# Products Policy

This Policy was last updated on September 30, 2025.

## 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, Essential Business Security, Premium Business Security, Ultimate Business Security, Small Office Protection

(collectively as “Antivirus for Desktop”)

#### Core Functionality

The Antivirus for Desktop provides protection against malicious, harmful or unwanted software and technologies as well as detection for advanced scams. It may also detect other 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 helps detects browser threats, outdated applications, hidden viruses, system issues, online privacy threats and other issues depending on the provided features.
- **Protection features** provide core defenses for blocking malware and other threats including protection against malicious files, QR codes, suspicious applications, web attacks and unsafe downloads, unauthorized remote access attempts or dangerous email attachments. To do this, we scan files, programs, applications, attachments, URLs or

other sources for potential threats. Sometimes, we may directly analyze suspicious files in our safe environment to make sure you are protected.

- **Network inspector** scans for vulnerabilities and potential security issues in your network (including for example router and connected devices).
- **Firewall** helps control what data goes in and out of your computer to block traffic from malicious sources and prevent unauthorized access to your device.
- **Scam Guardian** features help block potentially dangerous websites and analyze texts, emails, messages or other media to avoid scams. It can also respond, if possible, to questions related to cybersecurity or our products.
- **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.
- **Email Guard** is a cloud-based service which monitors emails from supported providers for potential threats. By default, we don't store the emails, but we create and store non-personal numeric representations of the text to detect potential scam and other unwanted messages. You can allow us to store the whole email message (EML file with message metadata) we identified as suspected malicious by consenting to it in the product. This helps us keep better detections and improve the protection against scams. Our human reviewers may check the email message in case it is needed to investigate the accuracy of our detections (esp. in case of false negatives or false positives). Suspicious messages in the raw form are stored for 30 days and then we remove personal identifiers and keep them in our malware database. 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.
- **Hack Alerts** 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 features** (Browser Shield, Webcam Shield, Sensitive Data Shield and other similar shields) provide an extra layer of protection for your browser data, passwords, sensitive documents, webcam, microphone or other assets against malware and unauthorized access. Sensitive data shield checks your hard drive and looks for files that contain sensitive data. It helps secure your private data by controlling which applications and users have access to selected files.

## 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 and source of malicious software - IP address is part of malware infection file |
| Samples, files | **Service Provision** (36 months)<br>● For protection, detection, analysis, blocking, quarantining and deleting of malicious software |

| | |
|---|---|
| | ● For protecting files containing sensitive information (not stored) |
| Detection metadata | **Service Provision** (36 months)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |
| URLs and referrers (malicious URL information may also include search terms or cookie information associated with the malware) | **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 |
| User credentials (usernames, hashes of passwords) | **Service Provision** (90 days)<br>● To provide with password safety checks and inform users about potential leaks |
| 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 |

| | |
|---|---|
| | **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) |
| Email Guard - Email | **Service Provision**<br>● In order to check your email and detect threats, we download it whole, together with metadata and attachments. By default, we keep it in our systems only during the processing, we don't store it except the non-personal numeric representation of it. (seconds)<br>● If you consent, we can store suspicious email messages for in-depth analysis and to keep our detection models up to date (30 days in raw form, 60 months in de-identified form) |
| Email Guard – malicious identifiers (URL, phone, email, crypto, or other identifier types that may be identified as significant for threat detection) | **Service provision** (60 months)<br>● We extract malicious identifiers from emails to maintain our threat detection models up to date |
| Email Guard - Snippets of email around detected phone numbers | **Service provision** (30 days)<br>● To detect malicious phone numbers, we analyse snippets of the message around detected phone numbers (few words before and after). These snippets are not connected to you. |
| Email Guard - Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |

| | |
|---|---|
| Email Guard - 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 Guard - 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<br>• IP addresses of mail servers (SMTP servers) | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance of detections<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |
| Email Shield - Detections<br>• email subject<br>• sender email address | **Service Provision** (1 month)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |

