



# Barracuda PhishLine

Data Privacy Overview



## Overview

This document describes data privacy measures and data storage policies that are specific to the PhishLine service (“PhishLine”).

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).

PhishLine provides leading-edge user awareness training to counter sophisticated phishing and socially engineered spear phishing attacks. PhishLine helps your users sharpen their anti-phishing skills with advanced phishing simulations along with end-user testing, reporting, and comprehensive metrics that let you take prompt and meaningful action against threats.

## 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 PhishLine. 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.

If you wish to send a Right to Be Forgotten (RTBF) request, please send an email to [legal@barracuda.com](mailto:legal@barracuda.com) and Barracuda will provide timely updates through the process of data deletion.



## Data Transmission and Storage

Barracuda PhishLine maintains campaign data after the customer has completed the training. The campaign data is transmitted over a TLS encrypted connection and data at rest is stored via AES 256-bit encryption in secure data centers.

## Access Control

PhishLine supports SAML integration in which customers have the flexibility to manage access according to their standards.

## 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 PhishLine is deployed in the Americas region via colocation data centers which provide physical and environmental security to the Barracuda infrastructure. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws.