

Identity and Trust Privacy Data Sheet

This Privacy Data Sheet explains how Check Point's Identity and Trust processes personal data.

About Identity and Trust

Check Point Identity and Trust is an identity security solution that helps organizations centralize identity-based information across their environments.

The product analyzes identity activity and authentication events from identity providers (systems that manage user identities and authentication), endpoints, and cloud services and maps IP addresses to user identities, devices, and organizational attributes. The product connects to customer-selected systems ("connectors") and processes data based on permissions granted by the customer.

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 Identity and Trust Process?

Check Point Identity and Trust processes certain Personal Data related to users, devices, and group membership (organizational groups or roles) to calculate identity-based information and provide security monitoring and enforcement capabilities.

Directory sync (connection to customer identity directories such as identity providers, as configured by the customer). The product processes:

- Usernames
- Device names
- User email addresses
- User login attributes
- User and device directory attributes
- Group membership (organizational groups or roles)

Login information (received from integrations configured by the customer, such as identity or access systems). The product processes:

- User and/or device login attributes
- Device IP address

The scope of Personal data processed depends on the directories and integrations configured by the customer.

Why does Check Point Identity and Trust Process Personal Data?

The Identity and Trust processes data to allow real-time identity-based enforcement and monitoring capabilities in Check Point products.

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?

Personal data is processed on a continuous basis for the duration of the subscription term.

What are the Retention Periods?

Data Type	Retention Period
Directory information	Directory information is kept for ongoing use. In case the customer deletes the identity provider (IDP) or disconnects the directory sync, the data is deleted within up to 24 hours from this action. *
Login information	Default expiration time (typically a few hours). Data is deleted upon expiration if no update is received. Retention may vary depending on the integration type and configuration and may be retained for a defined duration (e.g., up to 12 hours from the last activity, unless otherwise configured).

* Data deletion is triggered by disconnection of the relevant identity provider or directory integration.

Where is Personal Data Stored?

Personal information is stored in Check Point cloud hosting environments (including AWS). The hosting locations available are EU, U.S, Australia, Canada, 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 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 can limit which directory information is synchronized to Check Point Identity and Trust using the SCIM standard (a method for exchanging identity data between systems), where supported by their identity provider.
- Customers can configure filters to include or exclude login information.

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.