Barracuda Cloud Security Guardian

Data Privacy Overview

Overview

This document describes data privacy measures and data storage policies that are specific to the Barracuda Cloud Security Guardian service ("CSG").

Barracuda is dedicated to protecting our customers' privacy and helping them protect the privacy of their users and customers. Our products help customers comply with global, regional, and national privacy regulations, including technical requirements of the General Data Protection Regulation (GDPR).

Barracuda Cloud Security Guardian is an agentless SaaS service that makes it easy to stay secure while building applications in and moving workloads to public-cloud infrastructures. It provides end-to-end visibility of your security posture in your public-cloud deployment and ensures continuous compliance and automated remediation of security controls so that you can better understand and reduce your risk posture.

Data Inventory, Data Protection Impact Assessment (DPIA), and Data Mapping

Barracuda has conducted and maintains a data inventory and data mapping of the collection, transfer, and storage of Personal Information for Barracuda Cloud Security Guardian. Further, the required Data Protection Impact Assessment (DPIA) for applicable controls has been completed and safeguards are in place to mitigate potential risks.

Customer Consent

Barracuda's Data Processing Addendum sets forth each party's rights and obligations with regard to the processing of personal data. Barracuda's Data Processing Addendum for data controllers can be executed at the following address:
https://barracuda.na1.echosign.com/public/esignWidget?wid=CBFCIBAA3AAABLblqZhBqXmYuJpHVTH_mOt4uza7m5WPQS76SAhDubdNrXFYMBHbqQIc5oNXaBTWcQjGhrlU*

Cross-Border Data Transfer

Barracuda complies with the EU – US cross-border data transfer mechanisms approved by the European Commission regarding the collection, use, and retention of Personal Information transferred from the European Union to the United States. Any transfer of customer data outside the European Union will be done in compliance with the GDPR and applicable local privacy laws. Barracuda's Standard Contractual Clauses are located within our DPA at the following address:
https://www.barracuda.com/company/legal/trust-center

Employee Training

Upon hire and annually thereafter, Barracuda employees who have access to customer data undergo security and data privacy awareness training to ensure their continued knowledge of obligations and responsibilities to comply with data protection requirements.

Retention and Right to Be Forgotten (RTBF)

For this product offering, Barracuda is not hosting any associated raw personal information of customers. You may reach out to legal@barracuda.com if you wish to submit a Right to Be Forgotten (RTBF) request for transactional level data.

Data Transmission and Storage

Barracuda CSG does not store any customer data or PII. It reads customer infrastructure telemetry and shares it securely over an encrypted channel to the SaaS solution. Infrastructure telemetry data is stored at rest in AWS Elasticsearch in an AES 256-bit encrypted format.

Access Control

Customers can configure user roles to manage access privileges to the account. More information about this feature is available at the following address:
https://campus.barracuda.com/product/cloudsecurityguardian/doc/78156014/user-management/

Data Location

Barracuda maintains a global network of data centers and annually verifies that each one meets defined security and privacy requirements. The cloud infrastructure for Barracuda Cloud Security Guardian is deployed in the Americas region via AWS. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws.