Check Point Cloud Firewall as a Service Privacy Data Sheet

This Privacy Data Sheet explains how Check Point's Cloud Firewall as a Service processes personal data.

About Check Point Cloud Firewall as a Service

Check Point Cloud Firewall as a Service includes firewall infrastructure management by Check Point security experts, coupled with native integration with cloud vendor control planes to improve operational visibility, and enable dynamic policies based on cloud tags. This enables teams to leverage cloud infrastructure monitoring and logging frameworks as part of their security operations. This is increasingly important as organizations rely on cloud network firewalls and WAF to secure their GenAI applications. Cloud Firewall as a Service helps customers maintain compliance, reduce manual effort, and strengthen their overall cloud security posture.

The Cloud Firewall as a Service operates by routing customer traffic from the customer's cloud network to Check Point's Cloud Network (the as a Service dedicated network) for processing in Firewall modules.

Check Point Cloud Firewall as a Service is a cloud-native security gateway, identical in architecture to Check Point Network Security (formerly known as CGNS), that is owned by Check Point and infrastructure managed by Check Point in the cloud.

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 agreement 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 Check Point Cloud Firewall as a Service Process?

- **Firewall:** The firewall of the Check Point Cloud Firewall as a Service does not actively process any personal information. It works at the gateway level, handling data like Gateway MAC addresses and device hostnames which are used to distinguish between VMs. This data stays within the gateway and is not associated with any individual user or person. Additionally, based on your preference, logs can be stored on a log server owned by you. These logs are not shared with Check Point.

- **Threat Prevention:** Check Point Cloud Firewall as a Service integrates Check Point's Threat Prevention solution (depending on your selected Cloud Firewall as a Service). For additional information regarding Check Point's Threat Prevention privacy data sheet please click here.

- **Customer-defined tags:** Check Point Cloud Firewall as a Service reads and processes customer-defined cloud resource tags to support policy configuration and enforcement. Cloud Firewall as a Service does not require or control the content of these tags. However, if a customer includes personal data within a tag (for example, a name or email address), this information may be processed as part of the service when the scanner analyzes the tags.

Why Does Check Point Cloud Firewall as a Service Process Personal Data?

Check Point Cloud Firewall as a Service processes personal data primarily to enhance the security and integrity of network environments, protect users, and comply with regulatory requirements.

Where personal data appears within customer-defined tags, it is processed to support policy logic and enforcement.

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?

Data is shared with Check Point Cloud Firewall as a Service throughout the subscription term.

What Are the Retention Periods?

Check Point Cloud Firewall as a Service does not retain personal information as part of its core functionality.

If customer-defined tags contain personal data, it is processed only as needed to operate the service and is not retained by Check Point beyond this operational use.

Additionally, Check Point Cloud Firewall as a Service integrates Check Point's Threat Prevention solution (depending on your selected Cloud Firewall as a Service Network Security package). For additional information regarding Check Point's Threat Prevention privacy data sheet please click here.

Where Is Personal Data Stored?

Check Point Cloud Firewall as a Service is designed to secure and manage cloud network environments and does not require the storage of personal data as part of its core functionality.

Check Point Cloud Firewall as a Service does not persistently store personal data within Check Point–controlled systems. However, if a customer includes personal data within customer-defined cloud resource tags, this information may be processed transiently by the cloud-based scanner solely to support policy configuration and enforcement. Such tag information is not stored by Check Point outside the operational workflow.

Any logs or configurations that contain customer-defined tags or other customer-generated data remain within the customer's secure environment, unless the customer chooses otherwise.

For additional information regarding Check Point's Threat Prevention privacy data sheet please click here.

Privacy Options

At Check Point, we provide the following configurations, empowering our customers to select their data and privacy preferences:

- **Restricting users' access to certain data, per customer's choice:** Customers can define which users within their organization can access specific security configurations and security logs. This allows organizations to maintain strict separation of duties and enforce role-based access control.
- **Security policy and logging control:** Customers manage and configure the security policy and security logging. Security logs are regularly collected by the SmartCenter or Log Server.
- **Infrastructure management:** As the Firewall modules are owned and operated by Check Point, internal infrastructure information (including storage status, system telemetry, and platform-level details) is not exposed to the customer. Access to the underlying infrastructure is restricted to authorized Check Point personnel under strict access control procedures.
- **Disabling diagnostics reporting to Check Point, per customer's choice:** Customers are offered the option to disable the automatic transmission of diagnostic data to Check Point. Diagnostic data, such as system performance metrics and technical error reports, is intended not to include Personal Information. By disabling this feature, customers can prevent the transmission of such technical telemetry.
- **Data residency:** Customers can select cloud location based on data residency when creating the tenant.

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
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.