PRIVACY DATA SHEET

RIVERBED IQ OPS CLOUD SERVICE

This Privacy Data Sheet describes the processing of personal data by the Riverbed IQ Ops Cloud Service.

OVERVIEW

The Riverbed IQ Ops Cloud Service is a SaaS-delivered platform that uses full-fidelity cross-domain data and applies AI techniques and automation workflows to collect diagnostic content and prioritize IT events for fast, focused route cause analysis. The platform includes the following capabilities:

- Telemetry: Broad-based telemetry brings together a unified view of performance and insights by leveraging full-fidelity packet, network device, flow, and end user experience metrics.
- Correlation: Delivers actionable insights through AI/ML capabilities such as correlation, by automating the process of gathering and correlating across time, device, location, users, and applications, as well as leveraging analytics techniques like threshold violations and anomaly detection.
- Automation: Replicates the investigative workflows of IT experts to automate the process of gathering evidence, building context, and setting priorities when troubleshooting issues. These workflows are customizable and additional workflows can be created as needed.
- Dashboards: User interface screen where incidents are displayed by user impact, most impacted locations, and most impacted services to help prioritize events and their effect on the business. Also view active event distribution by event priority and how incident priority changes over time.

DATA PROCESSING

To deliver the Riverbed IQ Ops Cloud Service, Riverbed processes:

"**Customer Data**" consisting of (i) performance measurements, like wait times, response times, or resource consumption ("**Performance Data**"); and (ii) non-measurable descriptive attributes, which add context to the performance measurements to help troubleshoot the problem, e.g., device name, username, location name, application name ("**Metadata**"). Metadata may include certain categories of personal data outlined below:

- Full name
- Email address
- Login credentials
- IP address
- Device name
- Browser version
- Network activity

PROCESSING LOCATIONS

Riverbed uses third-party data centers and infrastructure. Customer Data is hosted and stored in the data center region selected by the customer. As of this document's publication date, customers may designate a hosting and storage region from the options below:

- Germany
- United States
- Australia
- UK

CROSS-BORDER DATA TRANSFER MECHANISMS

Riverbed leverages the EU Standard Contractual Clauses related to the lawful use of personal data across jurisdictions.

ACCESS CONTROL

The table below lists the data used by Riverbed personnel to deliver the Riverbed IQ Ops Cloud Service, who can access that data, and why.

Data Category	Who Has Access	Access Location	Access Purpose
Customer Data	Select Riverbed IQ Ops development and support personnel	France India Israel Romania United Kingdom United States	To operate and maintain the Riverbed IQ Ops Cloud Service platform

DATA PORTABILITY

Customers may export Customer Data by submitting a request via Riverbed's Support Portal.

DATA SECURITY

The Riverbed IQ Ops Cloud Service technical and organizational security measures ("**Security Measures**") and certifications (i.e., SOC 2 Type 2 and ISO 27001) are available via the Riverbed Trust Center (https://www.riverbed.com/trust-center).

SUBPROCESSORS

Riverbed has engaged the subprocessors listed below to deliver the Riverbed IQ Ops Cloud Service:

Subprocessor	Processing Description	Processing Location	Additional Details
Microsoft Corporation	Cloud hosting and infrastructure provider	United States Germany Australia UK	Customers may select an Azure data center region from the options at left.
Amazon Web Services, Inc.	Cloud hosting and infrastructure provider	United States Germany Australia UK	Maps to a customer's underlying Azure data center region selection.

A complete list of Riverbed's subprocessors is published publicly at https://www.riverbed.com/legal/subprocessors.