Customer Personal Data, the parties acknowledge and agree that:

        i. Riverbed is a Processor of the Customer Personal Data under the applicable Data Protection Laws and Regulations; and

ii. Customer is a Controller or Processor, as applicable, of the Customer Personal Data under the applicable Data Protection Laws and Regulations.

b. **Customer Processing**. Customer shall, in its use of the Services, Process Customer Personal Data in accordance with the requirements of applicable Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services.

i. Customer's Instructions. By entering into this DPA, Customer instructs Riverbed to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; and (b) as further documented in any other written instructions given by Customer and acknowledged by Riverbed as constituting instructions for purposes of this DPA.

c. **Riverbed Processing**. Riverbed shall only Process Customer Personal Data on behalf of and in accordance with instructions described in Section 2.b.i (Customer's Instructions) unless EU or EU Member State law to which Riverbed is subject requires other processing of Customer Personal Data by Riverbed, in which case Riverbed will inform Customer unless otherwise prohibited by law.

i. Customer warrants it will secure and maintain all rights necessary in Customer Personal Data, including obtaining the necessary consents from third parties including Users, to permit it to legally provide the Customer Personal Data to Riverbed and permit Riverbed to use such Customer Personal Data as contemplated by this DPA.

d. **Details of the Processing**. The subject matter and details of the processing are described in Schedule 1 (Details of the Processing) to this DPA.

3. **Riverbed Personnel**.

a. **Confidentiality**. Riverbed will ensure that all Riverbed personnel authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

b. **Security Compliance**. Riverbed will take appropriate steps to ensure compliance with the Security Measures by its personnel, contractors and Subprocessors to the extent applicable to their scope of performance.

c. **Access Limitation**. Riverbed shall ensure that Riverbed's access to Customer Personal Data is limited to those personnel who require such access to perform the Services in accordance with the Agreement.

d. **Data Protection Lead(s)**. Riverbed will appoint data protection lead(s); Riverbed will provide the contact details of the appointed person(s) upon request.

4. **Security**.

a. **Riverbed's Security Measures**. Riverbed will maintain appropriate technical and organizational measures designed to ensure the security of the Customer Personal Data and to prevent unauthorized or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data as set forth in the Privacy and Security Documentation (the "**Security Measures**"). Riverbed may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

b. **Third-Party Certifications and Audits**. Riverbed has obtained the third-party certifications and audits set forth in Privacy and Security Documentation. Upon Customer's written request at reasonable intervals, and subject to appropriate confidentiality obligations, Riverbed will make available to Customer a copy of Riverbed's then most recent third-party audits or certifications, as applicable.

c. **Customer's Security Responsibilities**. Customer agrees that without prejudice to Riverbed's obligations under Section 4.a (Riverbed's Security Measures) and Section 7 (Customer Personal Data Breaches):

i. Customer is solely responsible for its use of the Services, including:

1. Making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;

2. Securing the account authentication credentials, systems and devices Customer uses to access the Services;

3. backing up its Customer Personal Data; and

ii. Riverbed has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Riverbed's or its Subprocessors' systems (for example, offline or on-premises storage).

5. **Subprocessors**.

a. **Consent to Subprocessor Engagement**. Customer specifically authorizes the engagement as Subprocessors of (i) those third party entities and (ii) Riverbed Affiliates listed as of DPA Effective Date at www.riverbed.com/legal/subprocessors.html. Customer acknowledges and expressly agrees that the above authorizations constitute Customer's prior written consent to the subcontracting by Riverbed of the processing of Customer Data as required under the Standard Contractual Clauses.

b. **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Riverbed shall:

i. ensure via a written contract:

1. the Subprocessor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA) and any Standard Contractual Clauses as described in Section 12; and

2. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this DPA, are imposed on the Subprocessor; and

ii. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

c. **List of Current Subprocessors and Notification of New Subprocessors**. A list of Riverbed's current Subprocessors is available at www.riverbed.com/legal/subprocessors.html. Customer may subscribe to notifications of new Subprocessors via the subscription mechanism available at www.riverbed.com/legal/subprocessors.html, and if Customer subscribes, Riverbed will inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the email address with which Customer subscribes to receive such notifications prior to authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable Services.

