

# Check Point Browser Security Privacy

*This Privacy Data Sheet explains how Check Point Browser Security processes personal data.*

WE SECURE YOUR AI TRANSFORMATION

## About Check Point Browser Security

Check Point Browser Security is a browser-based security solution that protects users directly inside the web browser. It provides capabilities such as Zero Phishing protection, Sandboxing & Threat Extraction (CDR), URL Filtering, Corporate Password Reuse prevention, Safe Search, Search Reputation, and, in its advanced license, Browser-based Data Loss Prevention (DLP). It is delivered via a browser extension and a lightweight executable, designed for quick deployment, cloud-only management, and seamless protection of web browsing activity across supported browsers.

## 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 Check Point Browser Security Process?

Check Point Browser Security processes the following types of personal data in order to provide its browser-based security functionality:

- **User and Device Information:** Username of users synced by the organization, email address, computer/device name, organization domain,
- **Network and Technical Identifiers:** IP address, domain names and URLs accessed, web browser type and version, registry keys
- **Activity and Content-Related Data:** Folder and file names, page titles, limited portions of webpage content (e.g., text extracts), limited portions of HTML page headers, favicon (website-associated icon)
- **Geolocation Data:** General geographic location (derived from IP or similar signals)
- **Files:** Files uploaded by the users to pre-defined webpages

The above data elements may be collected directly by the product as part of its operation or provided by the customer during user and device enrollment, including via integrations with directory services (e.g., Active Directory or UEM). The scope of personal data processed depends on customer configuration, enabled features, integrations, and implementation.

## Why Does Check Point Browser Security Process Personal Data?

Check Point Browser Security processes personal data for the purpose of providing browser-based security, threat prevention, and related administrative monitoring and management capabilities. Specifically, personal data is processed for the following purposes:

- **Security Monitoring and Threat Detection:** To detect, analyse, and prevent cyber threats such as phishing attacks, malware, malicious websites, and credential compromise attempts.
- **User and Device Identification:** To associate a device with a specific user within the organization and enable policy application, security management, and event correlation at the user or device level.
- **Alerting and Incident Response:** To generate alerts and enable administrators to investigate and respond to detected threats, including associating security events with relevant users or devices.
- **Geolocation-Based Analysis:** To derive general location information (based on IP address or similar signals) in order to identify anomalous or potentially risky access patterns.
- **Threat Hunting and Forensics:** To support the investigation of suspicious or malicious activity by providing relevant telemetry, which may include user-linked data such as usernames, device identifiers, file names, or URLs.
- **Reporting and Administration:** To provide administrators with visibility into security events, user activity, and device status through the management dashboard, and to support reporting and policy management capabilities.

Check Point Browser Security is designed to primarily process technical and security-related data. Where limited content inspection is required (for example, for phishing detection or data loss prevention), such inspection is minimized and performed solely for security purposes.

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?

Personal data is processed on a continuous basis as part of the service's real-time security functionality throughout the subscription term.

Processing occurs in real time in response to user browsing activity, including access to web content and file downloads. Certain processing activities may also be performed on-demand, for example when administrators investigate security events or when files are analyzed for threats.

## What are the Retention Periods?

| Data Type                         | Retention Period * |
|-----------------------------------|--------------------|
| User and Device Information       | Up to 90 days      |
| Network and Technical Identifiers | Up to 90 days      |
| Activity and Content-Related Data | Up to 90 days      |
| Geolocation Data                  | 7 days             |
| User and Device Information       | Up to 90 days      |
| Files                             | Up to 10 minutes   |

Files, URLs, and other security artifacts inspected by ThreatCloud AI may be retained in accordance with the ThreatCloud AI retention practices. For additional information regarding applicable retention periods, please refer to the ThreatCloud AI Privacy Data Sheet.

## Where is Personal Data stored?

Personal data is stored in Check Point cloud hosting environments, including infrastructure provided by third-party cloud service providers. Available hosting locations are US and EU. The location is selected according to the customer's choice during the onboarding process.

## 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 configuration options that enable customers to manage access to data and integrate Browser Security with their organizational environment:

- **Log Export Configuration**—Customers may export logs and security events in accordance with their operational and compliance requirements.
- **Identity Provider (IdP) Integration**—Customers may integrate Browser Security with their identity management systems to support user management and authentication workflows.
- **Strong Authentication Controls**—Customers may implement strong authentication mechanisms for administrative and user access, subject to the capabilities of the integrated identity provider.
- **Files Scans**—Files will be scanned only in accordance with the Customer's specifically designated policy rules that enable Threat Emulation and Threat Extraction for files.

## 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 personal data is restricted to authorized representatives for whom access is necessary to perform their intended functions.

*The information contained in this Privacy Data Sheet is provided for information purposes only, may be modified from time to time, and does not constitute legal or professional advice or a warranty of fitness for a particular purpose.*

*This Privacy Data Sheet supplements Check Point's [Privacy Policy](#). Please visit it for more information on how Check Point collects and uses personal data.*

#### **Worldwide Headquarters**

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

#### **U.S. Headquarters**

100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

[www.checkpoint.com](http://www.checkpoint.com)