CHECK POINT

Harmony SASE

This Privacy Data Sheet explains how Check Point's Harmony SASE processes personal data.

About Harmony SASE

Check Point's Harmony SASE (Secure Access Service Edge) solution is specifically designed to secure modern, distributed workforces by offering a unified platform for security and networking. Tailored for hybrid work environments, it addresses the complexities of protecting both cloud-based and on-premises networks while ensuring secure access for remote employees and branch offices. Harmony SASE consolidates critical network and security services into a single solution, enhancing both performance and protection through a combination of cloud-based and on-device security measures.

Key features include accelerated internet security, zero-trust network access, secure web gateways, and advanced data protection tools. Harmony SASE meets the growing need for secure remote work and cloud-based applications, making it an indispensable tool for businesses navigating the digital age.

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 its various Check Point entities, including the EU Standard Contractual Clauses and UK International Data Transfer Addendum to the EU Standard Contractual Clauses. Check Point's U.S. subsidiary, 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 Harmony SASE Process?

Harmony SASE processes the following Personal Data:
- Identifiers: Name, email address

Harmony SASE may process Personal Data, which may include the following categories:
- Device Information: Device name, operating system version, assigned IP address, user IP address.
- Session and Authentication Data: Session tokens, user-agent strings.

The information above relates to Harmony Internet Access and Remote Access.

Why does Harmony SASE Process Personal Data?

Harmony SASE processes personal data to provide secure and efficient network and security services by authenticating users and devices, managing access rights, and ensuring secure connectivity to corporate networks and cloud environments. It identifies and mitigates security threats, optimizes network performance, enforces compliance with Customer's predefined policies, and supports incident detection and resolution.

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

What is the Frequency of Processing?

Data is shared with Harmony SASE throughout the subscription term.

Where is Personal Information Stored?

Personal information is stored on AWS Cloud Hosting Service. The hosting locations available are: Canada, United States, EU, Australia, and India. The location is selected per customer's choice during the onboarding process.

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

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 and Security Controls

We provide the following tools, empowering you to select your data privacy preferences:

- Role-Based Access Control (RBAC) ensures that only authorized users can access specific data.
- Customers may integrate their Identity Provider (e.g., Azure AD, Okta, Google) to enable seamless and secure access management.
- Tools such as Datadog, along with native monitoring features provided by AWS and MongoDB Atlas, are utilized to track system performance, and identify anomalies.
- Comprehensive logs provide detailed visibility into system activities, including user behavior and configuration changes.
- Select cloud location based on data residency when creating the tenant.

Authorized Access To Personal Data

Customer Access

Access to data is controlled by customer's selected administrators. Only users authorized by the administrators can access data.

All access and any action taken by administrators or by their authorized users are fully logged.

Check Point Access

Data contained within the customer's 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.