Barracuda Web Application Firewall (WAF) and Application Delivery Controller (ADC) Service

Data Privacy Overview

Overview

This document describes data privacy measures and data storage policies that are specific to the Barracuda Web Application Firewall (WAF) and Application Delivery Controller (ADC) Service.

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 Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda WAF scans all inbound web traffic to block attacks and inspects the HTTP responses from the configured back-end servers for Data Loss Prevention (DLP).

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 WAF and ADC. 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)

All customer data is stored directly on Barracuda WAF or ADC appliance in the customer's possession. 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

Customer application traffic is encrypted in transit using industry-standard TLS encryption. The WAF appliance and all respective data resides on the customer's premises.

Access Control

Customers have the ability to configure user roles to manage access privileges to the Barracuda WAF by integrating Azure AD. More information about this feature is available at the following address: https://campus.barracuda.com/product/webapplicationfirewall/doc/41108382/how-to-configure-multi-domain-ldap-authentication/

Data Location

Customers host the Barracuda WAF and ADC physical and virtual appliances on-premises. All data is stored on these appliances and is under the customer's control.