| | |
|---|---|
| • email content or attachment<br>• detection type and name | |
| Scam protection – texts, images, emails, messages or other similar samples submitted for scam check | **Service Provision** (30 days)<br>For detecting scams, evaluating potential cybersecurity risks, and helping to assess risks involved in the submitted information. |
| Scam Assistant - user conversations, questions or anything you submit | **Service Provision** (30 days)<br>● For effective functioning and for the purpose of responding to the questions or other inputs<br>**Product and Business Improvement** (30 days)<br>● For improving the quality of future conversations |
| Scam Assistant – samples and conversations with personal identifiers removed, detected malicious identifiers used in scam attempts (URLs, phone numbers, emails etc.) | **Service Provision**<br>● For effective detection of scams (as long as necessary to ensure effective protection but not stored in connection to users)<br>**Product and Business Improvement**<br>• For improving the scam detection rate (as long as necessary to ensure effective protection but not stored in connection to users) |
| Scam Assistant - Reporting data based on metadata collected by product (limited to number of users by general geolocations/regions, and operating systems) | **Product and Business Improvement** (25 months)<br>● For further developing and improving the product performance. |

| **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)<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) |
| 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 |

| | |
|---|---|
| | **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<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 |
| 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><br>**Product and Business Improvement** (36 months)<br><br>● To introduce a new feature or product based on previous experience |
| Browsers (installed, default) | **Service Provision** (36 months)<br><br>● For opening content in given browser<br><br>**In-product Messaging** (6 months)<br><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><br>**Product and Business Improvement**<br><br>● To better understand users' behavior (50 months)<br><br>● To introduce a new feature or product based on previous experience (36 months) |

Note that samples (files, URLs and other malicious identifiers) used for malware and scam 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 users or other 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 cybersecurity with added privacy features. It helps block malware, check the safety of installed apps, and scan public Wi-Fi networks for possible security weaknesses.

## What are Product’s Main Features

- **Smart Scan** scans your device for malware apps and files and various types of cybersecurity vulnerabilities.
- **Network inspector and Wi-Fi Speed Check** enables you to scan your network for vulnerabilities, and tests the speed of the network.
- **Web Guard** helps detect and notify you when accessing a malicious website that could represent a potential online security risk for you.
- **App Locking** helps protect your sensitive apps with a PIN, pattern, or fingerprint.
- **App Insights** 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.
- **Junk Clean** 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** 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.
- **VPN** feature helps protect your online privacy by encrypting your online communication. It allows you to pick a specific location to be connected from. Our VPN Policy sets out the basis on which any data we collect from you, or that you provide to us, will be processed by us.
- **Link Guard** helps warn you if you tap a dangerous link from an email, SMS, or messaging app by checking the URLs you visit.
- **SMS Guard** scans incoming messages for potential scam.

- **Call Guard** helps identify scam, junk, or business calls. Calls can be either labelled or automatically blocked per user preference. The feature is provided in cooperation with Hiya Inc.
- **Email Guard** is a cloud-based service which monitors emails from supported providers for potential threats. By default, we don't store the emails, but we create and store non-personal numeric representations of the text to detect potential scam and other unwanted messages. You can allow us to store the whole email message (EML file with message metadata) we identified as suspected malicious by consenting to it in the product. This helps us keep better detections and improve the protection against scams. Our human reviewers may check the email message in case it is needed to investigate the accuracy of our detections (esp. in case of false negatives or false positives). Suspicious messages in the raw form are stored for 30 days and then we remove personal identifiers and keep them in our malware database. 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.

## 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><br>**Product and Business Improvement** (50 months)<br><br>∉ To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br><br>● To detect the approximate location and source of malicious software - IP address is part of malware infection file |
| Samples, files | **Service Provision** (36 months)<br><br>● For the functionality of malware scanning and analysis |
| Detections | **Service Provision** (36 months)<br><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><br>● For detection of malicious websites |
| User's email address associated with your Account | **Service Provision (36 months)**<br><br>● To search for your credentials in data breaches. |

| | |
|---|---|
| | ● To send a requested report to you on whether or not their credentials have leaked.<br><br>**Product and Business Improvement** (36 months)<br><br>● To improve the user's overall experience |
| User's email for Hack Alerts | **Service Provision** (36 months)<br><br>● To send a requested report to you on whether or not their credentials have leaked<br><br>**Product and Business Improvement** (36 months)<br><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><br>● To ensure continuous functionality (installations, versions, updates, settings)<br><br>**Product and Business Improvement**<br><br>● To understand the user's behavior (14 months)<br><br>To improve the user's overall experience (36 months) |
| Email Guard – Email | **Service Provision**<br>● In order to check your email and detect threats, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it except the non-personal numeric representation of it. (seconds) |

| | |
|---|---|
| | ● If you consent, we can store suspicious email messages for in-depth analysis and to keep our detection models up to date (30 days in raw form, 60 months in de-identified form) |
| Email Guard – malicious identifiers (URL, phone, email, crypto, or other identifier types that may be identified as significant for threat detection) | **Service provision** (60 months)<br>● We extract malicious identifiers from emails to maintain our threat detection models up to date |
| Email Guard – Snippets of email around detected phone numbers | **Service provision** (30 days)<br>● To detect malicious phone numbers, we analyse snippets of the message around detected phone numbers (few words before and after). These snippets are not connected to you. |
| Email Guard – Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guard – 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 Guard – Detections<br>• hash of the email<br>• hash of the userID<br>• email subject<br>• hash of sender email address | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance of detections<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |

| | |
|---|---|
| • domain address of sender<br>• detection type and name<br>• name of the attachments and their hashes<br>• country of the user<br>• IP addresses of mail servers (SMTP servers) | |
| Email Guard– 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 |
| Call Guard<br>• incoming phone numbers, line type, country (for incoming non-contact calls); time, length and disposition of phone call | **Service Provision** (36 months, incoming phone number removed after 30 days)<br>● For the functionality of call filtering and evaluation of caller reputation.<br><br>**Product and Business Improvement** (12 months)<br>● To fix bugs, improve the detection models and to create, use and store aggregated statistics derived from call information to help us analyze unsolicited calls. The information is not connected to you. |

| | |
|---|---|
| SMS Guard<br>• text messages with URLs or sent by senders not in the contact list stripped off the user personal identifiers (may include phone numbers, emails, crypto identifiers, identifiers offered to user as target for user's requested response or other identifiers associated with the text message) | **Service Provision**<br>• For detection of malicious SMS (texts stripped off the personal identifiers together with URLs and other sender identifiers are stored up to 5 years) |

| **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) |

| | |
|---|---|
| | ∉ 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>● 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** |

| | |
|---|---|
| | ● 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) |
| 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) |

| | |
|---|---|
| | • 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
- Singular

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
- ∉ Liftoff Mobile

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 Mobile Security for iOS

**Core Functionality**

Avast Mobile Security for 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 VPN, which are described in detail below.

**What are Product's Features**

- **Smart Scan** scans your device for malware apps and files and various types of cybersecurity vulnerabilities.
- **Network inspector and Wi-Fi Speed Check** enables you to scan your network for vulnerabilities, and tests the speed of the network.
- **Web** Guard helps detect and notify you when accessing a malicious website that could represent a potential online 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 helps secure them with a PIN, Touch ID, or Face ID so that only you have access to them.
- **VPN** feature helps protect your online privacy by encrypting your online communication. It allows you to pick a specific location to be connected from. 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.

- **SMS Guard** scans incoming messages for potential scam.
- **Call Guard** helps identify scam, junk, or business calls. Calls can be either labelled or automatically blocked per user preference. The feature is provided in cooperation with Hiya Inc.
- **Email Guard** is a cloud-based service which monitors emails from supported providers for potential threats. By default, we don't store the emails, but we create and store non-personal numeric representations of the text to detect potential scam and other unwanted messages. You can allow us to store the whole email message (EML file with message metadata) we identified as suspected malicious by consenting to it in the product. This helps us keep better detections and improve the protection against scams. Our human reviewers may check the email message in case it is needed to investigate the accuracy of our detections (esp. in case of false negatives or false positives). Suspicious messages in the raw form are stored for 30 days and then we remove personal identifiers and keep them in our malware database. 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.

## Personal Data We Process

While using Avast Mobile Security for 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) | **Service Provision** (36 months)<br>● For detection of malicious websites |

| | |
|---|---|
| Timestamps of your connections for VPN | **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 VPN | **Service Provision** (36 months)<br>● To plan for increased network demand and capacity |
| IP address of the VPN server you're using for VPN | **Service Provision** (36 months)<br>● To troubleshoot our service and plan for new network capacity |
| Amount of data transmitted for VPN<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 Guard – Email | **Service Provision**<br>● In order to check your email and detect threats, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it except the non-personal numeric representation of it. (seconds)<br>● If you consent, we can store suspicious email messages for in-depth analysis and to keep our detection models up to date (30 days in raw form, 60 months in de-identified form) |
| Email Guard – malicious identifiers (URL, phone, email, crypto, or other identifier types that may be identified as significant for threat detection) | **Service provision** (60 months)<br>● We extract malicious identifiers from emails to maintain our threat detection models up to date |
| Email Guard – Snippets of email around detected phone numbers | **Service provision** (30 days)<br>● To detect malicious phone numbers, we analyse snippets of the message around detected phone numbers (few words before and after). These snippets are not connected to you. |
| Email Guard – Hash of email address of sender | **Service Provision** (36 months) |

| | |
|---|---|
| | ● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guard – 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 Guard – 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<br>• IP addresses of mail servers (SMTP servers) | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance of detections<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |
| Email Guard– Detections<br>• email subject | **Service Provision** (1 month)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |

| | |
|---|---|
| • sender email address<br>• email content or attachment<br>• detection type and name | |
| Call Guard<br>• incoming phone numbers, line type, country (for incoming non-contact calls); time, length and disposition of phone call | **Service Provision** (36 months, incoming phone number removed after 30 days)<br>● For the functionality of call filtering and evaluation of caller reputation.<br>**Product and Business Improvement** (12 months)<br>● To fix bugs, improve the detection models and to create, use and store aggregated statistics derived from call information to help us analyze unsolicited calls. The information is not connected to you. |
| SMS Guard<br>• text messages with URLs or sent by senders not in the contact list stripped off the user personal identifiers (may include phone numbers, emails, crypto identifiers, identifiers offered to user as target for user's requested response or other identifiers associated with the text message) | **Service Provision**<br>● For detection of malicious SMS (texts stripped off the personal identifiers together with URLs and other sender identifiers are stored up to 5 years) |

| **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 Mobile Security for iOS:

- ∉ Google Firebase Analytics and Crashlytics for iOS
- ∉ AppsFlyer
- ∉ Singular

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

AntiTrack helps keep your online activities and digital footprint private. Its key features help to obscure your identity from tracking and fingerprinting attempts made by browsers and individual websites.

## What are the Product’s Features

- **Anti Fingerprinting** helps stop scripts from fingerprinting the user’s device and tracking their browsing behavior across the web.
- **Fingerprint Randomizer** will automatically change the user’s digital ‘Fingerprint’ in regular intervals, or allow the user to manually change said ‘Fingerprint’.
- **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.
- **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.
- **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.
- **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.

## 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 |
|---|---|

| | |
|---|---|
| Events and product usage | **Service Provision** (36 months)<br><br>• To provide feature enhancement, customer support and product maintenance |
| Browser information (including information about extensions and browser properties and parameters) | **Service Provision** (processed on device, not stored)<br><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>  ○ To obfuscate browser information as part of the Anti-Fingerprint feature |
| Cookies | **Service Provision** (processed on device, not stored)<br><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** ( processed on device, not stored)<br><br>• To add websites into the Allowed Websites list. |
| Website Tracker Details (Javascript, HTML documents) | **Service Provision** ( processed on device, not stored)<br><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><br>**In-product messaging** (6 months)<br><br>• To update the user about product status |

| | |
|---|---|
| Crash reports | **Service Provision** (90 days)<br>• To ensure continuous functionality |
| Reported URL problems | **Service Provision (36 months)**<br>• To ensure proper functionality and resolve reported problems with URLs |

