



Barracuda Email Security Gateway (ESG)

Data Privacy Overview



Overview

This document describes data privacy measures and data storage policies that are specific to the Barracuda Email Security Gateway appliance ("ESG").

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 Email Security Gateway manages and filters all inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. Barracuda ESG is delivered to customers in the form of an on-premises or virtual appliance. Customers deploy Barracuda ESG on their internal networks.

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 ESG. 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 ESG 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 only data that is transmitted is email data into the Barracuda ESG appliance. The customer has the ability to determine whether this content is encrypted or in plain text. The ESG appliance and all respective data resides on the customer's premises.

Access Control

Customers can configure user roles to manage access privileges to the Barracuda Email Security Gateway manually or by integrating Azure AD. More information about this feature is available at the following address:

<https://campus.barracuda.com/product/emailsecuritygateway/doc/3866683/creating-and-managing-accounts/>

Data Location

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