Infinity Threat Exposure Management

This Privacy Data Sheet explains how Check Point's Infinity Threat Exposure processes personal data.

About Infinity Threat Exposure Management

Check Point's Infinity Threat Exposure offers Preemptive Exposure Management (PEM). It proactively identifies, prioritizes, and remediates risks across the entire security stack on-prem and in the cloud.
By efficiently integrating with your current security solutions, you can remove operational silos, achieve unified visibility into exposures, and address security gaps and misconfigurations proactively while maintaining uninterrupted business operations.

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.
1.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.

2. 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.

3. Disaster Recovery. We maintain comprehensive plans and procedures for disaster recovery and business continuity.

4. Transfers. In order to regulate the transfer of personal data between the Check Point entities, Check Point has adopted an intercompany agreements 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 Infinity Threat Exposure Management Process?

Infinity Threat Exposure processes the following information:

• Contact details of organization administrators and platform users (as defined by the customer), such as business email address.
Infinity Threat Exposure may also process the following information as part of providing the service, to the extent it constitutes personal data:
• Information included in the customer-configures security controls, such as IP addresses, usernames, profiles, or DNS information, where these data elements relate to an identifiable individual.
• Host IP address, where the IP address is associated with a detected vulnerability or threat.
• Name of the vulnerable instance, where such name includes personal data (depending on customer configuration).

Why does Infinity Threat Exposure Management Process Personal Data?

Infinity Threat Exposure processes personal data to support its ability to:
• **Continuously identify and remediate security risks** across multi-vendor environments, including firewalls, endpoints, WAFs, and cloud platforms.

• **Enforce real-time threat intelligence** by detecting and verifying indicators of compromise (IoCs) and applying protections across the security stack.

• **Enable automated, context-aware remediation** that is safe and tailored to each customer's environment.

This processing is essential for Infinity Threat Exposure 's ability to deliver proactive, non-disruptive security coverage and virtual patching across integrated systems.
For more information on the purposes for which we process personal data, please visit our Privacy Policy.

What is the Frequency

As an on-premises deployment, Personal Data is shared with Infinity Threat Exposure at the customer's discretion, where data sharing has been enabled, and for the duration of the subscription term.

What are the Retention Periods?

Data Type	Retention Period
Administrators contact details	Subscription term
Personal data that may be associated with a detected vulnerability or threat	14 days

Where is Personal Data Stored?

Where personal data is shared, it may be stored on servers in the United States.

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 tools, empowering our customers to select their data and privacy 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 Customer's system administrator and is managed by the customer.

Check Point Access

- On-premises deployments do not provide Check Point with access to customer data.

- Where data sharing is enabled by the customer, access to such data is limited to authorized representatives and only to the extent necessary to perform their assigned functions.