d. **Opportunity to Object to New Subprocessor(s)**. Customer may object to Riverbed's use of a new Subprocessor by notifying Riverbed promptly in writing within thirty (30) days after receipt of Riverbed's notice in accordance with the mechanism set out in Section 5.c. In the event Customer objects to a new Subprocessor, as permitted in the preceding sentence, Riverbed will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected-to new Subprocessor without unreasonably burdening the Customer. If Riverbed is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement with respect to only those Services which cannot be provided by Riverbed without the use of the objected-to new Subprocessor by providing written notice to Riverbed. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

6. **Data Subject Rights**. During the Term, Riverbed shall, to the extent legally permitted, promptly notify Customer if Riverbed receives a request from a Data Subject to exercise the Data Subject's rights set forth in Chapter III of the GDPR ("**Data Subject Request**"). Taking into account the nature of the Processing, Riverbed shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligations to respond to a Data Subject Request under the GDPR. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Riverbed shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Riverbed is legally permitted to do so and the response to such Data Subject Request is required under the GDPR.

7. **Personal Data Breaches**. Riverbed will: (a) notify Customer of the Customer Personal Data Breach promptly and without undue delay after becoming aware of the Customer Personal Data Breach; and (b) promptly take reasonable steps to minimize harm and secure Customer Personal Data.

a. Details of Breach. Notifications made pursuant to this section will describe, to the extent possible, details of the Customer Personal Data Breach, including the steps Riverbed deems necessary and reasonable

in order to remediate the cause of such a Customer Personal Data Breach to the extent the remediation is within Riverbed's reasonable control.

b. Delivery of Notification. Notification(s) of any Customer Personal Data Breach(es) will be delivered to the email address(es) designated by Customer below by any means Riverbed selects, including via email. Customer is solely responsible for ensuring its contact information remains current and valid.

Contact Name:	Contact Name:
Email Address:	Email Address:

c. No Acknowledge of Fault by Riverbed. Riverbed's notification of or response to a Customer Personal Data Breach under this Section 7 (Customer Personal Data Breaches) will not be construed as an acknowledgement by Riverbed of any fault or liability with respect to the Customer Personal Data Breach.

8. **Impact Assessment and Prior Consultation**. Upon Customer's request, Riverbed shall (taking into account the nature of the Processing and the information available to Riverbed) provide reasonable assistance to Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR.

9. **Personal Data Deletion**. At the end of the provision of the Services relating to processing of Customer Personal Data, Riverbed shall, at the request of the Customer, delete all Customer Personal Data and delete existing copies from Riverbed systems to the extent reasonably practicable unless otherwise required by applicable law.

10. **Audits and Certifications**. Upon Customer's request, and subject to appropriate confidentiality obligations, Riverbed will make available to Customer information regarding the Riverbed's compliance with the obligations set forth in this DPA, including the third-party certifications and audits set forth in the Privacy and Security Documentation to the extent Riverbed makes them generally available to its customers.

    a. **Audits**. Customer may no more than one time per year (unless (i) Riverbed notifies Customer of a Personal Data Breach, or (ii) such audit is required by a Supervisory Authority) request an audit of the procedures relevant to the protection of Personal Data. Customer must contact Riverbed at rvbd-privacy@riverbed.com at least six (6) weeks in advance to request such an audit; any audit must be conducted in accordance with the procedures set forth in Section 10.b (Audit Procedures) below.

    b. **Audit Procedures**. Prior to beginning any audit, Riverbed and Customer will mutually agree upon the reasonable start date, scope and duration of and security and confidentiality controls applicable to the audit in addition to allocation of costs between the parties. Riverbed may object in writing to an auditor appointed by Customer to conduct any audit if the auditor is, in Riverbed's reasonable opinion, not suitably qualified or independent, a competitor of Riverbed, or otherwise manifestly unsuitable. Customer shall promptly notify Riverbed with information regarding any noncompliance discovered during the course of any audit.

