CHECK POINT™

CloudGuard
Network
Security

CloudGuard Network Security

This Privacy Data Sheet explains how Check Point's CloudGuard Network Security processes personal data.

About CloudGuard Network Security

Check Point CloudGuard Network Security is a cloud-native security gateway that provides advanced threat prevention along with automated and flexible cloud network security. It is managed by unified security management and supports the broadest array of public, private, and hybrid cloud environments.

CloudGuard Network Security is an integral component of the CloudGuard Cloud Native Security platform, providing automated and scalable public cloud network security. CloudGuard Network Security is aimed to ensure your assets and data are safeguarded while adapting seamlessly to the ever-changing requirements of public cloud environments.

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 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 CloudGuard Network Security Process?

- **Firewall:** The firewall of the CloudGuard Network Security 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:** CloudGuard Network Security integrates Check Point's Threat Prevention solution (depending on your selected CloudGuard Network Security package). For additional information regarding Check Point's Threat Prevention privacy data sheet please click here.
- **Customer-defined tags:** CloudGuard Network Security reads and processes customer-defined cloud resource tags to support policy configuration and enforcement. CloudGuard 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 CloudGuard Network Security Process Personal Data?

CloudGuard Network Security 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 CloudGuard Network Security throughout the subscription term.

What are the Retention Periods?

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

CloudGuard Network Security is designed to secure and manage cloud network environments and does not require the storage of personal data as part of its core functionality.

Where is Personal Data Stored?

CloudGuard Network Security 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.

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

At Check Point, we are committed to empowering our customers to control their data and privacy preferences. To ensure maximum flexibility and compliance with data protection regulations, we provide the following privacy tools:

- Restricting users' access to certain data, per customer's choice: Customers have the ability to define which users within their organization can access specific data sets or security configurations. This allows organizations to maintain strict separation of duties and enforce role-based access control.
- 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. While diagnostic data, such as system performance metrics and error reports, which do not include any Personal Information, can help optimize security operations and ensure proactive support, we recognize the need for control over data sharing. By disabling this feature, customers can prevent the transmission of system-related information, ensuring that no performance or usage data is shared.

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

CloudGuard Network follows a customer-managed deployment model. This approach gives you complete control over your configuration and operation. Check Point will only have access to your environment if you explicitly grant them permission.

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.