# Products Policy

This Policy was last updated in December 2022.

## Antivirus

### Antivirus for Desktop (Mac and Windows)

#### Official Product Name

Avast Free Antivirus, Avast Internet Security, Avast Premium Security, Avast Premier, Avast Pro Antivirus, Avast Security Pro, Avast Security for Mac, Avast Premium Security for Mac

Avast Business Antivirus, Avast Business Antivirus Pro, Avast Business Antivirus Pro Plus, Avast Business Patch Management, Avast Business Management Console, Avast Business Antivirus for Mac, Avast Business Antivirus for Linux

(collectively as “Antivirus for Desktop”)

#### Core Functionality

The Antivirus for Desktop provides protection against malicious, harmful or unwanted software and technologies by performing key tasks, such as pinpointing specific files for the detection of malwares, scheduling automatic scans, and securing your device against malware. It may also detect threats to your online privacy and inform about possible protections against these risks.

#### What are Product’s Main Features

- **Smart Scan** is a comprehensive scan that detects browser threats, outdated applications, hidden viruses, system and privacy threats and other issues at the same time.

- **CommunityIQ** is a threat monitoring service for Windows and Mac which sends information about a threat detected in your device (samples of suspicious files and detection metadata) to our server, so we can observe how the threat spreads and block it. This is vital for the functioning of our Antivirus and our ability to keep your device secure.
- **CyberCapture** detects and analyses rare, suspicious files on your Windows. If you attempt to run such a file, CyberCapture locks the file from your PC and sends it to our Threat Lab where it is analysed in a safe, virtual environment. All files are uploaded over an encrypted connection, which means your data is inaccessible to hackers.
- **File Reputation** provides a real-time comparison with an up-to-date list of malware databases of executable files sourced from users of Windows who participate in the service. FileRep processes files or their hashed versions to evaluate which are infectious and updating virus databases.
- **Online Security** is a browser plug-in which needs to be specifically activated which checks if the site isn't malicious or phishing.
- **Browser Cleanup** is a module inside Antivirus for Desktop (Windows) which inspects the browser extensions of most browsers, tries to identify malicious extensions and offers to remove them. Browser Cleanup is on by default.
- **Web Shield** scans data that is transferred when you browse the internet in real-time to prevent malware from being downloaded and run on your computer. By default, Web Shield is on and configured to provide optimal protection when switched on.
- **File Shield** scans programs and files saved on devices for malicious threats in real time before allowing them to be opened, run, modified, or saved.
- **Email Guardian** is a cloud-based service which monitors emails from supported providers, scans them the minute they hit your inbox and flags them as malicious if they contain a threat. This feature processes for its functionality, products and business improvement personal data, such as e-mail and its content, including attachments. When enabled, it provides optimal protection even when your device is switched off. To connect to Gmail accounts we need to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertake to limit its use of information accessed through the APIs. As a result, Product's use and transfer to any other product of information received from these Google APIs will adhere to Google API Services

User Data Policy, including the Limited Use requirements. In line with the privacy-by-design principle, we use privacy-preserving techniques (in particular Presidio) to remove personal data from emails to ensure the highest level of protection (this applies to Email Shield, too). These techniques, however, cannot guarantee full effectiveness and, therefore, we still treat all data as personal.

- **Email Shield** scans for threats in your incoming and outgoing email messages and attachments. Scanning applies only to messages sent or received using mail management software, such as Microsoft Outlook, Apple Mail or Mozilla Thunderbird.
- **Hack Alerts** when enabled, it searches and monitors email addresses associated with your Account for data breaches to alert you when your data has been compromised in a breach and your information is exposed on the dark web. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.

## Personal Data We Process

While using Antivirus for Desktop, we collect and process the following Service and Device Data (in addition to Account Data and Billing Data, if relevant):

| Service Data | What we use it for and for how long |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (50 months)<br>● To monitor messaging performance |

| | |
|---|---|
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country |
| Samples, files | **Service Provision** (36 months)<br>● For protection, detection, analysis, blocking, quarantining and deleting of malicious software |
| Detections | **Service Provision** (36 months)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |
| URLs and referrers | **Service Provision** (36 months)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |
| Information about cookies and other tracking technologies | **Service Provision** (stored locally on device only)<br>● To detect tracking and privacy issues and inform users about solutions |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (50 months) |

| | |
|---|---|
| | ● To introduce a new feature or product based on previous experience (36 months) |
| Email Guardian - Email | **Service Provision** (seconds)<br>● In order to check your email, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it |
| Email Guardian - Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guardian - Subject of emails, MessageIDs of emails | **Service Provision** (4 weeks)<br>● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guardian - Detections<br>● hash of the email<br>● hash of the userID<br>● email subject<br>● hash of sender email address<br>● domain address of sender<br>● detection type and name<br>● name of the attachments and their hashes<br>● country of the user | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |
| Email Shield - Detections<br>● email subject<br>● sender email address<br>● email content or attachment | **Service Provision** (1 month)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |

| | |
|---|---|
| • detection type and name | |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Internal online identifiers (GUID, Device ID) | **Service Provision** (36 months)<br>• For ensuring continuous functionality and breaking down entries in database<br>**In-product Messaging** (24 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>• To better understand our users' behavior (50 months)<br>• To introduce a new feature or product based on previous experience (36 months) |
| Information concerning computer or device | **Service Provision** (36 months)<br>• To check for compatibility issues in automated crash dumps<br>**In-product Messaging** (6 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>• To better understand users' behavior (50 months)<br>• To introduce a new feature or product based on previous experience (36 months) |
| Location | **Service Provision** (36 months)<br>• To set up a proper product language version for Windows<br>**In-product Messaging** (6 months) |

| | |
|---|---|
| | ● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior based on approximate location (50 months)<br>● To introduce a new feature or product based on approximate location (36 months) |
| Applications - other security SW / antiviruses present | **Service Provision** (36 months)<br>● To determine how Antivirus should behave (e.g. if it should be activated in Windows Security Centre or not, whether it should run in passive or active mode) |
| Applications on the device | **Service Provision** (36 months)<br>● For formulating rules of how Antivirus should behave in relation to other SW installed (e.g. exceptions in scanning, filtering, notifications, applying Do not Disturb rules)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (up to 36 months)<br>● To improve the users' overall experience by developing new features and products<br>● To understand/estimate market opportunity |
| Our other products/licenses on the device and their status | **Service Provision** (36 months)<br>● To recognize what features should be enabled or disabled, what product should be installed or uninstalled |

| | |
|---|---|
| | **In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (up to 36 months)<br>● To improve the users' overall experience by developing new features and products<br>● To understand/estimate market opportunity |
| Internet and connection / Network data / Number of devices on Network | **Service Provision** (36 months)<br>● For security prerequisites (e.g. DNS settings check, port restrictions enabling or disabling Security status check of devices on the network)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (36 months)<br>● To introduce a new feature or product based on previous experience |
| Browsers (installed, default) | **Service Provision** (36 months)<br>● For opening content in given browser<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

Note that samples (files, URLs) used for malware analysis are kept in our systems as long as it is necessary to ensure proper functionality of the AV product. These samples are not connected with any identifiers or individuals and the retention periods indicated above do not apply to this use.

The third-party analytics tools we use for Antivirus for Desktop is Google Analytics. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy.

## Antivirus for Mobile (Android)

### Official Product Name

Avast Mobile Security, Avast Mobile Security Premium (collectively as "Antivirus for Mobile (Android)")

### Core Functionality

Antivirus for Mobile (Android) provides people with essential mobile security with added privacy and performance-boosting features. Block malware, check the safety of installed apps, scan public Wi-Fi networks for possible security weaknesses, and locate your phone if it becomes lost or stolen — all with a single app.

### What are Product's Main Features

- **Device Scan** scans your device or a specific file for malware apps and files and various types of security vulnerabilities.
- **Wi-Fi Security and Speed Check** enables you to scan your network for vulnerabilities, and tests the speed of the network.
- **Web Shield** detects and notifies you when accessing a malicious website that could represent a potential security risk for you.
- **Anti-Theft** is designed to protect your private mobile data and help you recover your device in case of loss or theft. This feature is off by default. When you choose to turn it on, you can request location on demand from my.avast.com. Anti-Theft is designed to protect data residing on your mobile phone in the event of theft. For Anti-Theft to function, we must collect and store information about your phone and

its approved users. We use this data to locate and identify your lost devices. If the phone was stolen, it may block the thief from using the device. The collected data is used to provide you the functionality. Within Anti-Theft there is a Last Known Location premium feature which is also off by default. When you activate the feature, we send more frequent location updates to the server to help you track your device's last known location.

- **App Locking** is a paid feature, which protects your sensitive apps with a PIN, pattern, or fingerprint.
- **App Insights** consists of three features: App Usage, Data Usage and App Permissions. App Insights requires your device user permission in order to work and we ask you for this permission (if not granted yet). When you grant the permission, we keep the data from your list of installed apps stored locally in your phone's database. App Usage provides information about how much time you spend using each app. App Permissions allows you to view which permissions are required by each of your installed apps. Data Usage monitors your data consumption and helps you avoid additional charges by notifying you when you approach the limit. This feature requires access to IMEI and IMSI.
- **Boost RAM** kills apps running in the background of your device.
- **Clean Junk** analyzes the space on your device and displays the amount of storage space that is being used by junk files.
- **Photo Vault** allows you to protect access to your photos with a PIN code.
- **Hack Alerts** when enabled, it searches and monitors email addresses associated with your Account for data breaches to alert you when your data has been compromised in a breach and your information is exposed on the dark web. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.
- **Privacy Audit** provides the user with an evaluation of installed apps based on data collected and permissions asked by the app compared to similar apps. The feature also compares its findings with the app's privacy policy declarations.

## Personal Data We Process

While using Antivirus for Mobile (Android), we collect and process the following Service and Device Data (in addition to Account Data and Billing Data, if relevant):

| **Service Data** | **What we use it for and for how long** |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country |
| Samples, files | **Service Provision** (36 months)<br>● For the functionality of malware scanning and analysis |
| Detections | **Service Provision** (36 months)<br>● For the functionality of malware scanning |
| Information concerning URLs of websites visited (malicious and non-malicious) and referrers (previous page with link to malware-hosting site) | **Service Provision** (36 months)<br>● For Web Shield feature's detection of malicious websites |

| | |
|---|---|
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Contextual promotional messaging (upsell, cross-promotion)<br>**Product and Business Improvement**<br>● To better understand our users' behavior and users' acquisition (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| User's email address associated with your Account | **Service Provision (36 months)**<br>● To search for your credentials in data breaches.<br>● To send a requested report to you on whether or not their credentials have leaked.<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUID, Device ID (Android ID), Advertising ID) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (50 months)<br>● To recognize reinstalls of the app on the same device (36 months)<br>**Third-party Ads** (not stored after provision)<br>● We process Advertising ID only for IronSource which allows it to place advertisements |
| Information concerning computer or device (carrier, OS version, OS build number, Hardware ID, device model, device brand, device manufacturer, device API level) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| Location (city/country, longitude and latitude) | **Service Provision** (36 months)<br>● For Anti-Theft functionality to locate a lost phone or track its locations per users request<br>● Delivering geo-specific changes to app's configuration (can be controlled by both local/on-device or remote features)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior based on approximate location (50 months)<br>● To introduce a new feature or product based on approximate location (36 months) |
| IMSI | **Service Provision** (accessed only locally)<br>● For App Insights's feature Data Usage to provide data consumption of installed apps based on IMSI |
| MSISDN (Mobile phone number) | **Service Provision** (30 days)<br>● For white-labeled versions of the app sold through partner carriers serves as unique ID connected with license<br>● For customer service purpose to verify that the user contacting customer support has valid and working license for the product |
| Applications, for privacy features their characteristics such as permissions, signing certs, package and library info, app versions | **Service Provision** (36 months)<br>● To define rules for malware protection<br>● To enable the calculation of the privacy features and tell whether the app rating and classification you received are relevant and up-to-date<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (36 months)<br>● To improve the product or its feature based on the user's feedback and use |

| | |
|---|---|
| Internet and connection | **Service Provision** (36 months)<br>● For security prerequisites<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

Note that samples (files, URLs) used for malware analysis are kept in our systems as long as it is necessary to ensure proper functionality of the AV product. These samples are not connected with any identifiers or individuals and the retention periods indicated above do not apply to this use.

These are the third-party analytics tools we use for Antivirus for Mobile (Android):

- Google Analytics
- Google Firebase and Crashlytics Analytics for Android
- AppsFlyer

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

The free version of Antivirus for Mobile (Android) serves relevant third-party advertisements. These are the advertising partners we use for this product:

- Google AdMob
- Amazon
- Facebook Audience Network
- InMobi
- AppLovin
- Unity Technologies

- IronSource

For further information regarding our third-party ads partners, including their privacy policies, please refer to our Consent Policy.

**Antivirus for Mobile (iOS)**

**Official Product Name**

Avast Security & Privacy

**Core Functionality**

Avast Security & Privacy (hereinafter as “Antivirus for Mobile (iOS)”) provides protection for your browsing, passwords, photos and Wi-Fi. The product consists of several free and paid features, such as Hack Alerts and Secure Browsing, which are described in detail below.

**What are Product’s Features**

- **Web Shield** detects and notifies you when accessing a malicious website that could represent a potential security risk for you.
- **Hack Alerts** looks for leaked personal information, whether your data has been compromised in a breach and your information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.
- **Photo Vault** locks your photos in an encrypted vault and secures them with a PIN, Touch ID, or Face ID so that only you have access to them.
- **Wi-Fi Security** automatically scans Wi-Fi networks for vulnerabilities to verify that the network you’re connected to is safe. Receive alerts if any risk is detected.
- **Secure Browsing** (available only for paid version) protects your privacy by making sure no one can spy on what you’re doing online with Secure Browsing VPN feature.
- **Email Guardian** is a cloud-based service which monitors emails from supported providers, scans when they arrive in your inbox and flags

them as malicious if they contain a threat. In order to deliver its functionality and allow us to improve our products and business, this feature processes personal data, such as e-mail and its content, including attachments. When enabled, it provides protection to your device even when the device is switched off. Connecting this feature to Gmail accounts requires us to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertake to limit its use of information accessed through the APIs. As a result, the use and transfer of information received from these Google APIs to any other product will adhere to Google API Services User Data Policy, including the Limited Use requirements. In line with the privacy-by-design principle, we use privacy-preserving techniques (in particular Presidio) to remove personal data from emails to ensure the highest level of protection. These techniques, however, cannot guarantee full effectiveness and, therefore, we still treat all data as personal.

## Personal Data We Process

While using Antivirus for Mobile (iOS), we collect and process the following Service and Device Data (in addition to Account Data and Billing Data, if relevant):

| Service Data | What we use it for and for how long |
|---|---|
| Information concerning URLs of websites visited (malicious and non-malicious) and referrers (previous page with link to malware-hosting site) | **Service Provision** (36 months)<br>● For Web Shield feature's detection of malicious websites |
| Timestamps of your connections for Secure Browsing | **Service Provision** (36 months)<br>● To manage the number of concurrent active connections, and handle abuse<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |

| | |
|---|---|
| The subnet of your originating IP address for Secure Browsing | **Service Provision** (36 months)<br>● To plan for increased network demand and capacity |
| IP address of the VPN server you're using for Secure Browsing | **Service Provision** (36 months)<br>● To troubleshoot our service and plan for new network capacity |
| Amount of data transmitted for Secure Browsing<br><br>E.G. 5GB up or down | **Service Provision** (36 months)<br>● To plan for new network capacity and server improvements<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |
| User's email for Hack Alerts | **Service Provision** (36 months)<br>● To send a requested report to you on whether or not their credentials have leaked<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |
| Events and product usage (app metadata, number of hack alerts checks, number and result of Wi-Fi scans, error logs and screen flow) | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings)<br>**Product and Business Improvement**<br>● To understand the user's behavior (14 months)<br>● To improve the user's overall experience (36 months) |
| Email Guardian - Email | **Service Provision (seconds)**<br>● In order to check your email, we download the whole email message, including metadata and attachments. We keep it in our systems only during the processing, we don't store it |

| | |
|---|---|
| Email Guardian - Hash of email address of sender | **Service Provision (36 months)**<br>● To provide the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guardian - Subject of emails, MessageIDs of emails | **Service Provision (4 weeks)**<br>● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guardian - Detections<br>● hash of the email<br>● hash of the userID<br>● email subjecthash of sender email address<br>● domain address of sender<br>● detection type and name<br>● name of the attachments and their hashes<br>● country of the user | **Service Provision (36 months)**<br>● To provide the functionality of malware scanning and to do maintenance<br>**Product and Business Improvement (36 months)**<br>● To do threat statistics and internal analysis |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| OS Version<br><br>E.g. iOS 13.1 | **Service Provision** (36 months)<br>● For user support and troubleshooting<br>**Product and Business Improvement**<br>● To understand the user's behavior and product development planning (14 months)<br>● To improve the user's overall experience (36 months) |

| | |
|---|---|
| Mobile Security for iOS version<br><br>E.G. Mobile Security for iOS version 1.2.2 | **Service Provision** (36 months)<br>● For user support and troubleshooting<br>**Product and Business Improvement**<br>● To understand the user's behavior and product development planning (14 months)<br>● To improve the user's overall experience (36 months) |
| MSISDN (Mobile phone number) | **Service Provision** (30 days)<br>● For white-labeled versions of the app sold through partner carriers serves as unique ID connected with license<br>● For customer service purpose to verify that the user contacting customer support has valid and working license for the product |

These are the third-party analytics tools we use for Antivirus for Mobile (iOS):

- Google Firebase Analytics and Crashlytics for iOS
- AppsFlyer

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

# AntiTrack

**Official Product Name**

Avast AntiTrack Premium, Avast AntiTrack for Mac, Avast AntiTrack for Android (collectively as “AntiTrack”)

**Core Functionality**

As you browse the web, cookies and digital fingerprint-based tracking technologies collect and link information about your activities in order to create profiles of your behavior . This data is then shared, bought and sold by

analytics and ad-tech firms. AntiTrack removes cookies and masks the device's "fingerprint" to prevent third- parties from identifying you and following your behavior across the web.

## What are the Product's Features

- **AntiFingerprinting** stops scripts from fingerprinting the user's device and tracking their browsing behavior across the web. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale and AntiTrack version.
- **Privacy Score** provides the user with an evaluation of how private they are based on various in-app configurations. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale, AntiTrack version, In-app settings (such as features that are turned on/off).
- **Fingerprint Randomizer** will automatically change the user's digital 'Fingerprint' in regular intervals, or allow the user to manually change said 'Fingerprint'. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale and AntiTrack version.
- **Browser cleanup** helps the user manage browsing history and cookies by allowing the user to manually clear this information or schedule an automatic deletion at a specific time. In particular, this feature relies on processing of browser version, hardware data, Cookies, OS version, OS locale, AntiTrack version, In-app settings (such as features that are turned on or off).
- **Browser protection** helps users stay protected from online tracking attempts and similar threats through supported browsers. Any time a suspicious script (tracking attempt) encounters the user's 'Fingerprint', the user is notified. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale, website scripts and tracking elements, and AntiTrack version.
- **Allowed Websites and whitelisting processes** allows the user to add their favorite websites into the Allowed Websites list so that their stored browser data is not be cleared during the automatic and manual cookie clearing process. Additionally, no anti-tracking measures will be active on these websites once they are added to the Allowed Websites list. In

particular, this feature relies on processing of whitelisted websites, browser version, hardware data, OS version, OS locale and AntiTrack version.

- **System Privacy** helps stop third parties from seeing, tracking, and collecting customer information from the supported operating system. Specifically, this is related to the customer's computer login security, protecting files and data on that machine, and keeping the customer's computer activities private.This provides another layer of security by giving the customer the ability to configure their Privacy Settings within AntiTrack. In particular this feature relies on processing of browser version, hardware data, OS version, OS locale, information about operation system's keys and tasks associated with privacy risks, and AntiTrack version.

## Personal Data We Process

We process only the following Service and Device Data (in addition to Billing Data for paid version or Account Data if necessary):

| **Service Data** | **What we use it for and for how long** |
|---|---|
| Usage Frequency (e.g., the amount of time the application is in use) | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• , To provide feature enhancement, customer support and product maintenance |
| Number of Application Launches | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• To provide product maintenance and customer support |
| License Key | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• To regulate access to the product, provide customer support, and administer product updates |

| | |
|---|---|
| Browser information (including information about extensions) | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• To show Browser Protection and Cookie Cleanup status in the product, and identify the default browser for opening the links from the app.<br>• To check the browser extension status (only in supported browsers).<br>• When Browser Protection feature from the product is ON, for AntiTrack to obfuscate the following properties of the browser under Anti-Fingerprinting:<br>  ○ User-Agent<br>  ○ Plugins<br>  ○ HTTP Headers |
| Cookies | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• To identify the "Total (number of) Cookies, and Tracking Cookies" available for a browser<br>• To perform the cookie cleanup (delete the cookies, cache, and browser history). |
| Whitelisted websites | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• To add websites into the Allowed Websites list |
| Website Tracker Details (Javascript, HTML documents) | **Service Provision** (the earlier lifetime of the account and 24 months)<br>• To identify website trackers on the website that the user is visiting and determine if the Javascript/Html is a tracker or not.<br>**In-product messaging** (6 months)<br>• To update the user about tracking. |

| | |
|---|---|
| AntiTrack version | **Service Provision** (the earlier lifetime of the account and 24 months)<br>● To provide user support, troubleshoot<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (24 months)<br>● To better understand how users' interact with certain aspects |
| Install Date or Time | **Service Provision** (the earlier lifetime of the account and 24 months)<br>● To do license management<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (24 months)<br>● To know when to market new features and or products |
| Crash Incidents | **Service Provision** (the earlier lifetime of the account and 24 months)<br>● To ensure continuous functionality |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| OS information (version, keys, tasks) | **Service Provision** (the earlier lifetime of the account and 24 months)<br>● To provide user support, troubleshoot<br>**Product and Business Improvement**<br>● When developing new features - to adjust the scope of the feature based upon the |

| | |
|---|---|
| | requirements and the functionality of certain operating systems (24 months)<br>● To better understand how users' interact with certain aspects 24 months) |
| OS Locale | **Service Provision** (the earlier lifetime of the account and 24 months)<br>● To segment updates by location<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (24 months)<br>● To determine which segments of our users to roll out a new feature or product<br>● To better understand how users' interact with certain aspects |
| Hardware Data (device model, RAM, GPU, CPU) | **Service Provision** (the earlier lifetime of the account and 24 months)<br>● To install the product, provide application updates, customer support<br>**Product and Business Improvement** (24 months)<br>● To better understand how users' interact with certain aspects |

The third party analytics tool we use for the AntiTrack Mac platform is App Center. For further information regarding our third party analytics partner, including its privacy policy, please refer to our Privacy Policy.

# Battery Saver

**Official Product Name**

Avast Battery Saver for Windows

## Core Functionality

Battery Saver is a tool designed to extend the battery life of your PC by reducing internal and external power demands.

## What are Product's Features

- **Battery Saver (profiles)** creates a power plan profile to apply the predefined set of various settings which shall reduce the amount of power consumed by the PC.

## Personal Data We Process

While using Battery Saver, we collect and process the following Service and Device Data (in addition to Billing Data or Account Data if relevant):

| Service Data | What we use it for and for how long |
|---|---|
| Events and product usage | **Service Provision** (up to 12 months)<br>● To monitor service functionality<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (12 months)<br>● To improve users' overall experience by developing new features or products (up to 12 months) |

| Device Data | What we use it for and for how long |
|---|---|
| Internal online identifiers (GUID, MIDEX, UUID) | **Service Provision** (up to 12 months)<br>● To monitor service functionality<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |

| | |
|---|---|
| Information concerning device (platform, computer type, vendor, model, brightness, wifi_status, bluetooth_status, battery, capacity, state, lifetime, critical bias, cycle count, voltage, granularity, manufacturer date) | **Service Provision** (12 months)<br>● To check for compatibility issues in automated crash dumps<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand users' behavior<br>● To introduce a new feature or product based on previous experience |
| Location (country, region, city, latitude, longitude, internet service provider, internet autonomous system) | **Service Provision** (up to 12 months)<br>● To set up a proper product language version for Windows<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand users' behavior based on approximate location<br>● To introduce a new feature or product based on approximate location |
| Other Avast products/licenses on the device and their status | **Service Provision** (12 months)<br>● To recognize what features should be enabled or disabled, what product should be installed or uninstalled<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |

The third-party analytics tool we use for Battery Saver is Google Analytics. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy**.**

# BreachGuard

## Official Product Name

BreachGuard

## Core Functionality

Our goal is to enable people to take back their privacy online. Remediate past breaches and minimise the risk of abuse of their data in the future. We aim to provide convenient solutions for everyday life online without sacrificing privacy.

1. Enabling users to discover and fix online privacy threats.
2. Prevent data collection by advertising companies and data brokers, depending on region.
3. Educating users about privacy and security online.

## What are Product's Features

- **Risk Monitor** is 24/7 dark web monitoring for leaked personal information. BreachGuard leverages the most comprehensive database of the dark web – it detects whether users have been compromised in a breach and their information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here. The feature also has the capability, if you consent, to scan your browser for weak, reused or breached passwords and provides instructions to fix these passwords.
- **Personal info remover** submits opt-out requests to data brokers in North America. This feature processes names (first name, middle name,

last name), address (street, city, country, state, zip code), phone number, email and Date of Birth (DOB). The reason for this is that data broker opt-out forms require some of, if not all of the information to submit a valid opt-out request and verify that you are, in fact in their database. As a result, we collect this basic information from you to submit the opt-out requests on your behalf.

- **Privacy Advisor** provides updates and guidance related to online privacy, including but not limited to: recent data breaches and guides to optimize your privacy for social media sites and other common services. If you opt-in, this functionality will process your bookmarks and browsing history to improve the quality of content so we can distinguish guides which are relevant to you (we are not processing full urls but we need only the domain name).
- **Identity Assist** We have partnered with a third party, Generali Global Assistance, to provide Identity Assist in BreachGuard.The service consists of two sub-features, ScamAssist and Identity Resolution. ScamAssist specialists act as trusted advisors to customers by helping them identify which of the solicitations they have received are potentially fraudulent. Resolution Specialists are available 24/7/365 to educate customers about how identity theft and cyber crimes occur, as well as provide tips and tools to help keep their identity and digital privacy secure. Note we do not process any personal data from your interaction with Generali, Generali does, see its privacy policy here.

## Personal Data We Process

By default, BreachGuard processes locally on your system the following data:

- Names (first name, middle name, last name), address (street, city, country, state, zip code), phone number, email and date of birth – to send data opt-out requests on your behalf via Personal Info Remover**.**
- Browser credentials (website, username, password) – to scan your browser for weak, reused or breached passwords and provide instructions how to fix

This data is not sent to our environment.

While using BreachGuard service, we collect and process data in our environment about you and your device in the following situations:

| **Service Data** | **What we use it for and for how long** |
|---|---|
| Browsing history and bookmarks (only domain name) | **Service Provision** (6 months)<br>● To display relevant privacy guides<br>**Product and Business Improvement** (6 months)<br>● For development of new features or products |
| Events and product usage (app metadata, page views, clicks, installs, Number of Application Launches, updates, error logs and screen flow) | **Service Provision** (24 months)<br>● To improve user experience and application performance<br>**Product and Business Improvement** (39 months)<br>● For development of new features or products |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| OS Version, BreachGuard Application Version, Activation Key<br><br>E.g. Windows 10, BreachGuard v1.2.0 | **Service Provision** (24 months)<br>● For users' support and troubleshooting<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (39 months)<br>● For development of new features or products<br>● To understand the users' behavior and product development planning |
| OS Locale | **Service Provision** (24 months)<br>● For users' support and troubleshooting as well as rendering the data broker removal service<br>**Product and Business Improvement** (39 months) |

| | |
|---|---|
| | • For development of new features or products |
| Hardware Data<br><br>e.g. Device Model (e.g. Windows 10 (13-inch 2017), RAM (Random Access Memory), GPU (Graphical Processing Unit), and Central Processing Unit (CPU) | **Service Provision** (24 months)<br>• For users' support and troubleshooting<br>**Product and Business Improvement** (39 months)<br>• For development of new features or products |

# Cleanup

## Cleanup for Desktop (Windows, Mac)

### Official Product Name

Avast Cleanup Premium, Avast Cleanup Premium for Mac (collectively as "Cleanup for Desktop")

### Core Functionality

Cleanup for Desktop is an ultimate tune-up program which speeds up and cleans your PC (Windows and Mac), updates installed apps, and fixes other problems.

### What are Product's Features

Avast Cleanup Premium for Windows:

- **Maintenance** scans and deletes registry items, shortcuts, system and programs temp or unnecessary files, browser caches, history and cookies.
- **Program Deactivators** scans and disables installed third-party programs which have background, startup or scheduled tasks.

- **Software, Disk** or **Browser Cleaner** scan and temporarily hide or uninstall third-party programs, deletes unnecessary files from disk or browser history.
- **Fix Problems** scans and fixes common Windows problems which might put PC at risk (e.g. missing Windows updates, administrative shares on public folders).
- **Disk Doctor** or **Defrag** scans for potential errors and fixes system drive or defrags your system drive.
- **Software Updater** scans and updates third-party programs and their versions installed on PC.

Avast Cleanup Premium for Mac:

- **Clutter Scan** scans and deletes application caches, log files, trash, downloads folder, development junk. It looks for similar data on connected external drives as well. Only data on the amount of KB and cleaned is processed.
- **Find Duplicates** scans for duplicate files in directories selected by you. Only data on the amount of KB and duplicate files found and cleaned is processed.
- **Find Photos** scans photos and evaluates their quality and similarity to help you decide which you want to keep. Only data on the amount of KB and photos found and cleaned is processed.
- **Uninstall Apps** scans and removes applications and programs for which it is necessary to process app name, size, version and last date of its usage.

## Personal Data We Process

While using Cleanup for Desktop, we collect and process the following Service and Device Data (in addition to Billing Data or Account Data if relevant):

| **Service Data** | **What we use it for and for how long** |
|---|---|

| | |
|---|---|
| Events and product usage (such as product version, product language, license type, days to expiration, number of potential problems or detected junk) | **Service Provision** (up to 12 months)<br>● To monitor service functionality<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (12 months)<br>● To improve users' overall experience by developing new features or products (up to 12 months) |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Internal online identifiers (GUID, MIDEX, UUID, Device ID) | **Service Provision** (up to 12 months)<br>● To identify correct installation<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |
| Information concerning device (platform, types of cleaning objects, objects size, app name, vendor, version, rating, certification) | **Service Provision** (up to 12 months)<br>● To check for compatibility issues in automated crash dumps<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (up to 12 months)<br>● To better understand users' behavior<br>● To introduce a new feature or product based on previous experience |

| | |
|---|---|
| Location (country, region, city, latitude, longitude, internet service provider, internet autonomous system) | **Service Provision** (up to 12 months)<br>● To set up a proper product language version for Windows<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand users' behavior based on approximate location<br>● To introduce a new feature or product based on approximate location |
| Applications (our other products, installed applications on a user's computer) | **Service Provision** (up to 12 months)<br>● Our other apps to know which products users already have on their computer<br>● Third-party applications or programs installed on users' computers to improve Cleanup Sleep Mode, Software Cleanup and Software Updater functionality<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (up to 12 months)<br>● To improve the users' overall experience by developing new features and products<br>● To understand/estimate market opportunity for new products and new features |

The third-party analytics tool we use for Cleanup for Desktop is Google Analytics. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy.

## Cleanup for Mobile (Android)

### Official Product Name

Avast Cleanup, Avast Cleanup Premium (collectively as "Cleanup for Mobile (Android)")

### Core Functionality

Cleanup for Mobile (Android) detects and removes unnecessary files to free up storage space. Equally, it can stop running processes to optimize device performance.

### What are Product's Features

- **App Overview** allows to browse installed and pre-installed applications, provides functionality to uninstall or stop. In particular, this feature relies on processing device provided stats about other apps. These stats are processed locally (on device) in order to provide the service.
- **Media Overview** provides an overview of files broken down by type (eg images, audio files, video). This feature does not need any specific data processing outside of operations made locally (on device).
- **Battery Saver** allows you to select conditions where desired actions (system settings changes) should be applied by this product. For example one can automatically decrease screen brightness when at home. Location based condition require permission to get location data, however these data are never transmitted from the device and all are processed locally.
- **Cloud Transfers** allows you to backup their files to an external cloud storage. We are using Google Drive and Dropbox APIs to do so, e.g. you can login using their Google or Dropbox credentials to establish such connections. Note credentials are not visible to us.

## Personal Data We Process

While using Cleanup for Mobile (Android), we collect and process the following Service and Device Data (in addition to Billing Data for paid version):

| **Service Data** | **What we use it for and for how long** |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (14 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● Replaced with city/country for delivering geo-specific changes to app's configuration (both local or remote)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (14 months)<br>● To monitor messaging performance |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior and users' acquisition (14 months)<br>● To consider roadmap for type of features and products we want to develop in future (36 months) |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUID, Device ID (Android ID), Hardware ID, Profile ID, Advertising ID) | **Service Provision** (36 months)<br>● For counting users, ensuring functionality and stability<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (14 months)<br>● To recognize reinstalls of the app on the same device (39 months)<br>**Third-party Ads** (not stored after provision)<br>● We process Advertising ID only for IronSource which allows it to place advertisements |
| Information concerning computer or device (carrier, OS version, OS build number, hardware ID, device model, device brand, device manufacturer, device API level) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** |

| | |
|---|---|
| | ● To better understand our users' behavior (14 months)<br>● To determine whether a new feature or product should be developed for subset of users (36 months) |
| Location (city/country, longitude and latitude) | **Service Provision** (36 months)<br>● Delivering geo-specific changes to app's configuration (both local or remote)<br>● Related to Battery Profile feature, as users can set being in a certain location as a trigger to automatically launch a Battery saving profile.<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior based on approximate location (14 months)<br>● To introduce a new feature or product based on approximate location (36 months) |
| Applications | **Service provision** (36 months)<br>● To provide insights, such as usage stats to help identify unused apps (storage cleaning opportunity), drain impact (battery, data) to help identify apps that have significant effect on device resources, or notification stats to help identify "noisy" apps which can be "muted" by links to system settings<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (14 months)<br>● To better understand users' behavior |

| | |
|---|---|
| Internet and connection | **Service provision** (36 months)<br>● For functionality of our features, providing error messaging<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (14 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

These are the third-party analytics tools we use for Cleanup for Mobile (Android):

- Google Firebase Analytics and Crashlytics for Android
- AppsFlyer

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

The free version of Cleanup for Mobile (Android) serves relevant third-party advertisements. These are the advertising partners we use for this product:

- Google AdMob
- Amazon
- Facebook Audience Network
- InMobi
- AppLovin
- Unity Technologies
- IronSource

For further information regarding our third-party ads partners, including their privacy policies, please refer to our Consent Policy.

# Driver Updater

## Official Product Name

Avast Driver Updater

## Core Functionality

Driver Updater provides scan and potential update or fix of outdated drivers on a users' PC to optimize it for better performance and avoid potential crashes or malfunctions.

## Personal Data We Process

While using our Driver Updater services, we collect and process data about you in the following situations:

| Service Data | What we use it for and for how long |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (12 months)<br>● To monitor service functionality<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To monitor messaging performance |
| Events and product usage | **Service Provision** (12 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand our users' behavior<br>● To introduce a new feature or product based on previous experience |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUID, MIDEX, UUID, Device ID) | **Service Provision** (12 months)<br>● For ensuring continuous functionality and breaking down entries in database<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand our users' behavior<br>● To introduce a new feature or product based on previous experience |
| Information concerning device (type, vendor, model, manufacturer, version) | **Service Provision** (12 months)<br>● To check for compatibility issues in automated crash dumps<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand users' behavior<br>● To introduce a new feature or product based on previous experience |
| Information concerning drivers | **Service Provision** (12 months)<br>● To monitor service functionality |

| | |
|---|---|
| (driver version, updated date, name, matching device id, driver rank, driver flags) | **In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand our users' behavior<br>● To introduce a new feature or product based on previous experience |
| Location (country, region, city, latitude, longitude, internet service provider, internet autonomous system) | **Service Provision** (12 months)<br>● To set up a proper product language version for Windows<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (12 months)<br>● To better understand users' behavior based on approximate location<br>● To introduce a new feature or product based on approximate location |
| Other Avast products/licenses on the device and their status | **Service Provision** (12 months)<br>● To recognize what features should be enabled or disabled, what product should be installed or uninstalled<br>**In-product Messaging** (12 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |

The third-party analytics tools we use for Driver Updater for Desktop is Google Analytics. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy.

# Family Space

## Official Product Name

Avast Family Space

## Core Functionality

Avast Family Space is a free mobile application for Android and iOS which keeps your kids safe both online and off with its advanced parental controls and location features.

## Personal Data We Process and Features

While using Family Space, we process the following Service and Device Data (in addition to Billing Data and Account Data):

1. **Location feature**

Parents are able to install the parent's app on their own device and kids app on children's devices. After activation, parents are able to locate their children on demand or set up automatic location alerts based on time or geofencing. Parents have the option to share their own location as well.

| **Location Data Feature** | **What we use it for and for how long** |
|---|---|
| Child location | **Service Provision** (12 months)<br>● We collect the child's geolocation GPS coordinates while the app is running in the foreground and background in order to show parents the child's current location, last-known location, and location history<br>● Children can also send their location from within the app. For example, Check-In and Pick Me Up are features that send the current location |

| | |
|---|---|
| | ● If the child has more than one device paired, location data is only collected from the most recently-used device<br>**Product and Business Improvement** (12 months)<br>● We use this data to train machine learning algorithms to notify parents when a child is in an unexpected place at a given time |
| Parent location | **Service Provision** (12 months)<br>● Parents can find a setting to share their location with all family members, other parents or off. The setting is off by default<br>**Product and Business Improvement** (up to 24 months)<br>● We track behavior such as turning this setting on or off, but we don't send location coordinates to third party analytics services |
| Saved locations | **Service Provision** (12 months)<br>● Parents can enter a saved location for use in geofencing alerts. They can be alerted when a child enters or exits that saved location, such as home or school<br>● Time spent at unsaved locations may be used to recommend a new saved location to parents<br>**New Product Development** (12 months)<br>● Saved Locations may be used in machine learning location anomaly detection. For example, when a child is at a saved location, it may not warrant an alert about unexpected behavior<br>**Product and Business Improvement** (up to 24 months)<br>● We track feature usage data to third parties for analytics, but not names or locations of saved places |

**2. Activity feature**

Parents are able to view web and app activity from their children's devices. The summary view categorizes connections made by category and the list view shows specific usage information.

| **Activity Data Feature** | **What we use it for and for how long** |
|---|---|
| DNS connections, device and app usage | **Service Provision** (12 months)<br>● When the child device is connected to our VPN, the device's IP address and DNS connection information are stored by our partner for 24 hours and then by us for 12 months. We also collect information about whether the device is locked, and whether the screen is on. On Android we also collect device and app usage information from the system. Together these records are used to present a summary and list view of your child's device, web, and app usage<br>● We collect the list of installed apps from the child's device to display to parents. We may notify the parent when a new app is installed. We do not share the complete app list with any third parties.<br>● We may alert parents to activity that might warrant attention, such as activity during late night hours, accessing objectionable content, or spending a lot of time on a new activity<br>● We may also display the same information to child app users for greater transparency<br>**Product and Business Improvement** (12 months)<br>● We use DNS usage history to develop machine learning models which will be used to notify the parent in case of |

| | |
|---|---|
| | usage anomalies that might warrant attention<br>● We use this data to develop machine learning models to predict how much time the child spends in each app, and on each device |

The third-party tool which we use for DNS lookup and content blocking is Akamai. For further information regarding this partner, please refer to their Privacy Policy.

### 3. Controls feature

Parents are able to block access to unwanted apps and websites individually or by category. Parents can pause and restore Internet access on demand.

| **Controls Data Feature** | **What we use it for and for how long** |
|---|---|
| Settings | **Service Provision** (the lifetime of account)<br>● To store parents' settings of blocked apps and websites in order to synchronize them across devices and apply the rules to children's devices<br>● We may provide the option to limit the time spent in each app, content category or device<br>**Product and Business Improvement**<br>● We track feature usage data to third parties for analytics (up to 24 months) |
| Pause internet logs | **Service Provision** (the lifetime of account)<br>● To store logs of when parents paused and resumed child access to the internet in order to provide customer support and understand usage behavior<br>**Product and Business Improvement**<br>● We track feature usage data to third parties for analytics (up to 24 months) |

## 4. Family setup

As a family app running on multiple devices, configuring your family profile is a required step.

| **Family Setup Data** | **What we use it for and for how long** |
|---|---|
| Names and photos | **Service Provision** (the lifetime of account or profile)<br>● Parents can enter any name and photo they wish for each family member. This information is then displayed on the devices of other family members as well<br>**Product and Business Improvement** (up to 24 months)<br>● We track usage information to third parties for analytics, but we don't send names or photos |
| Email addresses of secondary parents | **Service Provision** (the lifetime of account or profile)<br>● The primary parent must enter the email address of additional parents who wish to join the family. This is a security measure taken to ensure that only the invited parent is able to join. Email verification is required of all parents |
| Roles | **Service Provision** (the lifetime of account or profile)<br>● Each family member is assigned a Child or Parent role, depending on the configuration when family members are invited to join the family |
| MSISDN (mobile phone number) | **Service Provision** (30 days)<br>● For white-labeled versions of the app license sold through partner carriers serves as unique ID connected with<br>● For customer service purpose to verify that the user contacting customer support has valid and working license for the product |

We use third-party analytics tools for additional product insights. You can opt out of this collection in the product settings. These are the third-party analytics tools we use for Family Space:

- Amplitude
- Google Firebase and Crashlytics

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

# HackCheck

## Core Functionality

HackCheck is a website that allows users to input their email address into a form and check to see if their passwords have been stolen and published on the dark web. The email address is also registered for 24/7 monitoring and alerting which will send the user an email as soon as a password leak has been detected. Users can unsubscribe from this monitoring anytime.

Lastly, HackCheck offers some security tips and directions when or if your passwords have been compromised.

## What are Product's Features

- **Has my password been stolen?** which checks the database operated by our partner SpyCloud against the email address the user provided to see if the user's passwords have been leaked and sends an email to the user if the passwords leaked.
- **24/7 Automatic Email Alerts** which monitors the SpyCloud database and will send the user an email anytime their passwords show up in the SpyCloud database.

## Personal Data We Process

If you wish to use the HackCheck, you submit your email address so we can send you alerts about the passwords that have leaked based on results from SpyCloud Database. This email address is used by us for the purposes of

service provision, cross-promotion of our other products and optimization of the service to help us understand how you use our product (e.g. number of detections per email).

Your email address is stored for as long as you use our service, as it is necessary for us to provide it. Should you choose to unsubscribe from our email list your email will be deleted and you will not receive any further emails from us.

The database of leaked passwords is operated by our partner SpyCloud. For further information please refer to its privacy policy here.

# Business Hub and CloudCare

### Official Product Name

Avast Business Hub, Avast Business CloudCare

### Core Functionality

The management console makes it easy to deploy various protection services to multiple devices, manage all devices from one place, mix and match device types, schedule regular scans, and quickly add more devices.

Please note that through this Business Management Console certain settings related to privacy are managed by and information from managed devices is accessible to the administrator of the console. You, as a user, are informed about the role of the administrator during the installation. Businesses are responsible for informing you about this fact and instructing administrators about best practices to ensure users' privacy.

### What are Product's Features

- **Monitor Device Security** uses the console to monitor the health of all managed devices from one place, reviews the number of blocked threats, schedules regular scans, and more.

- **Management Dashboard** activates devices, adds devices to groups, configures antivirus settings, and views blocked threats from an easy-to-read dashboard.
- **Master Agent** selects a device as the Local Update Server where all updates can be downloaded and saves bandwidth by scheduling and distributing updates to all endpoints in your network when it's convenient.
- **Tasks** sets up security tasks for all managed endpoints, such as scans, messages, updates, and shutdowns to ensure optimal security for the entire network.
- **Updates** remotely downloads and distributes virus and program updates to all devices from one console to save time and bandwidth.
- **Notifications** receives instant email notifications on any security threats or network issues that need your attention, including outdated antivirus applications, extended device inactivity, and additional device update.
- **Reporting** views detailed reports that include blocked threats, task lists, and protected devices, making it simple to improve security and customize protection.
- **Subscriptions Overview** lists all valid subscriptions and licenses.
- **Network Discovery** scans your network for connected devices to bring visibility over what devices should be taken care of.
- **Cloud Backup** securely stores selected data in the cloud as backup in case of data loss or disaster resulting in data loss/damage.
- **Remote Control** enables IT admins to quickly and securely connect to a user's device, access files and applications, and help troubleshoot issues in real time.
- **Patch Management** - scans for missing operating system updates and third-party application patches and enables remote installation of those patches to resolve application vulnerabilities of endpoints.
- **Secure Web Gateway** (CloudCare only) inspects all web connections using DNS-layer protection and full web proxy. It also inspects full SSL and non-SSL paths for risky and new sites.
- **Content Filtering** (CloudCare only) boosts productivity and security by controlling your employees' internet usage and allowing to restrict their access to specific sites.
- **Email Security Services** (CloudCare only) is a hosted solution that checks emails for spam, viruses, and unwanted mail using a variety of

custom filters. It makes sure that mail is clean before it arrives on the customer's email server, and also offers email archives and encryption.

## Personal Data We Process

We process only the following Data in addition to Account Data and Billing Data for paid versions of the products you purchased:

| **Device Data** | **What we use it for** |
|---|---|
| Internal online identifiers (Device ID) | **Service Provision**<br>● For ensuring continuous functionality and breaking down entries in database<br>**Product and Business Improvement**<br>● To better understand our users' behavior<br>● To introduce a new feature or product based on previous experience |
| Device name, brand, type | **Service Provision**<br>● For users to better identify devices detected on the network<br>● To determine whether it supports installation of Avast services |
| Information concerning computer or device | **Service Provision**<br>● To check for compatibility issues in automated crash and agent log dumps<br>**Product and Business Improvement**<br>● To better understand users' behavior<br>● To introduce a new feature or product based on previous experience |
| Applications | **Service Provision**<br>● To determine which application needs to be updated, to provide support and troubleshooting |
| Files, content | **Service Provision**<br>● To provide cloud backup, email archive |

| | |
|---|---|
| Location, IP and MAC addresses | **Service Provision**<br>● For admins to have a possibility to localize their devices |
| Device status (last connection to Avast) | **Service Provision**<br>● For admins to see which devices were active and when and determine the risk profile |
| Location | **Service Provision**<br>● To set up a proper product language version<br>**In-product Messaging**<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior based on approximate location<br>● To introduce a new feature or product based on approximate location |
| Language | **Service Provision**<br>● To set the right language settings<br>**In-product Messaging**<br>● To send campaigns localized based on users' language |

| **Service Data** | **What we use it for** |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision**<br>● For ensuring continuous functionality of notifications |
| Detections | **Service Provision** |

| | |
|---|---|
| | ● For administrators to review and analyze what threats were detected in the network, files or emails |
| URLs | **Service Provision**<br>● For protection, detection and blocking of malicious or restricted content |
| Other Avast products/licenses on the device and their status | **Service Provision**<br>● For administrators to have an overview of running services and expiration dates |
| Internet and connection / Network data / Number of devices on Network | **Service Provision**<br>● For security prerequisites (e.g. DNS settings check, port restrictions enabling or remote deployment)<br>**Product and Business Improvement**<br>● To introduce a new feature or product based on previous experience |
| Events and product usage | **Service Provision**<br>● To provide reporting capability for admins and to ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging**<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior<br>● To introduce a new feature or product based on previous experience |

| **Admin and User Data** | **What we use it for** |
|---|---|

| | |
|---|---|
| Name, surname, email address | **Service provision**<br>● To provide access and services, possibility to send reports or notifications about security events or product updates |
| User access rights | **Service provision**<br>● To provide access to the product |

| **Company Data** | **What we use it for** |
|---|---|
| Name and contact information | **Service Provision**<br>● To provide support and to contact the company when needed |
| Business type | **Service Provision**<br>● To offer the right solution based on the type of the company |

We will process this data only as long as necessary for the purposes we described. We use rolling deletion periods which means we regularly delete the data we collected within a certain period of time after the collection.

We cooperate with the following third parties when providing our services:

- The Cloud Backup service is provided in cooperation with Infrascale Inc. See their Privacy Policy.
- The Remote Control service is provided in cooperation with XLAB d.o.o. See their Privacy Policy.
- The Secure Web Gateway service is provided by Zscaler, Inc. See their Privacy Policy.
- The Email Security Services service is provided in cooperation with Sophos Limited. See their Privacy Policy.

The third-party analytics tool we use for the Business Hub is Google Analytics. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy.

# News Companion

## Product Name

Avast News Companion - free browser extension for Chromium-based browsers across all platforms.

## Core Functionality and Features

- **Avast News Companion** helps you to check your sources for biases and accurate reporting. It alerts you when sites have a known political bias. Bias categories range from Left to Right, but we'll also tell you about scientific, satiric, and questionable sources. With this extension you make sure you're reading the facts. Avast News Companion uses algorithms that analyze factual reporting, and check the statements from the articles against fact-checking databases. Based on that you'll get alerted about misleading claims or incorrect news. We have a full list of the websites where we track reading. Download it here.

## Personal Data We Process

While using Avast News Companion, we collect and process the following Service and Device Data:

| Service Data | What we use it for and for how long |
| --- | --- |

| | |
|---|---|
| Selected URLs | **Service Provision** (30 days)<br>● To display claims related to articles read on selected news websites you're visiting<br>**Product and Business Improvement** (up to 36 months)<br>● To improve users' overall experience by developing new features or products by analyzing aggregated URLs counts |
| User's feedback<br>(rating, comments) | **Service Provision** (36 months)<br>● To tell whether the site rating and classification you received are relevant and up-to-date<br>**Product and Business Improvement** (36 months)<br>● To improve the product or its feature based on the user's feedback |
| Events and product usage<br>(open extension, rated site, change settings) | **Product and Business Improvement** (24 months)<br>● To measure user's behavior in UI and how user interacts with the extension |

| **Device Data** | **What we use it for and for how long** |
|---|---|

| | |
|---|---|
| Internal extension identifier (GUID) | **Service Provision** (up to 36 months)<br>● To monitor service functionality and provide users with reading reports<br>**Product and Business Improvement** (36 months)<br>● To measure product telemetry, and calculate statistics |
| Extension information (installation source and time, version and campaign ID) | **Service Provision** (up to 36 months)<br>● To monitor service functionality<br>**Product and Business Improvement** (up to 36 months)<br>● To obtain usage statistics, and perform feature A/B testing |
| Country | **Service Provision** (up to 36 months)<br>● To be able to display the correct online content and to improve features<br>**Product and Business Improvement** (up to 36 months)<br>● To improve users' overall experience by developing new features or products |

The third-party analytics tool we use for News Companion is Mixpanel. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy.

# Omni

**Official Product Name**

Avast Omni

## Core Functionality

Omni provides protection and insights for all connected devices in the home and on the go, through a combined hardware-software solution that easily connects to the existing home router without impacting Wi-Fi performance.

## What are Product's Features

- **Home Network Protection** enables users to find out which people and what devices are connected to their home network. Omni provides alerts if unusual behavior is detected on any device, and blocks hackers trying to access any device. It connects to the home router, meaning users do not need to replace their router or compromise on their choice of router.
- **On-the-go Security** extends Antivirus protection seamlessly to mobile devices including Windows, Mac, Android and iOS to secure them outside the home.
- **Parental Controls** serve families to filter content and apps that children can access including social media and videos. They can also pause gaming or the internet at any time. Geo-location services help keep track of children with the option to set up alerts for when they leave or arrive at certain places.

## Personal Data We Process

Avast Omni integrates features of Family Space, Antivirus for Desktop, Antivirus for Mobile (Android), Antivirus for Mobile (iOS) and Network Security. For further information regarding data associated with Avast Omni please see portraits of those products.

### Network Security

In order for Avast Omni to protect devices on user's local network, we collect and process the following Service and Device Data (in addition to Account and Billing Data, if relevant):

| **Service Data** | **What we use it for and for how long** |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (up to 50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● Part of malware infection file, replaced in 30 days with city/country to detect the approximate location of malicious software |
| Samples, files | **Service Provision** (36 months)<br>● For protection, analysis, detection, blocking, quarantining and deleting of malicious software |
| Detections | **Service Provision** (36 months)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |
| URLs and referrers | **Service Provision** (36 months)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure functionality (installations, versions, updates, settings), map how users interact with the app and improve its design or flows<br>**In-product Messaging** (24 months) |

| | |
|---|---|
| | ● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behaviors (up to 50 months)<br>● Learnings from one product usage data may have an effect on the design or layout of the new one (36 months) |

| **Device Data** | **What we use it for** |
|---|---|
| Online identifiers (GUID, Device ID, MAC address) | **Service Provision** (36 months)<br>● For ensuring continuous functionality and breaking down entries in database<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (up to 50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |
| MSISDN (Mobile phone number) | **Service Provision** (30 days)<br>● For white-labeled versions of the app sold through partner carriers serves ss unique ID connected with license<br>● For customer service purpose to verify that the user contacting customer support has valid and working license for the product |
| Information concerning computer or device | **Service Provision** (36 months) |

| | |
|---|---|
| | ● To check for compatibility issues in automated crash dumps<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (up to 50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |
| GEO data / locale data | **Service Provision** (36 months)<br>● Setting up a proper product language version for Windows<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (36 months)<br>● To introduce a new feature or product based on country |
| Applications - other security SW / antiviruses present | **Service Provision** (36 months)<br>● To determine how Antivirus should behave |
| Applications on the device | **Service Provision** (36 months)<br>● Used for defining rules of how Antivirus should behave in relation to other SW installed (e.g. exceptions in scanning, filtering, notifications, applying Do not Disturb rules)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem |
| Other Avast products/licenses on the device and their status | **Service Provision** (36 months)<br>● To recognize what features should be enabled or disabled, what product should be installed or uninstalled<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |
| Internet and connection / Network data / Number of devices on Network | **Service Provision** (36 months)<br>● Security prerequisites (e.g. DNS settings check, port restrictions enabling or disabling Security status check of devices on the network)<br>**In-product Messaging** (6 months)<br>● Suitable offering in case these products might increase security or privacy of the given connection, network type etc.<br>**Product and Business Improvement** (36 months)<br>● To introduce a new feature or product based on previous experience |
| Browsers (installed, default) | **Service Provision** (36 months)<br>● For opening content in given browser<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (up to 50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

Note that samples (files, URLs) used for malware analysis are kept in our systems as long as it is necessary to ensure proper functionality of the AV product. These samples are not connected with any identifiers or individuals and the retention periods indicated above do not apply to this use.

The third-party analytics tools we use for Omni are:

- Amplitude on iOS and Android
- Google Fabric Crashlytics on iOS and Android
- AppsFlyer Analytics for iOS and Android
- Google Analytics

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

# Avast One

## Avast One for Mobile (Android)

### Official Product Name

Avast One Essential, Avast One Individual, Avast One Family (collectively as "Avast One (Android)")

### Core Functionality

Avast One (Android) provides a comprehensive set of features protecting users against potential security and privacy threats, and features for optimizing device's performance.

### What are Product's Features

- **Device Scan** scans your device or a specific file for malware apps and files and various types of security vulnerabilities.
- **Malware Shields** constantly scans all new apps and files being downloaded to the device for malware.
- **VPN** feature protects your privacy by encrypting your online communication so no one can spy on what you're doing online. It allows you to pick a specific location to be connected from.

- **Wi-Fi Scan** enables you to scan your network for vulnerabilities and encourages you to connect to VPN if any issues are detected.
- **Web Shield** detects and notifies you when accessing a malicious website that could represent a potential security risk for you.
- **Personal Identity Scan and Monitoring** looks for leaked personal information, whether your data has been compromised in a breach and your information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.
- **Performance Scan** analyzes the space on your device and displays the amount of storage space that is being used by junk files. Also, it detects apps running in the background of your device that can be stopped in order to free up the device's memory and speed it up.
- **Online Safety Score** analyzes data collected by Avast One such as files scanned for malware and websites scanned for dangerous links and provides you with an insight into your behavior.
- **Email Guardian** is a cloud-based service which monitors emails from supported providers, scans them the minute they hit your inbox and flags them as malicious if they contain a threat. This feature processes for its functionality, products and business improvement personal data, such as e-mail and its content, including attachments. When enabled, it provides optimal protection even when your device is switched off. To connect to Gmail accounts we need to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertake to limit its use of information accessed through the APIs. As a result, Product's use and transfer to any other product of information received from these Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements. In line with the privacy-by-design principle, we use privacy-preserving techniques (in particular Presidio) to remove personal data from emails to ensure the highest level of protection. These techniques, however, cannot guarantee full effectiveness and, therefore, we still treat all data as personal.

**Personal Data We Process**

While using Avast One (Android), we collect and process the following Service and Device Data (in addition to Account Data and Billing Data for paid version):

| **Service data** | **What we use it for and for how long** |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country |
| Samples, files | **Service Provision** (36 months)<br>● For the functionality of malware scanning and analysis |
| Detections | **Service Provision** (36 months)<br>● For the functionality of malware scanning |
| Information concerning URLs of websites visited (malicious and non-malicious) and referrers (previous page with link to malware-hosting site) | **Service Provision** (36 months)<br>● For Web Shield feature's detection of malicious websites |

| | |
|---|---|
| User’s email address(es) for Identity leaks scanning and monitoring | **Service Provision** (36 months)<br>● To send a requested report to you on whether or not their credentials have leaked (one time or regularly depending on users preferences)<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |
| Timestamps of connections for VPN | **Service Provision** (35 days)<br>● To calculate peak times of service demand in order to plan the network capacity<br>● To manage the number of concurrent active connections, and handle abuse<br>● To troubleshoot our service |
| Amount of data transmitted for VPN | **Service Provision** (35 days)<br>● To plan for new network capacity and server improvements<br>● To calculate a free usage quota |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Contextual promotional messaging<br>**Product and Business Improvement**<br>● To better understand our users’ behavior and users’ acquisition (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |

| | |
|---|---|
| Email Guardian - Email | **Service Provision (seconds)**<br>● In order to check your email, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it |
| Email Guardian - Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guardian - Subject of emails, MessageIDs of emails | **Service Provision** (4 weeks)<br>● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guardian - Detections<br>● hash of the email<br>● hash of the userID<br>● email subject<br>● hash of sender email address<br>● domain address of sender<br>● detection type and name<br>● name of the attachments and their hashes<br>● country of the user | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUID, Device ID (Android ID), Advertising ID) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (50 months)<br>● To recognize reinstalls of the app on the same device (36 months) |
| Information concerning device (carrier, OS version, OS build number, Hardware ID, device model, device brand, device manufacturer, device API level) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| Location (city/country, longitude and latitude) | **Service Provision** (36 months)<br>● Delivering geo-specific changes to app's configuration (both local or remote)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Delivering geo-specific promotional messaging<br>**Product and Business Improvement**<br>● To better understand users' behavior based on approximate location (50 months)<br>● To introduce a new feature or product based on approximate location (36 months) |

| | |
|---|---|
| Installed applications | **Service Provision** (36 months)<br>● To define rules how Antivirus should behave<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |
| Internet and connection | **Service Provision** (36 months)<br>● For security prerequisites<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

Note that samples (files, URLs) used for malware analysis are kept in our systems as long as it is necessary to ensure proper functionality of the AV product. These samples are not connected with any identifiers or individuals and the retention periods indicated above do not apply to this use.

These are the third-party analytics tools we use for Avast One (Android):

- Google Firebase and Crashlytics Analytics for Android
- AppsFlyer

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

**Avast One for Mobile (iOS)**

## Official Product Name

Avast One Essential, Avast One Premium, Avast One Individual, Avast One Family (collectively as “Avast One (iOS)”)

## Core Functionality

Avast One (iOS) provides a comprehensive set of features protecting users against potential security and privacy threats, and features for optimizing device’s performance.

## What are Product’s Features

- **VPN** feature protects your privacy by encrypting your online communication so no one can spy on what you’re doing online. The paid version of Avast One Premium allows you to pick a specific location to be connected from.
- **Web Shield** detects and notifies you when accessing a malicious website that could represent a potential security risk for you.
- **Photo Vault** locks your photos in an encrypted vault and secures them with a PIN, Touch ID, or Face ID so that only you have access to them.
- **Data Breach Monitoring** looks for leaked personal information, whether your data has been compromised in a breach and your information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.
- **Online Safety Score** analyzes data collected by Avast One such as files scanned for malware and websites scanned for dangerous links and provides you with an insight into your behavior.
- **Email Guardian** is a cloud-based service which monitors emails from supported providers, scans when they arrive in your inbox and flags them as malicious if they contain a threat. In order to deliver its functionality and allow us to improve our products and business, this feature processes personal data, such as e-mail and its content, including attachments. When enabled, it provides protection to your device even when the device is switched off. Connecting this feature to Gmail accounts requires us to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertake to limit its use of information accessed through the APIs. As a result, the use and transfer of information received from these Google APIs to any

other product will adhere to Google API Services User Data Policy, including the Limited Use requirements. In line with the privacy-by-design principle, we use privacy-preserving techniques (in particular Presidio) to remove personal data from emails to ensure the highest level of protection. These techniques, however, cannot guarantee full effectiveness and, therefore, we still treat all data as personal.

## Personal Data We Process

While using Avast One (iOS), we collect and process the following Service and Device Data (in addition to Account Data and Billing Data for paid version):

| Service data | What we use it for and for how long |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country |
| Information concerning URLs of websites visited (malicious and non-malicious) and referrers (previous page with link to malware-hosting site) | **Service Provision** (36 months)<br>● For Web Shield feature's detection of malicious websites |

| | |
|---|---|
| User’s email address(es) for Identity leaks scanning and monitoring | **Service Provision** (36 months)<br>● To send a requested report to you on whether or not their credentials have leaked (one time or regularly depending on users preferences)<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |
| Timestamps of connections for VPN | **Service Provision** (35 days)<br>● To calculate peak times of service demand in order to plan the network capacity<br>● To manage the number of concurrent active connections, and handle abuse<br>● To troubleshoot our service |
| Amount of data transmitted for VPN | **Service Provision** (35 days)<br>● To plan for new network capacity and server improvements<br>● To calculate a free usage quota |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Contextual promotional messaging<br>**Product and Business Improvement**<br>● To better understand our users’ behavior and users’ acquisition (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |

| | |
|---|---|
| Email Guardian - Email | **Service Provision** (seconds)<br>● In order to check your email, we download the whole email message, including metadata and attachments. We keep it in our systems only during the processing, we don't store it |
| Email Guardian - Hash of email address of sender | **Service Provision** (36 months)<br>● To provide the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guardian - Subject of emails, MessageIDs of emails | **Service Provision** (4 weeks)<br>● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guardian - Detections<br>● hash of the email<br>● hash of the userID<br>● email subject<br>● hash of sender email address<br>● domain address of sender<br>● detection type and name<br>● name of the attachments and their hashes<br>● country of the user | **Service Provision** (36 months)<br>● To provide the functionality of malware scanning and to do maintenance<br>**Product and Business Improvement** (36 months)<br>● To do threat statistics and internal analysis |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUID, Device ID (Apple Bundle ID), Advertising ID) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed |

| | |
|---|---|
| | product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (50 months)<br>● To recognize reinstalls of the app on the same device (36 months) |
| Information concerning device (carrier, OS version, OS build number, Hardware ID, device model, device brand, device manufacturer, device API level) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| Location (city/country, longitude and latitude) | **Service Provision** (36 months)<br>● Delivering geo-specific changes to app's configuration (both local or remote)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Delivering geo-specific promotional messaging<br>**Product and Business Improvement**<br>● To better understand users' behavior based on approximate location (50 months)<br>● To introduce a new feature or product based on approximate location (36 months) |

| | |
|---|---|
| Installed applications | **Service Provision** (36 months)<br>● To define rules how Antivirus should behave<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |
| Internet and connection | **Service Provision** (36 months)<br>● For security prerequisites<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

These are the third-party analytics tools we use for Avast One (iOS):

- Google Firebase and Crashlytics Analytics for iOS
- AppsFlyer

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

**Avast One for Desktop (Windows)**

**Official Product Name**
Avast One Essential, Avast One for Windows (collectively as "Avast One (Windows)")

**Core Functionality**

Avast One (Windows) provides a comprehensive set of features protecting users against potential security and privacy threats, and features for optimizing device's performance.

## What are Product's Features

- **Security**
  - **CommunityIQ** is a threat monitoring service for Windows and Mac which sends information about a threat detected in your device to our server, so we can observe how the threat spreads and block it. This is vital for the functioning of our Antivirus and our ability to keep your device secure.
  - **CyberCapture** detects and analyses rare, suspicious files on your Windows. If you attempt to run such a file, CyberCapture locks the file from your PC and sends it to our Threat Lab where it is analysed in a safe, virtual environment. All files are uploaded over an encrypted connection, which means your data is inaccessible to hackers.
  - **File Reputation** provides a real-time comparison with an up-to-date list of malware databases of executable files sourced from users of Windows who agree to participate in the service. FileRep processes files or their hashed versions to evaluate which are infectious and updating virus databases.
  - **Web Shield** scans data that is transferred when you browse the internet in real-time to prevent malware from being downloaded and run on your computer. By default, Web Shield is on and configured to provide optimal protection when switched on.
  - **File Shield** scans programs and files saved on devices for malicious threats in real-time before allowing them to be opened, run, modified, or saved
  - **Email Guardian** (on the web) is a cloud-based service which monitors emails from supported providers, scans when they arrive in your inbox and flags them as malicious if they contain a threat. In order to deliver its functionality and allow us to improve our products and business, this feature processes personal data, such as e-mail and its content, including attachments. When enabled, it provides protection to your device even when the device is switched off. Connecting this feature to Gmail accounts requires us to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertake to limit its

use of information accessed through the APIs. As a result, the use and transfer of information received from these Google APIs to any other product will adhere to Google API Services User Data Policy, including the Limited Use requirements.In line with the privacy-by-design principle, we use privacy-preserving techniques (in particular Presidio) to remove personal data from emails to ensure the highest level of protection. These techniques, however, cannot guarantee full effectiveness and, therefore, we still treat all data as personal.

    - **Email Guardian** (on your device) scans for threats in your incoming and outgoing email messages and attachments. Scanning applies only to messages sent or received using mail management software, such as Microsoft Outlook, Apple Mail or Mozilla Thunderbird.
- **VPN** feature protects your privacy by encrypting your online communication, so no one can spy on what you're doing online. It allows you to pick a specific location to be connected from.
    - **VPN reminders** remind users to connect to the VPN based on the type of the visited URL with an option to turn it off.
- **Personal Identity Scan and Monitoring** looks for leaked personal information, whether your data has been compromised in a breach and your information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here. The feature also has the capability, if you consent, to scan your browser for weak, reused or breached passwords and provides instructions to fix these passwords.
- **Performance**
    - **Disk Cleaner** detects and removes junk files from your PC.
    - **App Optimizer** detects apps that slow you down and allows the user to temporarily disable it when not in use.
    - **Software Updater** detects a list of outdated software applications and gets them up-to-date.
    - **Driver Updater** detects outdated drivers and gets them up-to-date.
- **Online Safety Score** analyzes data collected by Avast One such as files scanned for malware and websites scanned for dangerous links and provides you with an insight into your behavior.

## Personal Data We Process

While using Avast One (Windows), we collect and process the following Service and Device Data (in addition to Account Data and Billing Data for paid version):

| Service data | What we use it for and for how long |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country |
| Samples, files | **Service Provision** (36 months)<br>● For the functionality of malware scanning and analysis |
| Detections | **Service Provision** (36 months)<br>● For the functionality of malware scanning |
| Information concerning URLs of websites visited (malicious and non-malicious) and | **Service Provision** (36 months)<br>● For Web Shield feature's detection of malicious websites |

| | |
|---|---|
| referrers (previous page with link to malware-hosting site) | **In-product Messaging (with option to opt-out)**<br>● To recommend user to turn on the VPN for better protection |
| User's email address(es) for Identity leaks scanning and monitoring | **Service Provision** (36 months)<br>● To send a requested report to you on whether or not their credentials have leaked (one time or regularly depending on users preferences)<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |
| Timestamps of connections for VPN | **Service Provision** (35 days)<br>● To calculate peak times of service demand in order to plan the network capacity<br>● To manage the number of concurrent active connections, and handle abuse<br>● To troubleshoot our service |
| Amount of data transmitted for VPN | **Service Provision** (35 days)<br>● To plan for new network capacity and server improvements<br>● To calculate a free usage quota |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Contextual promotional messaging<br>**Product and Business Improvement** |

| | |
|---|---|
| | ● To better understand our users' behavior and users' acquisition (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| Email Guardian - Email | **Service Provision** (seconds)<br>● In order to check your email, we download the whole email message, including metadata and attachments. We keep it in our systems only during the processing, we don't store it |
| Email Guardian - Hash of email address of sender | **Service Provision** (36 months)<br>● To provide the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guardian - Subject of emails, MessageIDs of emails | **Service Provision** (4 weeks)<br>● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guardian - Detections<br>● hash of the email<br>● hash of the userID<br>● email subject<br>● hash of sender email address<br>● domain address of sender<br>● detection type and name<br>● name of the attachments and their hashes<br>● country of the user | **Service Provision** (36 months)<br>● To provide the functionality of malware scanning and to do maintenance<br>**Product and Business Improvement** (36 months)<br>● To do threat statistics and internal analysis |

| **Device Data** | **What we use it for and for how long** |
|---|---|

| | |
|---|---|
| Online identifiers (GUID, Device ID (Android ID), Advertising ID) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (50 months)<br>● To recognize reinstalls of the app on the same device (36 months) |
| Information concerning device (carrier, OS version, OS build number, Hardware ID, device model, device brand, device manufacturer, device API level) | **Service Provision** (36 months)<br>● To ensure functionalities of the product and its features<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| Location (city/country, longitude and latitude) | **Service Provision** (36 months)<br>● Delivering geo-specific changes to app's configuration (both local or remote)<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Delivering geo-specific promotional messaging<br>**Product and Business Improvement** |

| | |
|---|---|
| | ● To better understand users' behavior based on approximate location (50 months)<br>● To introduce a new feature or product based on approximate location (36 months) |
| Installed applications | **Service Provision** (36 months)<br>● To define rules how Antivirus should behave<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |
| Internet and connection | **Service Provision** (36 months)<br>● For security prerequisites<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To introduce a new feature or product based on previous experience (36 months) |
| Email Guardian (on the device) - Detections<br>● email subject<br>● sender email address<br>● email content or attachment<br>● detection type and name | **Service Provision** (1 month)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |

Note that samples (files, URLs) used for malware analysis are kept in our systems as long as it is necessary to ensure proper functionality of the AV product. These samples are not connected with any identifiers or individuals and the retention periods indicated above do not apply to this use.

## Avast One for Desktop (Mac)

### Official Product Name

Avast One Essential, Avast One for Mac (collectively as "Avast One (Mac)")

### Core Functionality

Avast One (Mac) provides a comprehensive set of features protecting users against potential security and privacy threats, and features for optimizing device's performance.

### What are Product's Features

- **Security**
  - **CommunityIQ** is a threat monitoring service for Windows and Mac which sends information about a threat detected in your device to our server, so we can observe how the threat spreads and block it. This is vital for the functioning of our Antivirus and our ability to keep your device secure.
  - **CyberCapture** detects and analyses rare, suspicious files on your Mac. If you attempt to run such a file, CyberCapture locks the file from your Mac and sends it to our Threat Lab where it is analysed in a safe, virtual environment. All files are uploaded over an encrypted connection, which means your data is inaccessible to hackers.
  - **File Shield** looks for malware on your device and secures it before it can harm you
  - **Ransomware Shield** secures your most important folders and your files within.
  - **Quarantine** locks away suspicious and dangerous files found during scans
  - **Web Hijack Guard** ensures that the websites you visit are legitimate and safe.

    - **Web Shield** scans data that is transferred when you browse the internet in real-time to prevent malware from being downloaded and run on your computer. By default, Web Shield is on and configured to provide optimal protection when switched on.
    - **Email Guardian** (across all devices) is a cloud-based service which monitors emails from supported providers, scans them the minute they hit your inbox and flags them as malicious if they contain a threat. This feature processes for its functionality, products and business improvement personal data, such as e-mail and its content, including attachments. When enabled, it provides optimal protection even when your device is switched off. To connect to Gmail accounts we need to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertakecomply with their rules to limit its use of information accessed through the APIs. As a result, **the p**roduct's use and transfer to any other product of information received from these Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements. In line with the privacy-by-design principle, we use privacy-preserving techniques (in particular Presidio) to remove personal data from emails to ensure the highest level of protection (this applies to Email Shield, too). These techniques, however, cannot guarantee full effectiveness and, therefore, we still treat all data as personal.
    - **Email Guardian** (only on particular Mac device) scans for threats in your incoming and outgoing email messages and attachments. Scanning applies only to messages sent or received using mail management software, such as Microsoft Outlook, Apple Mail or Mozilla Thunderbird.
- **VPN** feature protects your privacy by encrypting your online communication so no one can spy on what you're doing online. It allows you to pick a specific location to be connected from.
    - **VPN reminders** remind users to connect to the VPN based on the network you are connected to with an option to turn it off.
- **Data Breach Monitoring** looks for leaked personal information, whether your data has been compromised in a breach and your information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials

against its repository of stolen accounts. For further information please refer to its privacy policy here. The feature also has the capability, if you consent, to scan your browser for weak, reused or breached passwords and provides instructions to fix these passwords.

- **Clear Browsing Data** deletes browsing items that can be used by third parties to create a long term record of your browsing history.
- **Performance**
  - **Disk Cleaner** detects and removes junk files from your Mac.
  - **App Uninstaller** shows apps that you have not used in a long time and helps you to completely unistall them.
  - **Photo Cleaner Scans** your photos to find duplicate and low quality pictures and helps you to remove them.
- **Online Safety Score** analyzes data collected by Avast One such as files scanned for malware and websites scanned for dangerous links and provides you with an insight into your behavior.

## Personal Data We Process

While using Avast One (Mac), we collect and process the following Service and Device Data (in addition to Account Data and Billing Data for paid version):

| Service data | What we use it for and for how long |
|---|---|
| Identifier of the content (message) being delivered | **Service Provision** (36 months)<br>● To monitor service functionality<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** (50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware |

| | |
|---|---|
| | infection file replaced in 30 days with city/country |
| Samples, files | **Service Provision** (36 months)<br>● For the functionality of malware scanning and analysis |
| Detections | **Service Provision** (36 months)<br>● For the functionality of malware scanning |
| Information concerning URLs of websites visited (malicious and non-malicious) and referrers (previous page with link to malware-hosting site) | **Service Provision** (36 months)<br>● For Web Shield feature's detection of malicious websites<br>**In-product Messaging (with option to opt-out)**<br>● To recommend user to turn on the VPN for better protection |
| User's email address(es) for Identity leaks scanning and monitoring | **Service Provision** (36 months)<br>● To send a requested report to you on whether or not their credentials have leaked (one time or regularly depending on users preferences)<br>**Product and Business Improvement** (36 months)<br>● To improve the user's overall experience |
| Timestamps of connections for VPN | **Service Provision** (35 days)<br>● To calculate peak times of service demand in order to plan the network capacity<br>● To manage the number of concurrent active connections, and handle abuse<br>● To troubleshoot our service |
| Amount of data transmitted for VPN | **Service Provision** (35 days)<br>● To plan for new network capacity and server improvements<br>● To calculate a free usage quota |

| | |
|---|---|
| Events and product usage | **Service Provision** (36 months)<br>● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>● Contextual promotional messaging<br>**Product and Business Improvement**<br>● To better understand our users' behavior and users' acquisition (50 months)<br>● To improve the user's overall experience by developing new features and products (36 months) |
| Email Guardian (across all devices) - Email | **Service Provision (seconds)**<br>● In order to check your email, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it |
| Email Guardian (across all devices) - Hash of email address of sender | **Service Provision (36 months)**<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guardian (across all devices) - Subject of emails, MessageIDs of emails | **Service Provision (4 weeks)**<br>● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guardian (across all devices) - Detections<br>● hash of the email<br>● hash of the userID<br>● email subject | **Service Provision (36 months)**<br>● For the functionality of malware scanning and maintenance<br>**Product and Business Improvement (36 months)** |

