DATA TRANSFER IMPACT ASSESSMENT GUIDE

Background

The Court of Justice of the European Union ("**CJEU**") published its judgement in the case of the Data Protection Commissioner Ireland v Facebook Ireland Ltd., Maximillian Schrems, known as "**Schrems II**" in July 2020. The subject matter of the CJEU's decision were the transfer mechanisms of the Standard Contractual Clauses ("**SCC**") and the Privacy Shield for transferring data from the European Union (EU) to the United States of America (US). The CJEU declared the Privacy Shield to be invalid and the SCC to be valid but with the restriction that a case-by-case basis analysis is required. Of principal concern for the CJEU in this decision was the potential for surveillance of EU citizens under two US national security legal regimes and what it considered inadequate judicial redress available for EU citizens with respect to each: Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333.

Purpose

In light of the Schrems II ruling and the recommendations issued by the European Data Protection Board ("**EDPB**"), Riverbed Technology LLC and its affiliates ("**Riverbed**" or "**we**") provides this document to assist customers in conducting data transfer impact assessments in connection with their use of Riverbed products.

Overview

Where Riverbed processes personal data subject to European data protection laws as a Processor (on behalf of our customers), Riverbed complies with its obligations under its Data Processing Addendum ("**DPA**"). Riverbed's DPA incorporates the SCCs as a transfer mechanism.

Processing Description

Riverbed's DPA provides the following information:

- Schedule 1 describes of Riverbed's processing of personal data (including the categories of data subjects, categories of personal data, the nature and subject matter of the processing, etc.).
- Schedule 2 describes the Security Measures implemented and maintained by Riverbed

Riverbed's Subprocessors List is available here.

Riverbed may transfer Customer Data (inclusive of personal data) wherever we or our subprocessors maintain facilities. The locations will depend on the particular Riverbed product and/or service used as outlined in the applicable Privacy Data Sheet and/or Processing Details documentation.

Regulatory Framework

- ***FISA 702***: Riverbed may act as electronic communications services ("**ECS**") and also potentially as remote computing services ("**RCS**") (as defined in Sections 2510 and 2711 of Title 18 U.S.C., respectively) in connection with the products and services we provide to customers. Riverbed is therefore among the large number of U.S. companies upon which the U.S. government could technically serve a targeted directive under FISA 702. However, as the U.S. government has applied FISA 702, Riverbed is not eligible to receive the type of order that was of principal concern to the CJEU in the Schrems II decision—i.e., a FISA 702 order for "upstream" surveillance. As the U.S. government has applied FISA 702, it uses upstream orders solely to target traffic flowing through internet backbone providers that carry Internet traffic for third parties (i.e., Google, Yahoo). Riverbed does not provide such Internet backbone services. As a result, it is unlikely that Riverbed would receive the type of order principally addressed in the Schrems II decision.
- ***EO 12333***: EO 12333 is a general directive organizing U.S. intelligence activities and does not include any authorization to compel private companies to disclose data.

To date, Riverbed has never received a request for access under FISA 702 or direct access under EO 12333 in connection with the Customer Data (inclusive of personal data) that we process. While Riverbed may generally be subject to the U.S. surveillance laws identified in Schrems II, Riverbed's day-to-day operations have not been impacted by these requests and the types of Customer Data (inclusive of personal data) processed by Riverbed on behalf of its customers is not likely to be of interest to U.S. intelligence agencies.

Measures To Protect Transferred Data

Technical

- Riverbed's Cloud Services allow customers to select which locations in which their data is stored.
- Other technical measures are described under the "Security Measures" tab of Riverbed's Privacy Resource Center.

Contractual

- Riverbed's DPA commits Riverbed to baseline technical and organizational security measures.
- Riverbed's DPA outlines a process for Riverbed's response to Third Party Requests.

This document is provided for informational purposes only. It is not intended to provide legal advice. Customers are responsible for making their own independent assessment of the information in this document.

Organizational

- Riverbed follows its Third Party Data Request Policy in responding to government requests for data.
- Any Subprocessors engaged by Riverbed undergo a vendor risk management assessment process.
- Riverbed's products and services incorporate "Privacy by Design" principles.
- All Riverbed personnel must undergo annual data protection training.