



PRIVACY DATA SHEET ATERNITY MOBILE CLOUD SERVICE

This Privacy Data Sheet describes the processing of personal data through the Aternity Mobile cloud service.

OVERVIEW

The Aternity Mobile cloud service is a cloud-based enterprise-grade Software-as-a-Service (“**SaaS**”) digital experience management platform providing a comprehensive view of mobile app and device performance across employee mobile devices by capturing and storing technical telemetry data at scale (hereinafter referred to as “**Aternity Mobile SaaS**”) made available by Riverbed to companies (“**Customer**”) who acquire it for internal business use.

DATA PROCESSING

To deliver Aternity Mobile SaaS, Riverbed processes “**Customer Data**,” which consists of:

- IP address
- Telephone number
- If enabled by customer: IMEI, MAC, Serial Number, and/or SimICC
- Customer-defined “device alias” provided by customer such as name and surname, email address, phone number, internal user or device ID
- Other data: geolocation, installed applications, device usage, device settings, device hardware, websites visited, network and telephony information, application and data usage information, network activity (visited IP addresses, domain names, and/or brand of time)

DATA CENTER LOCATIONS

Riverbed uses third-party data centers and infrastructure to deliver Aternity Mobile SaaS. Customer Data is primarily hosted and stored in the data center region selected by Customer. As of this document’s publication date, Customers may designate a primary hosting and storage region from the options below:

- United States
- Australia
- Canada
- Germany
- United Kingdom (*available to UK government customers only*)
- Sweden
- Singapore
- Ireland (only available to existing Aternity Mobile SaaS customers already deployed in Ireland instance)

Additional processing locations may apply to Customer Data; see Riverbed’s [subprocessor list](#) for more details.

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 Aternity Mobile SaaS, who can access that data, and why.

Data Category	Who Has Access	Access Location	Access Purpose
Customer Data	Aternity Mobile DevOps Team	Spain Israel United States	To operate and maintain the Aternity Mobile SaaS platform

DATA PORTABILITY

Customers may export Customer Data at any time via the Aternity Mobile SaaS RESTful API.

DATA SECURITY

The Aternity Mobile SaaS 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 at www.riverbed.com/trust-center.

SUBPROCESSORS

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