11. **Processing Location**. Customer Personal Data that Riverbed Processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Riverbed or its Affiliates or Subprocessors maintain facilities. Customer appoints Riverbed to perform any such transfer of Customer Personal Data to any such country and to store and process Customer Personal Data in order to provide the Services. If the storage and/or processing of Customer Personal Data involves the transfer of Customer Personal Data out of the European Economic Area ("**EEA**"), and the Data Protection Laws and Regulations apply to the transfers of such Data, Riverbed will ensure that the transfers are subject to appropriate safeguards as described in Section 12.

12. **Transfers of Personal Data Out of the EEA**. If Riverbed's Processing in the course of providing the Services involves the transfer of Customer Personal Data from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the applicable Data Protection Laws and Regulations), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing adequate protection for personal data, then the Standard Contractual Clauses set forth in Schedule 2 to this DPA will apply, to the extent such transfers are subject to the Data Protection Laws and Regulations.

    a. **Additional Terms for Transfer of Customer Personal Data From the EEA**.

        i. **Instructions**. This DPA and the Agreement are Customer's complete and final documented instructions to Riverbed for the Processing of Customer Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Customer Personal Data: (a) Processing in accordance with the Agreement and

applicable orders; (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

ii. **Subprocessors**. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Riverbed may engage new Subprocessors as described in Sections 5.c and 5.d of this DPA. Riverbed shall make available to Customer a list of current Subprocessors in accordance with Section 5.c of this DPA.

iii. **Copies of Subprocessor Agreements**. The parties agree that the copies of the Subprocessor Agreements that must be provided by Riverbed to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Riverbed beforehand; and, that such copies will be provided by Riverbed, in a manner to be determined in its discretion, only upon request by Customer.

iv. **Audits and Certifications**. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out as described in Sections 10.a and 10.b of this DPA.

v. **Certification of Deletion**. The parties agree that the certification of deletion of Customer Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Riverbed to Customer only upon Customer's request.

vi. **Conflict**. In the event of any conflict or inconsistency between the body of this DPA and Schedule 1 and the Standard Contractual Clauses in Schedule 2, the Standard Contractual Clauses shall prevail.

13. **Limitation of Liability**. The total combined liability of either party and its Affiliates towards the other party and its Affiliates whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA.

14. **Legal Effect; Term; Termination**. This DPA shall only become legally binding between Customer and Riverbed once executed by both Customer and Riverbed (the "**DPA Effective Date**"). This DPA shall remain in effect from DPA Effective Date until the end of Riverbed's provision of the Services (the "**Term**") and will terminate when Riverbed's provision of the Services ends, without further action required by either party.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: Standard Contractual Clauses

AGREED AND ACCEPTED:

Customer:	**Riverbed Technology, Inc.**:
Signature:_____	Signature:_____
Name:_____	Name: _____
Title:_____	Title: _____
Date:_____	Date:_____

SCHEDULE 1 – DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Riverbed will Process Customer Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer (in accordance with Section 2.b.i of the DPA) in its use of the Services.

Duration of Processing

Subject to Section 9 of the DPA, Riverbed will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

- Employees of Customer
- Customer's Users

Types of Personal Data

- First and Last Name
- Title
- Position
- Employer
- Contact Information (company, email, phone, physical business address)
- Personal Data incidental to data provided to obtain technical support (which is determined and controlled by Customer in its sole discretion)

To the extent that Customer purchases or licenses the SteelCentral Aternity Cloud Service:

- Active IP Address
- AD Title
- Client Device Name
- Email Address
- Hostname
- IP Address
- User Full Name
- Username

To the extent that Customer purchases or licenses the SteelCentral AppInternals Cloud Service:

- User IP Address
- Username

To the extent that Customer purchases or licenses SteelConnect Manager:

- MAC Address
- Client IP Address
- Email Address
- Username
- Mobile number (*if multi-factor authentication enabled by Customer*)

SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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.

Name of the data exporting organisation:_____

Address:_____

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation:_____

……

(the data **exporter**)

And

Name of the data importing organisation: Riverbed Technology, Inc.

