Barracuda Cloud to Cloud Backup (CCB) Service

Data Privacy Overview

Overview

This document describes data privacy measures and data storage policies that are specific to the Barracuda Cloud to Cloud Backup Service ("CCB").

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 CCB for Office 365 protects Exchange Online and OneDrive for Business data by backing it up directly to Barracuda Cloud Storage. Use Barracuda CCB for Office 365 as an add-on to an on-premises Barracuda Backup appliance or as a standalone subscription without an appliance. For Exchange Online, Barracuda CCB protects all email messages, including all attachments, as well as the complete folder structure of each user's mailbox. In OneDrive for Business, all files under the Documents Library, including the entire folder structure, are protected.

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 CCB. 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)

At the expiration or termination of your service with Barracuda, Barracuda generally stores customer data for 30 days post termination to allow additional time for you to manually export your data or renew your subscription. After this 30-day retention period, Barracuda will fully disable the account and commence deletion of all customer data at its discretion, including any cached or backup copies.

Customers have the ability to define the retention period for their personal information from within the Barracuda Cloud Control interface. 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

Barracuda CCB secures data transfers using HTTPs. Before data is stored in the Barracuda Cloud, CCB breaks protected files down into parts that are variable in size and fingerprints those parts for analysis, comparison, and deduplication. These parts are AES 256-bit encrypted and are written into storage at the Barracuda Cloud in an encrypted state. Data remains encrypted until it is requested for a restore.

Access Control

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

Further, customers use the Barracuda Cloud Control interface to access and manage their CCB accounts. Barracuda Cloud Control supports Multifactor Authentication. Additional information about this feature is available address:
https://campus.barracuda.com/product/cloudcontrol/doc/69960137/multi-factor-authentication-in-barracuda-cloud-control

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