| | |
|---|---|
| • hash of sender email address<br>• domain address of sender<br>• detection type and name<br>• name of the attachments and their hashes<br>• country of the user | • Threat statistics and internal analysis |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUID, Device ID (Android ID), Advertising ID) | **Service Provision** (36 months)<br>• To ensure functionalities of the product and its features<br>**In-product Messaging** (24 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>• To better understand our users' behavior (50 months)<br>• To recognize reinstalls of the app on the same device (36 months) |
| Information concerning device (carrier, OS version, OS build number, Hardware ID, device model, device brand, device manufacturer, device API level) | **Service Provision** (36 months)<br>• To ensure functionalities of the product and its features<br>**In-product Messaging** (6 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>• To better understand users' behavior (50 months) |

| | |
|---|---|
| | • To improve the user's overall experience by developing new features and products (36 months) |
| Location (city/country, longitude and latitude) | **Service Provision** (36 months)<br>• Delivering geo-specific changes to app's configuration (both local or remote)<br>**In-product Messaging** (6 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>• Delivering geo-specific promotional messaging<br>**Product and Business Improvement**<br>• To better understand users' behavior based on approximate location (50 months)<br>• To introduce a new feature or product based on approximate location (36 months) |
| Installed applications | **Service Provision** (36 months)<br>• To define rules how Antivirus should behave<br>**In-product Messaging** (6 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem |
| Internet and connection | **Service Provision** (36 months)<br>• For security prerequisites<br>**In-product Messaging** (6 months)<br>• To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement** |

| | |
|---|---|
| | • To better understand users' behavior (50 months)<br>• To introduce a new feature or product based on previous experience (36 months) |
| Email Guardian (only on particular Mac device) - Detections<br>• email subject<br>• sender email address<br>• email content or attachment<br>• detection type and name | **Service Provision** (1 month)<br>• For protection, detection, blocking, quarantining and deleting of malicious software |

Note that samples (files, URLs) used for malware analysis are kept in our systems as long as it is necessary to ensure proper functionality of the AV product. These samples are not connected with any identifiers or individuals and the retention periods indicated above do not apply to this use.

# Online Security & Privacy

**Official Product Name**

Online Security & Privacy

**Core Functionality**

Online Security & Privacy is a browser extension (or plug-in) available for Chrome, Firefox, Edge, Safari, and also Avast Secure Browser. Whenever you visit a website we check if the site isn't malicious or phishing. We are able to provide you with this functionality by processing URLs.

**What are Product's Features**

- **Antivirus** checks the links in search results so the user knows if the page is trying to spread malware.
- **Anti-phishing** identifies and blocks phishing sites trying to steal your data.
- **Anti-tracking** blocks annoying tracking cookies that collect data on your browsing activities.
- **Marking Search Results** shows if the site is safe or not even before the user visits it.
- **Advertising Data Collection** opts out from ads based on user personal interests. By opting out of interest-based advertising it means the company or companies from which you opt out will no longer show ads that have been tailored to your interests.
- **Privacy Advisor** allows optimizing privacy settings on the most popular online platforms via step-by-step guidance.
- **Global Privacy Contro**l is a third-party solution we have implemented in the settings, the user can send web companies he visits a "GPC" signal that he wants to opt out of website selling or sharing his personal information. See the specifics here.
- **Cookie Manager** automatically accepts or declines cookie consent preference banners while users browse the web.

## Personal Data We Process

While using Online Security & Privacy, we process the following Service and Device Data (in addition to Account Data and Billing Data for paid features):

| **Service Data** | **What we use it for and for how long** |
|---|---|
| URL | **Service Provision** (24 months)<br>● To check if URLs and the preceding referral domains or URLs (as applicable) are malicious or not to identify its source for threat analysis<br>● To ensure the functionality of cookie consent manager (allowed websites, troubleshooting) |
| Usage data<br>(open extension, rated site, disabled trackers, | **Service Provision** (24 months)<br>● To ensure functionality (installations, versions, updates, settings), map how users interact with the app and improve its design or flows |

| | |
|---|---|
| change settings, site blocked) | **Product and Business Improvement** (24 months)<br>● To measure user's behavior in UI and how user interacts with the extension |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Internal extension identifier (GUID) | **Service Provision** (24 months)<br>● To distinguish unique malware hits and evaluate it in our systems<br>**Product and Business Improvement** (24 months)<br>● To measure product telemetry and calculate statistics |
| Information on computer or device (hardware ID, browser, OS) | **Product and Business Improvement** (24 months)<br>● To obtain usage statistics |
| Extension information (installation source and time, version and campaign ID) | **Product and Business Improvement** (24 months)<br>● To obtain usage statistics, evaluate our messages and perform feature A/B testing |
| Location / Country | **Service Provision** (24 months)<br>● To detect country specific malware campaigns<br>**Product and Business Improvement** (24 months)<br>● To measure product telemetry and calculate statistics |
| Language | **Service Provision** (24 months)<br>● To make sure we communicate in right language<br>**Product and Business Improvement** (24 months)<br>● To measure product telemetry and calculate statistics |
| Antivirus Status | **Service Provision** (24 months)<br>● To being able to turn on Bank Mode which works only when Avast Antivirus is installed and offers to user to open page in a safe |

| | |
|---|---|
| | sandbox environment on sensitive sites (banking) |

# Passwords

## Official Product Name

Avast Passwords, Avast Passwords for Mac, Avast Passwords for iOS and Avast Passwords for Android (collectively as “Passwords”)

## Core Functionality

Passwords captures, stores in an encrypted storage and automatically fills passwords, credit cards and notes entered by you.

The product consists of several components that differ by platform:

- **Windows** - Avast Passwords browser extensions for Google Chrome, Mozilla Firefox, Avast Secure Browser and Microsoft Edge are paired with Avast Antivirus
- **Mac** - Avast Passwords browser extensions for Google Chrome, Mozilla Firefox and Safari are paired with standalone Avast Passwords for Mac application
- **Mobile** - standalone Avast Passwords for iOS and Avast Passwords for Android applications

## What are Product’s Features

- **Password Guardian** immediately receives a notification if any of your stored passwords are found leaked online to keep your identity safe. The functionality also reports weak and duplicate passwords.
- **Logins and Credit Cards** stores your usernames and passwords in an encrypted vault and secure them with a master password or operating system login credentials so that only you have access to them.

- **Secure Notes** provides the same encryption as Logins and Credit Cards to any notes added in the application.

## Personal Data We Process

Passwords and its components store encrypted information, so that only you as the user who stored this information has access to it. Avast cannot decrypt and read the data.

Unencrypted Service and Device Data are detailed as follows (in addition to Billing Data or Account Data, if relevant):

| **Service data** | **What we use it for and for how long** |
|---|---|
| Events and product usage (app metadata, number of hack alerts checks, number and result of Wi-Fi scans, error logs and screen flow) | **Service Provision** (24 months)<br>● To encrypt data synchronization<br>**Product and Business Improvement** (39 months)<br>● For development of new features or products |
| Information about user interaction with web pages | **Service Provision** (60 days raw data)<br>● To improve quality of login and password change forms recognition |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Random extension identifier | **Service Provision** (24 months)<br>● For users' support and troubleshooting<br>**Product and Business Improvement** (39 months)<br>● For development of new features or products |

| | |
|---|---|
| Operating System Version,<br>Avast Antivirus / Avast Passwords application Version,<br>Browser Version,<br>Extension Version | **Service Provision** (24 months)<br>● For users' support and troubleshooting<br>**Product and Business Improvement** (39 months)<br>● For development of new features or products |
| Config name / Config AB test ID | **Service Provision** (24 months)<br>● To propagate various configurations based on different configuration sets entry values |

# SafePrice

## Official Product Name

Avast SafePrice

## Core Functionality

SafePrice is a browser extension available for Chrome, Firefox, Edge and Safari. Whenever you visit an online shop or product site, SafePrice will show relevant price comparison and discount coupons.

## What are Product's Features

- **Discount coupons** and other promotional offers are typically provided by store owners to incentivize purchases. This means that these coupons are relevant to specific domains, and sometimes specific pages only. In order to be able to offer relevant coupons, we need to check the current page URL against a list of available offers.

- **Price Comparison** looks for specific portions of the HTML code which allows it to identify basic information about the product you are shopping for – product name, SKU and current price. We then compare this information with a database of prices provided by our partners, and offer cheaper prices for the same product where available.

Information about available offers, coupons or cheaper prices is obtained from Ciuvo. We request this content based on the information obtained from the page, your language settings, country level location and search query within SafePrice. Once you click on the offer, your request will be processed by Ciuvo according to its privacy policy.

## Personal Data We Process

While using SafePrice, we process the following Service and Device Data:

| **Service Data** | **What we use it for and for how long** |
|---|---|
| URL and referrers | **Service Provision** (36 months)<br>● To display discount coupons and price comparison offers relevant to the website that you are visiting |
| Search query | **Service Provision** (36 months)<br>● If submitted you, to search for relevant products and discount coupons |
| Product name and price | **Service Provision** (36 months)<br>● To display price comparison offers relevant to the product that you are shopping for |
| User's feedback (ratings, comments) | **Service Provision** (36 months)<br>● To tell whether the offers you received are relevant and up-to-date, and collect product feedback<br>**Product and Business Improvement** (36 months)<br>● To develop new products based on the user's feedback |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Internal extension identifier (GUID) | **Service Provision** (36 months)<br>● For ensuring continuous functionality and breaking down entries in database<br>**Product and Business Improvement** (36 months)<br>● To measure product telemetry and calculate statistics |

| | |
|---|---|
| Information on computer or device (browser) | **Product and Business Improvement** (36 months)<br>● To obtain usage statistics |
| Extension information (installation source and time, version and campaign ID) | **Service Provision** (36 months)<br>● To make sure our offers are relevant and product features function as expected<br>**Product and Business Improvement** (36 months)<br>● To obtain usage statistics, evaluate our marketing campaigns and perform feature A/B testing |
| Country | **Service Provision** (36 months)<br>● To make sure our offers are relevant, and collect statistics on SafePrice usage by country |
| Language | **Service Provision** (36 months)<br>● To make sure our offers are relevant, and collect statistics on SafePrice usage by language |

SafePrice does not process Account or Billing Data.

# Secure Browser

## Secure Browser for Desktop

### Official Product Name

Avast Secure Browser (“Secure Browser for Desktop”)

### Core Functionality

Secure Browser for Desktop is a product currently offered for PC Windows and for macOS users.

### What are Product’s Features

- **Browser Security & Privacy Center** is built in Security & Privacy Center which is a curated collection of some key security and privacy features, tools and settings, organized into one management console making it easier for you to control and manage your online privacy and security.
- **Anti-Phishing** protects you from accessing dangerous websites, such as fake sites, sites that have harmful programs such as adware, spyware, ransomware, viruses, all types of other malware that aim at stealing your information.
- **Privacy Cleaner** cleans all your browser history, all cookies including 3rd party, cached images, and other tracking scripts with just one click, to ensure that your online activity is private as well as free up space on your device.
- **Private Mode** allows you to surf the web privately without saving your browsing history, cookies and other site data or information entered in the websites that you have visited. When browsing with Private Mode you also have Anti-track, Adblock, and Anti-phishing enabled by default to ensure maximum privacy.
- **Adblock** stops ads from loading on the webpages you visit making your online experience cleaner, faster, safer, and more private. Avast Adblock has 3 states (Essential, Balanced and Strict) to allow you to set your own adblocking level in order to customise your online browsing.
- **Anti-Tracking** protects you from being tracked or monitored by websites you visit. Anti-Tracking technology blocks tracking scripts and cookies from being loaded on the websites or downloaded to your computer.
- **Anti-Fingerprinting** disguises your unique browser fingerprint (i.e. browser type, browser version, extensions, etc.) to help prevent websites from identifying and tracking you without your consent. Anti-Fingerprinting might cause some websites to break as it hides your information that sometimes is needed in order for the website to load (i.e. online banking they rely on your device's information to ensure that it is you).
- **Sync** means you can sign into the browser using your Avast ID or Google account. Your browsing data (including bookmarks, history, settings, open tabs, passwords, address, phone numbers, and payment information) will be then backed up and available across all your devices. If you sign into the browser using your Avast ID, we

receive information that you sync across devices in encrypted form and we are not able to access it or read it.