Address: 680 Folsom Street, 6th Floor, San Francisco, CA 94107, USA

Tel.: + 1 415 247 8800 ; fax: +1 415 247 8801 ; e-mail: rvbd-privacy@riverbed.com

Other information needed to identify the organisation: Not applicable

(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.

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.

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_____

On behalf of the data importer:

Name (written out in full):_____

Position:_____

Address:_____

Other information necessary in order for the contract to be binding (if any):_____

Signature_____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed 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):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased the Services.

Data importer

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

Riverbed Technology, Inc. is a provider of enterprise application and networking solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

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

- Employees of Customer
- Customer's Users

Categories of data

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

- First and Last Name
- Title
- Position
- Employer
- Contact Information (company, email, phone, physical business address)
- Personal Data incidental to data provided to obtain technical support (which is determined and controlled by Customer in its sole discretion)

To the extent that Customer purchases or licenses the SteelCentral Aternity Cloud Service:

- Active IP Address
- AD Title
- Client Device Name
- Email Address
- Hostname
- IP Address
- User Full Name
- Username

To the extent that Customer purchases or licenses the SteelCentral AppInternals Cloud Service:

- User IP Address
- Username

To the extent that Customer purchases or licenses SteelConnect Manager:

- MAC Address
- Client IP Address
- Email Address
- Username
- Mobile number (*if multi-factor authentication enabled by Customer*)

Special categories of data (if appropriate): Not applicable

Processing operations

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

The objective of Processing of Customer Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Subject to Section 9 of the DPA, the data importer will Process Customer Personal Data for the duration of the Agreement, unless otherwise mutually agreed upon in writing.

DATA EXPORTER

Name:_____

Authorised Signature:_____

DATA IMPORTER

Name:_____

Authorised Signature:_____

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed 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):

Data importer will maintain appropriate technical and organizational safeguards, taking into account both the state of technologies and the costs of implementation, against unauthorized or unlawful processing of Customer Personal Data and against accidental loss or destruction of, and damage to the Customer Personal Data, as set forth in the Privacy and Security Documentation, as updated from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

DATA EXPORTER

Name:_____

Authorised Signature:_____

DATA IMPORTER

Name:_____

Authorised Signature:_____

Data Processing Addendum – Partners

This DPA forms part of the Channel Partner Agreement or other written agreement between Riverbed and the Partner for Partner's resale and/or Managed Service delivery of Riverbed products and services from Riverbed (hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

DATA PROCESSING TERMS

15. **Definitions**.

a. "**Affiliate**" means any legal entity that controls, is controlled by, or is under common control with a party.

b. "**Controller**" means the entity which determines the purposes and means of the processing of Personal Data.

c. "**Partner Personal Data**" means Personal Data provided by or on behalf of the Partner to Riverbed as part of the Services.

d. "**Data Breach** means any breach of Riverbed's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Partner Personal Data on systems managed by or otherwise controlled by Riverbed. "Data Breaches" will not include unsuccessful attempts or activities that do not compromise the security of Partner Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

e. "**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

f. "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

g. "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

h. "**Personal Data**" means any information relating to an identified or identifiable natural person.

i. "**Privacy and Security Documentation**" means the Privacy and Security Documentation applicable to the specific Services purchased by Partner, as may be updated from time to time, and accessible via Riverbed's Privacy Resource Center at www.riverbed.com/privacy (available under the "Privacy and Security Documentation" tab), or otherwise made generally available by Riverbed.

j. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

k. "**Processor**" means the entity which processes Personal Data on behalf of the Controller.

l. "**Standard Contractual Clauses**" mean the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection within the meaning of the applicable Data Protection Laws and Regulations.

m. "**Subprocessor**" means any Processor engaged by Riverbed.

n. "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

o. "**Users**" means the individuals Partner authorizes to use the Services.

