



Playblocks Privacy

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

About Playblocks

Playblocks is a cloud-based security automation and response platform that enables organizations to automatically trigger preventive and response actions across their security environment based on customer-configured workflows and triggers. Playblocks helps organizations identify, contain, and respond to security events while reducing operational overhead.

It works by coordinating collaborative, cross-product responses - such as isolating hosts, blocking malicious activity, and notifying administrators - based on customer-configured workflows, schedules, webhooks, and event-driven triggers

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 cybersecurity 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, please visit our [Privacy Policy](#) and our [Trust Point](#).

- **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 US 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 Playblocks Process?

Playblocks analyzes logs received from Check Point products and customer-configured third-party security integrations.

Logs from Check Point products become available to Playblocks when the customer connects the relevant management system to the cloud and enables configuration sharing. Additional logs and security information may be received from customer-configured third-party integrations.

Personal data processed by Playblocks may be contained within these logs, security records, and content uploaded or submitted to Playblocks agents, where such information contains personal data.

Such personal data may include:

- IP addresses
- Usernames
- Hostnames, where they identify or may identify an individual
- Personal data contained in customer-configured third-party integrations
- Other identifiers contained in source logs, integration data or content submitted to Playblocks agents

The specific personal data processed depends on the customer's configuration and the data sources connected to Playblocks.

Why Does Check Point Playblocks Process Personal Data?

Playblocks processes personal data to provide its security automation and response capabilities, including security monitoring, authentication, alerting, reporting, automation execution, incident investigation, and historical analysis.

For more information on the purposes for which we process personal data, please visit our [Privacy Policy](#).

What is the Frequency and Duration of Processing?

Personal data may be processed on a scheduled basis or when customer-configured events trigger an automation workflow. The frequency of processing therefore depends on the customer's configuration and operational activity. Processing occurs for the duration of the relevant automation or agent execution.

What Are the Retention Periods?

Logs, execution history, and related operational records may be retained for up to 12 months to support investigation, historical analysis, and service operations. Retention periods may vary depending on the functionality used and the manner in which the information is collected and processed.

Where is Personal Data stored?

Personal data is stored in Check Point cloud hosting environments, including infrastructure provided by third-party cloud service providers. Available hosting locations are EU, US, Canada, Australia, and India. The location is selected according to the customer's choice during the onboarding process, which should align with the location of their tenant.

Sub-Processors

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

Authorized Access to Personal Data

Customer Access

Access to data is controlled and managed by the Customer's system administrator.

Check Point Access

Access to data is restricted to authorized representatives whose access is necessary to perform their intended functions.

The information contained in this Privacy Data Sheet is provided for information purposes only, may be modified from time to time, and does not constitute legal or professional advice or a warranty of fitness for a particular purpose.

This Privacy Data Sheet supplements Check Point's [Privacy Policy](#). Please visit it for more information on how Check Point collects and uses personal data.

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com