Email Security Privacy Data Sheet

This Privacy Data Sheet explains how Check Point Email Security Solution (formerly known as Harmony Email & Collaboration) processes personal data.

About Check Point Email Security

Check Point Email Security is an innovative security solution for cloud email (Microsoft 365 and Gmail) and collaboration applications. It utilizes technology that enables deployment without requiring changes to mail exchange (MX) records while providing visibility into cloud-based communications and real-time prevention against threats before they reach users' mailboxes. Check Point Email Security secures business communication channels, including file sharing applications such as OneDrive and Google Drive, as well as messaging platforms such as Slack and Microsoft Teams.

Check Point Email Security is an integral part of Check Point's Workspace Security platform, leveraging ThreatCloud AI allowing it to easily integrate with many Check Point security services and other third-party security solutions to provide a comprehensive security solution for the organization's users and assets.

How Does Check Point Comply with Applicable Data Protection Regulations?

At Check Point, ensuring customer privacy and security remains our foremost concern, with the trust our customers place in our services being one of our most valued assets.

- **Security.** As a leading AI-powered, cloud-delivered cyber security platform provider over the past decades, we acknowledge the significance of implementing rigorous security measures to safeguard our customers' information. For more details, visit our Information Security Measures Policy.
- **Privacy by Design.** We operate under the principle of privacy by design. This means that we prioritize the protection of personal data and privacy throughout the entire lifecycle of our products and services. We treat personal data with the utmost care. Our commitment to privacy is reflected in our policies, procedures, and the way we do business. For more details, visit our Privacy Policy and our Trust point

© 2026 Check Point Software Technologies Ltd. All rights reserved.

- **Disaster Recovery.** We maintain comprehensive plans and procedures for disaster recovery and business continuity.
- **Transfers.** In order to regulate the transfer of personal data between the Check Point entities, Check Point has adopted an intercompany agreement for transfers of data between the various Check Point entities, including the EU Standard Contractual Clauses and UK International Data Transfer Addendum to the EU Standard Contractual Clauses. Check Point Software Technologies, Inc. (and its subsidiaries) has self-certified its compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (DPF).

What Types of Personal Data Does Check Point Email Security Process?

Check Point Email Security integrates with Microsoft 365, Google Workspace and other collaboration applications, collecting and processing data that customers have previously shared and stored within these platforms.

This data may include:

- Basic personal data, including name, job title, department/team, corporate email address and phone number
- Data extracted from subscribed mailboxes (including email's subject line, body and attachments)
- Data extracted from instant messages and files shared through apps connected to Check Point Email Security (such as Teams, Zoom and Google)
- URL addresses received in subscribed mailboxes. Such URLs are being scanned for threats detection before the user can click them. Check Point does not process these URLs' actual landing destination content
- Users' email usage patterns within subscribed mailboxes. Such patterns are being monitored in order to detect anomalies and prevent potential takeover threats. For example, Check Point Email Security monitors its users' logging history, including typical sign-in times, email quantities, number of recipients and files, etc. No actual content of the mailbox is being monitored for the purpose of establishing users' email usage patterns
- Activities performed by users within the Check Point Email Security dashboard, such as login time, duration of connectivity, etc.
- Action taken by administrators, which are fully logged
- Data provided through the Check Point Email Security dashboards and/or periodic reports. Such data is available to administrators and contains mostly aggregated data relating to blocked threats, but it may also contain personal data relating to certain users. For example, a report may contain a list of email addresses that experienced high numbers of potential attacks

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Why Does Check Point Email Security Process Data?

Check Point Email Security processes information to provide real-time prevention for email-based threats, as well as for threats found in collaboration tools and shared files. Check Point Email Security utilizes ThreatCloud AI to inspect files and URLs. As a global threat prevention AI service, ThreatCloud AI also saves the artifacts it inspects for research and troubleshooting purposes.

For additional information regarding the processing performed by ThreatCloud AI, please refer to the ThreatCloud AI Privacy Data Sheet.

For customers purchasing Check Point Email Security extended archive service, Check Point may retain data for a duration of up to 10 years, as per the specific instructions provided by the customer.

For more information on the purposes for which we process personal data, please visit our Privacy Policy.

What Is the Duration and Frequency of Processing?

Personal data may be processed by Check Point Email Security throughout the subscription term. Mailbox's content is being scanned upon onboarding to detect overlooked threats and assemble users' usage patterns.

What Are the Retention Periods?

Data Type	Retention Period
Emails not classified as Harmful	14 days *
Quarantined Emails	180 days*
Not-quarantined shared files in file storage applications	24 hours
Quarantined / Cleaned shared files in file storage applications (e.g., OneDrive, SharePoint, Teams, Google Drive etc.)	180 days
Email / File / Message Metadata	180 days
Inspected Teams messages	180 days
End User's Basic Personal Data	Duration of subscription term + 3 months following the end of subscription term, for the purpose of allowing the customer to renew the service
Archive (additional paid add-on)	Extended retention period of up to 10 years.

* Customers may configure the retention periods for emails not classified as harmful and quarantined emails and may reduce the retention period to as little as 2 days.

** Files, URLs, and other security artifacts inspected by ThreatCloud AI may be retained in accordance with the ThreatCloud AI retention practices. For additional information regarding applicable retention periods, please refer to the ThreatCloud AI Privacy Data Sheet.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Where Is Personal Data Stored?

Personal data is stored in Check Point cloud hosting environments, including infrastructure provided by third-party cloud service providers. The hosting locations available are: U.S., EU, Australia, India, Canada, United Kingdom, Israel, Singapore, and United Arab Emirates. The location is selected per customer's choice during the onboarding process.

Sub-Processors

Check Point engages third-party Sub-processors in connection with the provision of the Check Point's products and services. The list of Sub-processors is available at our Sub-Processors Page.

Privacy Options

We provide the following tools, empowering our customers to select their data and privacy preferences:

- Scoping the protected applications and users - Check Point Email Security allows administrators to select the protected applications and the users that will be monitored.
- Restricting storage of emails content classified as harmful - Administrators may choose how to store emails classified as harmful – they can either choose to fully store, store obfuscated or partly or not store at all.
- Restricting users' access to certain data, per customer's choice.

Authorized Access to Personal Data

Customer Access

Access to data is controlled by the Customer's system administrator. Only users authorized by the administrator can access the data. All access and actions performed by administrators and authorized users are fully logged.

Check Point Access

Data contained within the customer's Check Point Email Security environment may be accessed by Check Point's support and R&D teams for troubleshooting and security purposes. Such access is granted only to those authorized representatives for which access is necessary to perform their intended functions.

Information contained in this data sheet is for awareness only, may be modified, and does not constitute legal or professional advice or warranty of fitness for a particular purpose. This Privacy Data Sheet is a supplement to Check Point's Privacy Policy. Please visit it for more information on how Check Point collects and uses personal data.

© 2026 Check Point Software Technologies Ltd. All rights reserved.