Barracuda Advanced Threat Protection

Data Privacy Overview

Overview

This document describes data privacy measures and data storage policies that are specific to the Barracuda Advanced Threat Protection service ("ATP").

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 ATP service analyzes inbound email attachments with most MIME types and publicly accessible direct download links in a separate, secured cloud sandbox, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Service virus scanning features.

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 ATP. 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)

ATP analyzes submitted files for any malicious code. 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

By default, transmission of messages to ATP occurs via TLS.

Access Control

Barracuda personnel have two tiers of access. Access is limited to approved Barracuda Networks personnel on an 'as needed' basis. User activity is logged and stored for future reference.

- Overall access to the infrastructure, which is limited to members of the Advanced Threat Protection team.
- Operating-system-level access, which is limited to individuals with additional SSH credentials.

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 ATP is deployed in the Americas, EMEA, and APAC regions via AWS. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws.