AIOps Privacy Data Sheet

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

About AIOps

The AIOps is an advanced monitoring and operational intelligence solution designed to proactively manage the health and performance of Check Point Security Gateways and Servers. By leveraging AI and automation, AIOps continuously analyzes system behaviour, detects anomalies, and provides actionable insights to prevent outages, optimize resource usage, and reduce operational workload.

AIOps delivers end-to-end visibility into asset health, real-time metrics, and enriched alerts with root cause analysis and remediation guidance.

AIOps is designed to enhance uptime, simplify operations, and strengthen the security posture of organizations by providing intelligent, automated operational support across their infrastructure.

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 AIOps Process?

The AIOps processes the following personal data:

Configuration settings may include object names, gateway topology, IP addresses, and other configuration elements as defined by the customer (not personal data by default). Configuration settings are intended for technical and operational purposes and are not designed to include personal data beyond what is operationally necessary (e.g., IP addresses used for network security). Customers are advised not to include additional personal data in configuration elements, such as naming objects after individuals or assigning identifiers that directly relate to specific persons.

Telemetry data is collected as part of diagnostic processes. This data consists of system-generated information used for service operation, performance monitoring, and troubleshooting.

Optional log sharing

AIOps may process personal data as part of log sharing, where this capability is enabled or purchased by the customer. Such data may include access logs (traffic logs).

Why does AIOps Process Personal Data?

The AIOps processes data to deliver proactive and preventive monitoring capabilities for Check Point products, supporting system performance, reliability, and minimizing downtime. 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 shared with AIOps throughout the subscription term (per configuration sharing and log sharing policy).

What are the Retention Periods?

Data Type	Retention Period
Configuration data and log data (if enabled by the customer)	In accordance with the customer's configuration and applicable service settings.
Alerts and insights (generated when anomalies or predefined conditions are detected)	3 months following termination of the subscription

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 EU, US, Australia, and India. The location is selected per customer's choice during the onboarding process.

* Support for Canada is anticipated in 2026

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 preferences:

- Restricting users' access to certain data, per customer's choice.
- Disabling diagnostics reporting to Check Point, per customer's choice.

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.