16. **Processing of Personal Data**.

e. **Roles of the Parties**. In order to perform the Services, Riverbed may be required to process Partner Personal Data during the term of the Agreement. In that case and with respect to the Partner Personal Data, the parties acknowledge and agree that:

i. Riverbed is a Processor of the Partner Personal Data under the applicable Data Protection Laws and Regulations; and

ii. Partner is a Controller or Processor, as applicable, of the Partner Personal Data under the applicable Data Protection Laws and Regulations.

f. **Partner Processing**. Partner shall, in its use of the Services, Process Partner Personal Data in accordance with the requirements of applicable Data Protection Laws and Regulations. Partner shall have sole responsibility for the accuracy, quality, and legality of Partner Personal Data and the means by which Partner acquired Partner Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Services.

i. Partner's Instructions. By entering into this DPA, Partner instructs Riverbed to process Partner Personal Data only in accordance with applicable law: (a) to provide the Services; and (b) as further documented in any other written instructions given by Partner and acknowledged by Riverbed as constituting instructions for purposes of this DPA.

g. **Riverbed Processing**. Riverbed shall only Process Partner Personal Data on behalf of and in accordance with instructions described in Section 2.b.i (Partner's Instructions) unless EU or EU Member State law to which Riverbed is subject requires other processing of Partner Personal Data by Riverbed, in which case Riverbed will inform Partner unless otherwise prohibited by law.

i. Partner warrants it will secure and maintain all rights necessary in Partner Personal Data, including obtaining the necessary consents from third parties including Users, to permit it to legally provide the Partner Personal Data to Riverbed and permit Riverbed to use such Partner Personal Data as contemplated by this DPA.

h. **Details of the Processing**. The subject matter and details of the processing are described in Schedule 1 (Details of the Processing) to this DPA.

17. **Riverbed Personnel**.

a. **Confidentiality**. Riverbed will ensure that all Riverbed personnel authorized to process Partner Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

b. **Security Compliance**. Riverbed will take appropriate steps to ensure compliance with the Security Measures by its personnel, contractors and Subprocessors to the extent applicable to their scope of performance.

c. **Access Limitation**. Riverbed shall ensure that Riverbed's access to Partner Personal Data is limited to those personnel who require such access to perform the Services in accordance with the Agreement.

d. **Data Protection Lead(s)**. Riverbed will appoint data protection lead(s); Riverbed will provide the contact details of the appointed person(s) upon request.

18. **Security**.

a. **Riverbed's Security Measures**. Riverbed will maintain appropriate technical and organizational measures designed to ensure the security of the Partner Personal Data and to prevent unauthorized or unlawful processing of Partner Personal Data and against accidental loss or destruction of, or damage to, Partner Personal Data as set forth in the Privacy and Security Documentation (the "**Security Measures**"). Riverbed may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

b. **Third-Party Certifications and Audits**. Riverbed has obtained the third-party certifications and audits set forth in Privacy and Security Documentation. Upon Partner's written request at reasonable intervals, and subject to appropriate confidentiality obligations, Riverbed will make available to Partner a copy of Riverbed's then most recent third-party audits or certifications, as applicable.

c. **Partner's Security Responsibilities**. Partner agrees that without prejudice to Riverbed's obligations under Section 4.a (Riverbed's Security Measures) and Section 7 (Partner Personal Data Breaches) as between Partner and Riverbed:

i. Partner is solely responsible for its and its End Users' use of the Services, including:

1. Making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Partner Personal Data;

2. Securing the account authentication credentials, systems and devices Partner and its End Users uses to access the Services;

3. backing up its Partner Personal Data; and

ii. Riverbed has no obligation to protect Partner Personal Data that Partner or its End Users elect to store or transfer outside of Riverbed's or its Subprocessors' systems (for example, offline or on-premises storage).