| Device Data | What we use it for and for how long |
|---|---|
| OS information (version, keys, tasks) | **Service Provision** (36 months)<br>• To provide user support, troubleshooting, and product development planning<br><br>**Product and Business Improvement (36 months)**<br>• When developing new features - to adjust the scope of the feature based upon the requirements and the functionality of certain operating systems<br>• To better understand how users' interact with certain aspects |
| OS Locale | **Service Provision** (36 months)<br>• To segment updates by location<br><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><br>**Product and Business Improvement** (36months)<br><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 |
| Internal online identifiers (hardware ID) | **Service Provision** (36 months)<br><br>• To install the product, provide application updates, customer support<br><br>**Product and Business Improvement** (36 months)<br><br>• To better understand how users' interact with certain aspects |

The third party analytics tools we use for the AntiTrack are Firebase and Apple Appstore crashlytics 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) |

| | |
|---|---|
| | ● 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 | **Service Provision** (12 months) |

| | |
|---|---|
| the device and their status | • To recognize what features should be enabled or disabled, what product should be installed or uninstalled<br><br>**In-product Messaging** (12 months)<br><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. Help remediate past breaches and minimise the risk of abuse of their data in the future.

1. Helping users to discover and fix online privacy threats.
2. Help 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** provides dark web monitoring for leaked personal information. BreachGuard leverages a comprehensive database of the dark web – it works to detect 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 on your behalf to available data brokers in North America. .
- **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 24/7to educate customers about how identity theft and cyberthreats occur, as well as provide tips and tools to help keep their online 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**.**
- Browsing information (URL) and bookmarks – to highlight relevant privacy guides.

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** |
|---|---|
| Emails | **Service Provision** (while active) |

| | |
|---|---|
| | ● To check and monitor for breaches |
| Hashed credentials | **Service Provision** (not stored)<br><br>● To check and monitor for breaches |
| 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)<br>● For development of new features or products |
| Hardware Data | **Service Provision** (24 months)<br>● For users' support and troubleshooting |

| | |
|---|---|
| e.g. Device Model (e.g. Windows 10 (13-inch 2017), RAM (Random Access Memory), GPU (Graphical Processing Unit), and Central Processing Unit (CPU) | **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 works to speed up and clean your PC (Windows and Mac), updates installed apps, and helps fix 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 help fix 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 works to fix system drive or defrag your system drive.
- **Software Updater** scans and provides updates to third-party programs and their versions installed on PC.
- **Cloud Cleaner** feature helps users manage their cloud storage (optimize, remove duplicates) by checking metadata associated with stored files and pictures. Files and pictures are not downloaded or stored by us. To connect to Google Drive, 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.

Avast Cleanup Premium for Mac:

- **Clutter Scan** scans and allows to delete 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 offers to remove 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<br><br>(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) |
| File meta data (checksum, archive_state, created_date, modified_date, folder_path, file_name, file_size, file_type, file_id and thumbnail_link) | **Service Provision**<br>∉ To help manage storage of files (24 hours)<br>∉ To monitor service functionality and make it more reliable (90 days) |

| **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) helps detect and remove unnecessary files to free up storage space. Equally, it can help 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 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 |

| | |
|---|---|
| | **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) |

| | |
|---|---|
| | ● 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><br>**Product and Business Improvement**<br><br>● To better understand our users' behavior (14 months)<br><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><br>● Delivering geo-specific changes to app's configuration (both local or remote)<br><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><br>**In-product Messaging** (6 months)<br><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><br>**Product and Business Improvement**<br><br>● To better understand users' behavior based on approximate location (14 months)<br><br>● To introduce a new feature or product based on approximate location (36 months) |
| Applications | **Service provision** (36 months)<br><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><br>**In-product Messaging** (6 months)<br><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><br>**Product and Business Improvement** (14 months)<br><br>● To better understand users’ behavior |
| Internet and connection | **Service provision** (36 months)<br><br>● For functionality of our features, providing error messaging<br><br>**In-product Messaging** (6 months)<br><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><br>**Product and Business Improvement**<br><br>● To better understand users’ behavior (14 months)<br><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
- ∉ Singular

