Workforce AI Security Privacy Data Sheet

This Privacy Data Sheet explains how Check Point Workforce AI Security processes personal data.

About Check Point Workforce AI Security

Check Point Workforce AI Security provides an enterprise GenAI security solution that empowers organizations to adopt GenAI tools - safely and responsibly. It combines advanced data loss protection (DLP) and in-depth visibility into GenAI usage.

Key Capabilities include:

- **GenAI Discovery & Risk Assessment** – Provides comprehensive visibility into AI tools, agents, and AI-related activities across supported web and desktop applications, SaaS integrations, browser extensions, code assistants, AI agents, and Model Context Protocol (MCP) integrations, including shadow AI usage. Delivers insights into AI usage patterns, workflow context, data flows, and agentic behaviors, and automatically categorizes AI-related activities by use case (e.g., documentation, code generation, debugging, data analysis) to help security teams assess organizational risk and enforce acceptable use policies.

- **Governance & Access Controls** – Enables granular access and security policies for enterprise-managed and shadow AI applications. Governs SaaS integrations, agent actions, data types, and AI-related activities to help organizations manage AI usage in alignment with internal security and compliance policies.

- **Inline Prompt & Data Protection** – Helps prevent users from submitting prompts, pasting text, or sharing files and images containing customer-defined sensitive data with GenAI tools such as ChatGPT, Copilot, Gemini, and Claude. AI-powered contextual analysis helps identify sensitive content across predefined and custom data categories tailored to organizational requirements.

- **GenAI-Aware DLP** – Helps prevent sensitive data exposure through contextual DLP, file and image redaction, OCR, and runtime designed to enforce customer-defined policies before restricted agentic actions are executed.

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

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

- **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 Workforce AI Security Process?

Check Point Workforce AI Security processes the following types of personal data for the categories of data subjects defined by the customer and according to the security policy established within Check Point Workforce AI Security:

- **User and Device Information:** Device name, device ID, MAC address, username, IP address. and organizational unit assignment (e.g., department, team, business unit).

- **Information provided by the user,** including prompts, copied text, file uploads, images, and related interactions with AI tools (such as tool invocations and skills usage), which may be analyzed in accordance with customer-defined policies, with controls enforced based on those policies.

- **Website classification data:** Website URLs processed to determine whether a website constitutes an AI service, in accordance with customer security policies.

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

Why Does Check Point Workforce AI Security Process Personal Data?

Check Point Workforce AI Security processes personal data to enforce customer-defined data loss prevention (DLP) policies and provide visibility into GenAI tool usage. Prompts are scanned for sensitive content in accordance with customer-defined policies.

The product assesses prompt risk levels based on various factors, such as data types, the AI tool used, customer-defined policies, and product-defined risk categories.

If a prompt is identified as matching a risk category, Check Point Workforce AI Security generates a description of the identified risk and presents it to authorized administrators, including in cases where no blocking or access restriction is applied.

By default, prompt content is not visible to the organization. Administrators can configure role-based access controls to define which authorized personnel may review prompts flagged under customer-defined risk policies (e.g., no visibility, high-risk only, or all risk levels). Administrative actions and configuration changes relating to prompt visibility settings are logged and auditable.

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 by Check Point Workforce AI Security throughout the subscription term.

What are the Retention Periods?

Data Type	Retention Period
Device Information	90 days
Information provided by the user	90 days

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: United States, and the EU. The location is selected according to the customer's choice during the onboarding process, which should align with the location of the customer tenant.

© 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 Options

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

- The system honors user-level authorizations based on role-based access control (RBAC) settings. Prompt visibility within the platform is managed according to assigned permission level.
- Customer administrators can configure which authorized personnel may review prompts flagged as high-risk, critical-risk, or otherwise matching customer-defined risk policies.
- Administrative actions and configuration changes relating to prompt visibility settings are logged and auditable.
- Customer administrators can set whether files and images are included in the prompt scan review.
- Customer administrators can configure policies to allow or block specific AI tools, users, or event types, in which case prompts associated with allowed AI tools or use cases may not be scanned or displayed, in accordance with the customer's policy configuration.

Authorized Access to Personal Data

Customer Access

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

Check Point Access

- Access to any data is restricted to 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.