19. **Subprocessors**.

a. **Consent to Subprocessor Engagement**. Partner specifically authorizes the engagement as Subprocessors of (i) those third party entities and (ii) Riverbed Affiliates listed as of DPA Effective Date at www.riverbed.com/legal/subprocessors.html. Partner acknowledges and expressly agrees that the above authorizations constitute Partner's prior written consent to the subcontracting by Riverbed of the processing of Partner Data as required under the Standard Contractual Clauses.

b. **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Riverbed shall:

i. ensure via a written contract:

1. the Subprocessor only accesses and uses Partner Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA) and any Standard Contractual Clauses as described in Section 12; and

2. if the GDPR applies to the processing of Partner Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this DPA, are imposed on the Subprocessor; and

ii. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

c. **List of Current Subprocessors and Notification of New Subprocessors**. A list of Riverbed's current Subprocessors is available at www.riverbed.com/legal/subprocessors.html. Partner may subscribe to notifications of new Subprocessors via the subscription mechanism available at www.riverbed.com/legal/subprocessors.html, and if Partner subscribes, Riverbed will inform Partner of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the email address with which Partner subscribes to receive such notifications prior to authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable Services.

d. **Opportunity to Object to New Subprocessor(s)**. Partner may object to Riverbed's use of a new Subprocessor by notifying Riverbed promptly in writing within thirty (30) days after receipt of Riverbed's notice in accordance with the mechanism set out in Section 5.c. In the event Partner objects to a new Subprocessor, as permitted in the preceding sentence, Riverbed will use reasonable efforts to make available to Partner a change in the Services or recommend a commercially reasonable change to Partner's configuration or use of the Services to avoid Processing of Partner Personal Data by the objected-to new Subprocessor without unreasonably burdening the Partner. If Riverbed is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Partner may terminate the applicable Agreement with respect to only those Services which cannot be provided by Riverbed without the use of the objected-to new Subprocessor by providing written notice to Riverbed. This termination right is Partner's sole and exclusive remedy if Partner objects to any new Third Party Subprocessor.

20. **Data Subject Rights**. During the Term, Riverbed shall, to the extent legally permitted, promptly notify Partner if Riverbed receives a request from a Data Subject to exercise the Data Subject's rights set forth in Chapter III of the GDPR ("**Data Subject Request**"). Taking into account the nature of the Processing, Riverbed shall assist Partner by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Partner's obligations to respond to a Data Subject Request under the GDPR. In addition, to the extent Partner, in its use of the Services, does not have the ability to address a Data Subject Request, Riverbed shall upon Partner's request provide commercially reasonable efforts to assist Partner in responding to such Data Subject Request, to the extent Riverbed is legally permitted to do so and the response to such Data Subject Request is required under the GDPR.

21. **Personal Data Breaches**. Riverbed will: (a) notify Partner of the Partner Personal Data Breach promptly and without undue delay after becoming aware of the Partner Personal Data Breach; and (b) promptly take reasonable steps to minimize harm and secure Partner Personal Data.

a. Details of Breach. Notifications made pursuant to this section will describe, to the extent possible, details of the Partner Personal Data Breach, including the steps Riverbed deems necessary and reasonable in

order to remediate the cause of such a Partner Personal Data Breach to the extent the remediation is within Riverbed's reasonable control.

b. Delivery of Notification. Notification(s) of any Partner Personal Data Breach(es) will be delivered to the email address(es) designated by Partner below by any means Riverbed selects, including via email. Partner is solely responsible for ensuring its contact information remains current and valid.

Contact Name:	Contact Name:
Email Address:	Email Address:

c. No Acknowledge of Fault by Riverbed. Riverbed's notification of or response to a Partner Personal Data Breach under this Section 7 (Partner Personal Data Breaches) will not be construed as an acknowledgement by Riverbed of any fault or liability with respect to the Partner Personal Data Breach.

22. **Impact Assessment and Prior Consultation**. Upon Partner's request, Riverbed shall (taking into account the nature of the Processing and the information available to Riverbed) provide reasonable assistance to Partner in ensuring compliance with any obligations of Partner in respect of data protection impact assessments and prior consultation, including if applicable Partner's obligations pursuant to Articles 35 and 36 of the GDPR.

23. **Personal Data Deletion**. At the end of the provision of the Services relating to processing of Partner Personal Data, Riverbed shall, at the request of the Partner, delete all Partner Personal Data and delete existing copies from Riverbed systems to the extent reasonably practicable unless otherwise required by applicable law.

