Barracuda Firewall

Data Privacy Overview

Overview

This document describes data privacy measures and data storage policies that are specific to Barracuda Firewall ("Firewall").

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).

The Barracuda Firewall is an enterprise-grade, next-generation firewall that was purpose-built for efficient deployment and operation within dispersed, highly dynamic, and security-critical network environments. In addition to next-generation firewall protection, the Barracuda Firewall provides industry-leading operations efficiency and added business value by safeguarding network traffic against line outages and link quality degradation.

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 the Firewall. 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 on our Trust Center within the Self Service Center at the following address:
https://www.barracuda.com/company/legal/trust-center

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)

Customers have the ability to configure retention timelines for data passing through the Firewall. By default, data is retained as long as there is disk space. If you wish to send a Right to Be Forgotten (RTBF) request, please send an email to legal@barracuda.com and Barracuda will provide timely updates through the process of data deletion.

Data Transmission and Storage

All data is encrypted in transit using industry-standard TLS encryption. Further, customer data is secured at rest using AES 256-bit encryption.

Access Control

Barracuda personnel cannot gain access to the customer's Firewall unless the customer explicitly opens the portal to allow access (i.e. for troubleshooting or other requested services). Logs of all activities are created and maintained for future reference.

Data Location

The Barracuda Firewall appliance and all respective data resides on the customer's premises.