Barracuda Backup Product

Data Privacy Overview

Overview

This document describes data privacy measures and data storage policies that are specific to the Barracuda Backup product.

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 Backup appliance is designed from the ground up for the cloud-integrated systems you depend on today. It gives customers the flexibility to easily backup data whether it be on-premises or in a location of their choice.

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 Backup. 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 the Barracuda Backup 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

The Barracuda Backup server is typically deployed behind the customer's corporate firewall and protected by the same security that the customer uses to protect primary data sources. Communication between the appliance and the Barracuda Cloud is encrypted via a 256-bit encrypted VPN tunnel.

The Barracuda Backup server runs on a hardened Linux kernel. In the event that a security flaw is discovered, updates are pushed out to the cloud-connected device in a security definition administered by Barracuda.

Access Control

In order to provide customers the flexibility to limit access to their Barracuda Backup server, IP login restrictions can be set for each user who has access to the Barracuda Backup account. Those restrictions prevent access to the hosted web user interface from an IP address outside of the range specified.

Data Location

The Barracuda Backup server gives customers the flexibility to easily backup data whether it be on-premises or in a location of their choice.