24. **Audits and Certifications**. Upon Partner's request, and subject to appropriate confidentiality obligations, Riverbed will make available to Partner information regarding the Riverbed's compliance with the obligations set forth in this DPA, including the third-party certifications and audits set forth in the Privacy and Security Documentation to the extent Riverbed makes them generally available to its Partners.

    a. **Audits**. Partner may no more than one time per year (unless (i) Riverbed notifies Partner of a Personal Data Breach, or (ii) such audit is required by a Supervisory Authority) request an audit of the procedures relevant to the protection of Personal Data. Partner must contact Riverbed at rvbd-privacy@riverbed.com at least six (6) weeks in advance to request such an audit; any audit must be conducted in accordance with the procedures set forth in Section 10.b (Audit Procedures) below.

    b. **Audit Procedures**. Prior to beginning any audit, Riverbed and Partner will mutually agree upon the reasonable start date, scope and duration of and security and confidentiality controls applicable to the audit in addition to allocation of costs between the parties. Riverbed may object in writing to an auditor appointed by Partner to conduct any audit if the auditor is, in Riverbed's reasonable opinion, not suitably qualified or independent, a competitor of Riverbed, or otherwise manifestly unsuitable. Partner shall promptly notify Riverbed with information regarding any noncompliance discovered during the course of any audit.

25. **Processing Location**. Partner Personal Data that Riverbed Processes on Partner's behalf may be transferred to, and stored and processed in, the United States or any other country in which Riverbed or its Affiliates or Subprocessors maintain facilities. Partner appoints Riverbed to perform any such transfer of Partner Personal Data to any such country and to store and process Partner Personal Data in order to provide the Services. If the storage and/or processing of Partner Personal Data involves the transfer of Partner Personal Data out of the European Economic Area ("**EEA**"), and the Data Protection Laws and Regulations apply to the transfers of such Data, Riverbed will ensure that the transfers are subject to appropriate safeguards as described in Section 12.

26. **Transfers of Personal Data Out of the EEA**. If Riverbed's Processing in the course of providing the Services involves the transfer of Partner Personal Data from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the applicable Data Protection Laws and Regulations), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing adequate protection for personal data, then the Standard Contractual Clauses set forth in Schedule 2 to this DPA will apply, to the extent such transfers are subject to the Data Protection Laws and Regulations.

    a. **Additional Terms for Transfer of Partner Personal Data From the EEA**.

        i. **Instructions**. This DPA and the Agreement are Partner's complete and final documented instructions to Riverbed for the Processing of Partner Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Partner to process Partner Personal Data: (a) Processing in accordance with the Agreement and applicable orders; (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other

reasonable documented instructions provided by Partner (e.g., via email) where such instructions are consistent with the terms of the Agreement.

ii. **Subprocessors**. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Partner acknowledges and expressly agrees that Riverbed may engage new Subprocessors as described in Sections 5.c and 5.d of this DPA. Riverbed shall make available to Partner a list of current Subprocessors in accordance with Section 5.c of this DPA.

iii. **Copies of Subprocessor Agreements**. The parties agree that the copies of the Subprocessor Agreements that must be provided by Riverbed to Partner pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Riverbed beforehand; and, that such copies will be provided by Riverbed, in a manner to be determined in its discretion, only upon request by Partner.

iv. **Audits and Certifications**. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out as described in Sections 10.a and 10.b of this DPA.

v. **Certification of Deletion**. The parties agree that the certification of deletion of Partner Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Riverbed to Partner only upon Partner's request.

vi. **Conflict**. In the event of any conflict or inconsistency between the body of this DPA and Schedule 1 and the Standard Contractual Clauses in Schedule 2, the Standard Contractual Clauses shall prevail.

27. **Limitation of Liability**. The total combined liability of either party and its Affiliates towards the other party and its Affiliates whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA.

