Check Point AI Guardrails (Lakera Guard)

This Privacy Data Sheet explains how Check Point AI Guardrails processes personal data in connection with the provision of the service.

About Check Point AI Guardrails

Check Point AI Guardrails is an AI-powered security layer designed to provide organizations with an enterprise security solution to protect their use of large language model (LLM) applications from prompt injections, data leakage, policy bypass attempts, and other AI-related threats. It analyzes customer-submitted LLM inputs and outputs to detect malicious patterns, unsafe content, and policy violations, and provides structured threat intelligence, analytics, and developer tooling to secure AI applications.

On-Premises and Private Cloud (Self-Hosted) Version

Check Point AI Guardrails is also available in an on-premises or private cloud self-hosted deployment model.

In such deployments, personal data processed by the solution remains within the Customer's controlled environment and is not transmitted to or shared with Check Point, except where explicitly required for support, maintenance, or other services as agreed with the Customer.

Accordingly, the data processing practices described in this Privacy Data Sheet apply only to the cloud-hosted version of Check Point AI Guardrails.

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.

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

- **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 AI Guardrails Processes?

Check Point AI Guardrails processes the following categories of personal data, as submitted by Customer or generated in the course of delivering the service:

- **Administrator & User Account Information:** Administrator name, business email address, organization and user IDs, role information, and account configuration details.
- **Device & Technical Information:** IP address, session ID, timestamps, request metadata, token counts, prompt embeddings, and API usage logs.
- **Information Provided by the User or Processed by the AI Tool:** Prompts, messages, system prompts, tool information, uploaded files (if enabled), LLM-generated outputs, redacted personal data indicators, and security analytics derived from those inputs (e.g., threat categories, confidence scores).

Why Does Check Point AI Guardrails Process Personal Data?

Check Point AI Guardrails processes personal information to enforce customers' data loss prevention (DLP) policies and provide visibility into GenAI tool usage; detect and prevent unsafe or malicious activity and provide security insights and analytics.

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

Please note: Check Point AI Guardrails does not display the name of the user who uploaded the prompt. Additionally, when Check Point AI Guardrails detects personal identifiers in the prompt content - such as names, email addresses, IP addresses, credit card numbers, IBANs, or SSNs - it will mask them during the prompt review.

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?

Data may be processed by Check Point AI Guardrails throughout the subscription term.

What are the Retention Periods?

Data is retained for the duration of the subscription and for three (3) months after termination.

Where is Personal Data Stored?

Personal data is stored in Check Point cloud hosting environments, including infrastructure provided by Amazon Web Services (AWS). The hosting locations available are: EU, U.S, Singapore.

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 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:

- Customers may configure policies controlling what content is sent to the service
- Customers may delete prompts or request deletion through the service interface
- Customers may disable or restrict the retention of pseudonymized prompts

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

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.