- **Built-in VPN** (virtual private network) that creates an encrypted connection between your device and the internet, securing your browsing data against eavesdroppers, trackers, and hackers. This VPN feature does not track or store connection timestamps, session information, bandwidth usage, traffic data, IP addresses, or other similar in nature data. Using a VPN will keep you more private and secure but you are still accountable for everything you do online.
- **Statistics** Are displayed to you throughout the product including the new tab page or via the Anti-tracking UI. Data is shared from our Adblock to give you realistic, realtime and useful data to enhance your browsing experience.
- **Avast Addons Store** is an online store created and maintained by Avast that allows you to view and install a wide range of extensions. On installation of each extension, you will be asked what data you can share with the extension. Extensions are addons that are built to extend the functionality of the browser itself or integrate an existing service with the browser.

## Personal Data We Process

By default, Secure Browser for Desktop processes locally on your system the following data:

- Browsing history information; for example Secure Browser for Desktop may store the URLs of pages that you visit, a cache of text, images and other resources from those pages. If the pre-rendering feature is turned on, a list of IP addresses linked to those pages may also be stored for some period of time;
- Name, surname, email or passwords to help you fill out forms or signs in to sites you visit;
- Permission that you have granted to websites;
- Cookies or data from websites that you visit;
- Data saved by add-ons;
- Record of what you downloaded from websites;
- Any feedback which you decide to share with us.

This data is not sent to our environment. You can manage this data within Secure Browser for Desktop under the “Advanced” section of the Settings page.

If you enable the Sync feature, we will process Sync data in our environment to ensure the sync across your devices.

In our environment we process the following Service and Device Data (in addition to Account Data and Billing Data, if relevant) while using Secure Browser for Desktop:

| **Service Data** | **What we use it for and for how long** |
|---|---|
| IP address | **Service Provision** (36 months)<br>● Replaced with country for delivering geo-specific changes to configuration (both local or remote)<br>● For prerendering feature functionality, if activated |
| URLs and referrers | **Service Provision** (36 months)<br>● If you enable the Anti-phishing feature, for protection, detection, blocking, quarantining and deleting of malicious software |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure functionality (installations, versions, updates, settings), map how users interact with the application and improve its design or flows<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users’ behavior (up to 60 months)<br>● Findings about product have an effect on the design or layout of the new one (36 months) |
| User’s feedback ratings | **Service Provision** (36 months) |

| | |
|---|---|
| | ● To ensure functionality and prevent crashes based on the user's feedback<br>**Product and Business Improvement** (36 months)<br>● To improve the product or its feature based on the user's feedback |
| User's feedback comments | **Service Provision** (36 months)<br>● To ensure functionality and prevent crashes based on the user's feedback<br>**Product and Business Improvement** (36 months)<br>● To improve the product or its feature based on the user's feedback |
| Sync data (bookmarks, history, settings, open tabs, passwords, address, phone numbers, and payment information (name on card, card number, expiration date)) | **Service Provision** (3 months)<br>● If you enable the Sync feature to ensure the sync of browser data across devices |
| Secure Browser VPN events (such as "upgrade now" clicks, "free trial" clicks (called "application event identifier")) | **Service Provision** (36 months)<br>● If you enable the VPN feature to ensure the functionality (installations, versions, updates, settings), map how users interact with the application and improve its design or flows<br>**Product and Business Improvement** (36 months)<br>● If you enable the VPN feature, for product improvements, and development planning as we aim at developing best-in-class products |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUIDs, Device IDs) | **Service Provision** (36 months)<br>● For ensuring continuous functionality and breaking down entries in database<br>**In-product Messaging** (24 months) |

| | |
|---|---|
| | ● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (60 months)<br>● To introduce a new feature or product based on previous experience (36 months) |
| Information concerning computer or device | **Service Provision** (36 months)<br>● To check for compatibility issues in automated crash dumps<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (60 months)<br>● To introduce a new feature or product based on previous experience (36 months) |
| Location | **Service Provision** (36 months)<br>● Setting up a proper product language version for Windows<br>**In-product Messaging** (6 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand users' behavior (50 months)<br>● To introduce a new feature or product based on country (36 months) |
| Third-party extensions installed in the browser | **Service Provision** (36 months)<br>● To define rules of how the Browser should behave in relation to extensions installed (e.g. exceptions in scanning, filtering, notifications, whitelisting, blacklisting) |

| | |
|---|---|
| | **Product and Business Improvement**<br>● To better understand users' behavior (60 months)<br>● To introduce a new feature or product based on user engagement and preferences (36 months) |
| Other Avast products/licenses on the device and their status | **Service Provision** (36 months)<br>● To recognize what features should be enabled or disabled, what product should be installed or uninstalled<br>**Product and Business Improvement** (60 months)<br>● To better understand users' behavior |
| Browsers (installed, default) | **Service Provision** (36 months)<br>● To provide import functionality, improve user onboarding and product experience<br>**Product and Business Improvement**<br>● To better understand users' behavior (60 months)<br>● To introduce a new feature or product based on previous experience (36 months) |

The third-party analytics tools we use for Secure Browser for Desktop are:

- Google Analytics
- Mixpanel

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

Secure Browser for Desktop cooperates with these search engines:

- Google
- Yahoo
- Bing
- Seznam.cz
- Yandex.ru

For further information regarding these search engines please refer to their privacy policies under the links above.

Secure Browser for Desktop serves advertisements in cooperation with:

- Sovrn
- AdMarketplace
- Mocha
- Amazon
- Priceline
- AliExpress

For further information regarding these partners please refer to their privacy policies under the links above.

## Secure Browser for Mobile

### Official Product Name

Avast Secure Browser for Android and Avast Secure Browser for iOS (collectively as "Secure Browser for Mobile")

### Core Functionality

Secure Browser for Mobile is a private mobile browser offered for Android and iOS users.

### What are Product's Features

- **Browser Security & Privacy Center** is built in Security & Privacy Center which is a curated collection of some key security and privacy features, tools and settings, organized into one management console making it easier for you to control and manage your online privacy and security.
- **Adblock** stops ads being shown in your browser using publicly available blocking lists. AdBlock usually does not remove ads, it already prevents them from being loaded and thus also speeds up browser experience.
- **Anti-Tracking** prevents the user from being tracked across websites by avoiding tracking cookies to be created. This is done using publicly available blocking lists. Anti-Tracking usually does not remove the

tracking cookies, instead it prevents them from being loaded and created and thus also speeds up browser experience.

- **Anti-Fingerprinting** prevents the user from being tracked across websites using browser fingerprinting techniques. As fingerprinting itself cannot be prevented or avoided, this feature prevents being tracked by altering the digital fingerprint of the user's browser in a way that third-party sites cannot re-identify it.
- **Web Shield** protects you from accessing dangerous websites, such as fake sites, sites that have harmful content such as adware, spyware, ransomware, viruses, all types of other malware that aim at stealing your information.
- **Built-in VPN** (virtual private network) creates an encrypted tunnel between your device and the internet, securing your browsing data against eavesdroppers.
- **Security Scanner** feature will scan the device, its internet connection and browser configuration (otherwise known as Browser Shields) for threats and vulnerabilities, process the findings, and display a result screen with potential improvements.
- **Nuke** cleans your browser history, cached images, cookies including both first-party and third-party cookies, and other junk with just one click for a specified domain, to keep your activity on that domain private and free up disk space.
- **Remove Site Data** cleans your browser history, site cookies, and offline data with the current site with just one click, to keep your activity private and free up disk space.
- **Video Downloader** enables you to download videos from supported websites to your device.
- **Media Vault** allocates your files, including those you download during your browsing sessions, to the browser application’s encrypted file system. These files are stored on your device and are accessible through the browser application.
- **Secure Mode** encrypts your DNS queries, stops ads being shown in your browser, prevents your browsing history from being stored, and removes any tracking cookies (both first-party cookies and third-party cookies) or web cache you pick up during that browsing session.
- **Secure & Private Mode** creates an encrypted tunnel between your device and the internet, encrypts your DNS queries, stops ads being shown in your browser, prevents your browsing history from being stored, and removes any tracking cookies (both first-party cookies and

third-party cookies) or web cache you pick up during that browsing session.

- **PIN Protection** secures your device against real world threats from local attacks by locking access to the browser application on your device with a unique code only you know. Your PIN Code is encrypted on disk and is not stored on any servers.
- **Sync** means you can sign into the browser using your Avast ID. Your browsing data (including bookmarks, history, settings, open tabs, passwords, address, phone numbers, and payment information) will be then backed up and available across all your devices. All backed-up data is encrypted with an industry standard cryptographic scheme, and can only be decrypted by the user.
- **Privacy Statistics** are showing the users' the advantage of our AdBlock and VPN through numbers, by presenting the number of ads blocked, number of malware blocked by our Web Shield, amount of browsing data protected by our VPN.

## Personal Data We Process

By default, Secure Browser for Mobile processes locally on your system the following data:

- Browsing history information; for example Secure Browser for Mobile may store the URLs of pages that you visit, a cache of text, bookmarks, zones, images and other resources from those pages.
- Permission that you have granted to websites;
- Cookies or similar technologies such as pixel tags and web beacons from websites that you visit;
- Records of what you downloaded from websites when using Media Vault.

This data is not sent to our environment. You can manage this data within Secure Browser for Mobile under the "Browsing Mode Settings" and "Data Settings" section of the Security & Privacy Settings page.

If you enable the Sync feature, we will process Sync data in our environment to ensure the sync across your devices.

In our environment we process the following Service and Device Data while using Secure Browser for Mobile (in addition to Account Data and Billing Data, if relevant):

| **Service Data** | **What we use it for and for how long** |
|---|---|
| IP address | **Service Provision** (per session)<br>● Replaced with country for delivering geo-specific changes to configuration (both local or remote)<br>● For prerendering feature functionality, if activated |
| Events and product usage | **Service Provision** (36 months)<br>● To ensure functionality (installations, versions, updates, settings), map how users interact with the application and improve its design or flows<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (up to 24 months)<br>● Findings about product have an effect on the design or layout of the new one (24 months) |

| | |
|---|---|
| Sync data (bookmarks, history, ) | **Service Provision** (3 months)<br>● If you enable the Sync feature to ensure the sync of browser data across devices |

| **Device Data** | **What we use it for and for how long** |
|---|---|
| Online identifiers (GUIDs, Device IDs) | **Service Provision** (24 months)<br>● To ensure functionality (installations, versions, updates, settings) and to track users subscription trials and purchases<br>**In-product Messaging** (24 months)<br>● To inform users of problems that will not be solved by the currently installed product and to offer users a solution to the detected problem<br>**Product and Business Improvement**<br>● To better understand our users' behavior (24 months)<br>● To introduce a new feature or product based on previous experience (24 months) |

| | |
|---|---|
| Information concerning computer or device | **Service Provision** (36 months)<br>● To check for compatibility issues in automated crash dumps<br>**Product and Business Improvement**<br>● To better understand users' behavior (24 months)<br>● To introduce a new feature or product based on previous experience (48 months) |

These are the third-party analytics tools we use for Secure Browser for Mobile:

- Google Firebase Analytics and Crashlytics for Android
- Appsflyer

For further information regarding our third-party analytics partners, including their privacy policies, please refer to our Privacy Policy.

Secure Browser for Mobile cooperates with these search engines:

- Google

Secure Browser for Mobile serves advertisements in cooperation with:

- Sovrn
- AdMarketplace
- Mocha
- Amazon

- Priceline
- AliExpress

For further information regarding these partners please refer to their privacy policies under the links above.

# Secure Identity

### Official Product Name

Avast Secure Identity

### Core Functionality

Secure Identity helps keep yourself safe with the advanced identity protection - including credit monitoring, alerts to help you determine if your identity has been compromised and specialist support.

### Personal Data We Process

The product is provided in cooperation with Sontiq, Inc. We share your name, surname, license ID and email with Sontiq so that they can prepare the service for you. The data processing within the product is governed by this Privacy Notice.

# SecureLine

Avast SecureLine VPN (collectively as “VPN”)

We are a leading provider of security and privacy tools and therefore we are deeply committed to protecting and respecting your privacy. Our VPN Policy (together with any other documents referred to in it) sets out the basis on which any data we collect from you, or that you provide to us, will be processed by us.

# WebTrails

## Official Product Name

WebTrails

## Core Functionality

WebTrails is a browser extension (or plug-in) available for Chrome. It provides an alternative view of browsing history with detailed analysis and visualisations of privacy leaks and behaviour patterns. All reports are generated locally in the browser and no data is sent out to any remote servers.

All analyses are performed on-demand, on the device and with the data stored in your browser. No history data for these analyses is stored.

## What are Product's Features

- **PII leak detection** looks for any personal data (e.g., plaintext names, emails) in URLs visited, based on the Chrome browsing history.
- **Habits** generates browsing behaviour habits charts, based on URLs.
- **Social, Search, Video and Locations** provides detailed usage reports. Location information is derived from the URLs.

## Personal Data We Process

While using WebTrails, we process the following Service and Device Data:

| Service Data | What we use it for and for how long |
|---|---|
| URLs and access time stored in your Chrome browsing history | **Service Provision** (not stored by us)<br>• To generate detailed reports and provide users with insights into their browsing behaviour and habits. |

WebTrails does not process Account, Billing and Device Data.