28. **Legal Effect; Term; Termination**. This DPA shall only become legally binding between Partner and Riverbed once executed by both Partner and Riverbed (the "**DPA Effective Date**"). This DPA shall remain in effect from DPA Effective Date until the end of Riverbed's provision of the Services (the "**Term**") and will terminate when Riverbed's provision of the Services ends, without further action required by either party.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: Standard Contractual Clauses

AGREED AND ACCEPTED:

Partner:	**Riverbed Technology, Inc.**:
Signature:_____	Signature:_____
Name:_____	Name: _____
Title:_____	Title: _____
Date:_____	Date:_____

SCHEDULE 1 – DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Riverbed will Process Partner Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Partner (in accordance with Section 2.b.iof the DPA) in its use of the Services.

Duration of Processing

Subject to Section 9 of the DPA, Riverbed will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

- Employees of Partner
- Partner's Users
- Partner's End Users

Types of Personal Data

- First and Last Name
- Title
- Position
- Employer
- Contact Information (company, email, phone, physical business address)
- Personal Data incidental to data provided to obtain technical support (which is determined and controlled by Partner in its sole discretion)

To the extent that Partner purchases or licenses the SteelCentral Aternity Cloud Service for its Managed Service or Internal Use:

- Active IP Address
- AD Title
- Client Device Name
- Email Address
- Hostname
- IP Address
- User Full Name
- Username

To the extent that Partner purchases or licenses the SteelCentral AppInternals Cloud Service for its Managed Service or Internal Use:

- User IP Address
- Username

To the extent that Partner purchases or licenses SteelConnect Manager for its Managed Service or Internal Use:

- MAC Address
- Client IP Address
- Email Address
- Username
- Mobile number (*if multi-factor authentication enabled by Partner or Partner's End Users*)

SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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.

Name of the data exporting organisation:_____

Address:_____

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation:_____

……

(the data **exporter**)

And

Name of the data importing organisation: Riverbed Technology, Inc.

Address: 680 Folsom Street, 6th Floor, San Francisco, CA 94107, USA

Tel.: + 1 415 247 8800 ; fax: +1 415 247 8801 ; e-mail: rvbd-privacy@riverbed.com

Other information needed to identify the organisation: Not applicable

(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.

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.

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_____

On behalf of the data importer:

Name (written out in full):_____

Position:_____

Address:_____

Other information necessary in order for the contract to be binding (if any):_____

Signature_____

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed 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):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Partner established within the European Economic Area (EEA) and Switzerland that have purchased the Services.

Data importer

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

Riverbed Technology, Inc. is a provider of enterprise application and networking solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

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

- Employees of Partner
- Partner's Users
- Partner's End Users

Categories of data

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

- First and Last Name
- Title
- Position
- Employer
- Contact Information (company, email, phone, physical business address)
- Personal Data incidental to data provided to obtain technical support (which is determined and controlled by Partner in its sole discretion)

To the extent that Partner purchases or licenses the SteelCentral Aternity Cloud Service for its Managed Service or Internal Use:

- Active IP Address
- AD Title
- Client Device Name
- Email Address
- Hostname
- IP Address
- User Full Name
- Username

To the extent that Partner purchases or licenses the SteelCentral AppInternals Cloud Service for its Managed Service or Internal Use:

- User IP Address
- Username

To the extent that Partner purchases or licenses SteelConnect Manager: *for its Managed Service or Internal Use*

- MAC Address
- Client IP Address
- Email Address
- Username
- Mobile number (*if multi-factor authentication enabled by Partner or Partner's End Users*)

Special categories of data (if appropriate): Not applicable

Processing operations

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

The objective of Processing of Partner Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Subject to Section 9 of the DPA, the data importer will Process Partner Personal Data for the duration of the Agreement, unless otherwise mutually agreed upon in writing.

DATA EXPORTER

Name:_____

Authorised Signature:_____

DATA IMPORTER

Name:_____

Authorised Signature:_____

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed 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):

Data importer will maintain appropriate technical and organizational safeguards, taking into account both the state of technologies and the costs of implementation, against unauthorized or unlawful processing of Partner Personal Data and against accidental loss or destruction of, and damage to the Partner Personal Data, as set forth in the Privacy and Security Documentation, as updated from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

DATA EXPORTER

Name:_____

Authorised Signature:_____

DATA IMPORTER

Name:_____

Authorised Signature:_____