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 help 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 |

| | |
|---|---|
| | **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<br>(driver version, updated date, name, matching device id, driver rank, driver flags) | **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><br>**Product and Business Improvement** (12 months)<br><br>∉ To better understand our users' behavior<br><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><br>● To set up a proper product language version for Windows<br><br>**In-product Messaging** (12 months)<br><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><br>**Product and Business Improvement** (12 months)<br><br>● To better understand users' behavior based on approximate location<br><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><br>● To recognize what features should be enabled or disabled, what product should be installed or uninstalled<br><br>**In-product Messaging** (12 months)<br><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 helps keep 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 |

| | |
|---|---|
| | • 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<br>• 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) |

| | |
|---|---|
| | ● 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><br>**Product and Business Improvement** (up to 24 months)<br><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><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><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 |

| | |
|---|---|
| | **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 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 cybersecurity 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.
- **Automatic Email Alerts** which monitors the SpyCloud database and will send the user an email if 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

## Official Product Name

Avast Business Hub

## Core Functionality

The Business Hub enables you 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 the Business Hub certain settings related to privacy are managed by and information from managed devices is accessible to the administrator of the console or the Managed Service Provider you chose. 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 cybersecurity 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** include instant email notifications on any cybersecurity threats or network issues that need your attention, including outdated antivirus applications, extended device inactivity, and additional device update.

- **Reporting** shows detailed reports that include blocked threats, task lists, and protected devices, making it simple to improve cybersecurity 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** 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 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.
- **Content Filtering** boosts productivity and cybersecurity by controlling your employees' internet usage and allowing to restrict their access to specific websites or website categories.
- **USB Protection** is a service allowing you to control access to USB flash drives, external HDDs, optical discs, memory cards, digital cameras, smartphones (Windows only), tablets (Windows only), and other devices that have storage capabilities. With this service, removable devices won't be able to access your end users' data without permission.

## Personal Data We Process

We process only the following Data (in addition to Account Data and Billing Data, if you purchased paid services or products from us):

| **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, removable device name and serial number (for USB Protection) | **Service Provision**<br>● To better identify and manage devices detected on the network<br>● To determine whether it supports installation of Avast services |

| | |
|---|---|
| Information concerning computer or device (OS build, display) | **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 |
| 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 |
| 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** |

| | |
|---|---|
| | ● To better understand users' behavior based on approximate location<br>● To introduce a new feature or product based on approximate location |
| Language, time zone | **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**<br>● 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 |
| Our other products/licenses on the device and their status | **Service Provision**<br>● For administrators to have an overview of running services and expiration dates |
| | ● |

| | |
|---|---|
| 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 |
| Audit Logs | Service Provision<br>∉ To provide record of changes in application and endpoints |

| **Admin and User Data** | **What we use it for** |
|---|---|
| Name, surname, email address, locales | **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, business, finance and tax details and contact information | **Service Provision**<br>● To provide support and to contact the company when needed<br>● To process product purchases<br>● To renew & license products |
| Business type | **Service Provision**<br>● To offer the right solution based on the type of the company |

We will process the data described above only as long as necessary for the purposes we described. We delete the data we collected within 60 days after the termination of the service.

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 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.

# CloudCare

**Official Product Name**
Avast Business CloudCare

**Core Functionality**

CloudCare enables you 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 It also allows you to purchase subscriptions and manage them conveniently from a single platform.

Please note that, through CloudCare, certain settings related to privacy are managed by and information from managed devices is accessible to the administrator of the console or the Managed Service Provider you chose. Businesses are responsible for informing you about this fact and instructing administrators about best practices to ensure users' privacy.

## What are Product's Features

- **Dashboard** allows you to monitor the status of the managed devices, including their cybersecurity, allocation of subscriptions and service usage.
- **Alerts** allow you to configure and customize alerts which, if triggered by certain events, will be sent to selected users by email and/or texted to mobile numbers (available for selected wireless service providers).
- **Devices** provide detailed information on the status and active services for each enrolled device. It gives you the tools to deploy CloudCare services to more devices.
- **Policies** give you the ability to define sets of rules and settings for each service that will be enforced on the endpoint devices.
- **Account** and services allow you to view and manage the information we store about your company, users and companies that you added to the platform. It also allows you to buy and manage subscriptions that entitle you to use particular service on a particular set of devices.
- **Community forum** allows CloudCare partners to discuss their issues, needs, and provide feedback on CloudCare. This forum is also attended by our customer care staff.
- **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.
- **Updates** remotely downloads and distributes virus and program updates to all devices from one console to save time and bandwidth.
- **Reports** provide on-demand summary of blocked threats, task lists, and protected devices, making it simple to improve cybersecurity and customize the protection.
- **Online Backup** 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 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** 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** boosts productivity and cybersecurity by controlling your employees' internet usage, helps prevent devices from accessing malicious content, and allows the admin to restrict access to specific sites or content categories.

## Personal Data We Process

We process the following Data (in addition to Account Data and Billing Data, if you purchased paid services or products from us):

| **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><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><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 Online Backup |
| 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><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><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, time zone | Service Provision<br>● To set the right language settings |

| **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><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><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><br>Product and Business Improvement<br>● To better understand our users' behavior<br>● To introduce a new feature or product based on previous experience |

| | |
|---|---|
| Audit Logs | Service Provision<br>● To provide record of changes in application and endpoints |

| **Admin and User Data** | **What we use it for** |
|---|---|
| Name, surname, email address, locales | 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, business, finance and tax details and contact information | Service Provision<br>● To provide support and to contact the company when needed<br>● To process product purchases<br>● To renew & license products |
| Business type | Service Provision<br>● To offer the right solution based on the type of the company |

We will process the data described above only as long as necessary for the purposes we described. We delete the data we collected within 60 days after the termination of the service.

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.
- Payments are processed by our partner BrainTree. See their 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) includes a comprehensive set of features that provide protection against potential online 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 cybersecurity vulnerabilities.
- **Malware Shields** scans new apps and files being downloaded to the device for malware.
- **VPN** feature helps protect your online privacy by encrypting your online communication. 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** helps detect and notify you when accessing a malicious website that could represent a potential online security risk for you.
- **Data Breach 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 Guard** is a cloud-based service which monitors emails from supported providers for potential threats. By default, we don't store the emails, but we create and store non-personal numeric representations of the text to detect potential scam and other unwanted messages. You can allow us to store the whole email message (EML file with message metadata) we identified as suspected malicious by consenting to it in the product. This helps us keep better detections and improve the protection against scams. Our human reviewers may check the email message in case it is needed to investigate the accuracy of our detections (esp. in case of false negatives or false positives). Suspicious messages in the raw form are stored for 30 days and then we remove personal identifiers and keep them in our malware database. 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.
- Scam Protection works to warn you if you tap a dangerous link from any email, SMS, or messaging app by checking the URLs you visit.

**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 |

| | |
|---|---|
| | **Product and Business Improvement** (50 months)<br>● To monitor messaging performance |
| IP address | **Service Provision** (36 months)<br>● To detect the approximate location and source of malicious software - IP address is part of malware infection file |
| 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 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) |

| | |
|---|---|
| | **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) |

| | |
|---|---|
| | ● To improve the user's overall experience by developing new features and products (36 months) |
| Email Guard - Email | **Service Provision**<br>● In order to check your email and detect threats, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it except the non-personal numeric representation of it. (seconds)<br>● If you consent, we can store suspicious email messages for in-depth analysis and to keep our detection models up to date (30 days in raw form, 60 months in de-identified form) |
| Email Guard – malicious identifiers (URL, phone, email, crypto, or other identifier types that may be identified as significant for threat detection) | **Service provision** (60 months)<br>● We extract malicious identifiers from emails to maintain our threat detection models up to date |
| Email Guard - Snippets of email around detected phone numbers | **Service provision** (30 days)<br>● To detect malicious phone numbers, we analyse snippets of the message around detected phone numbers (few words before and after). These snippets are not connected to you. |
| Email Guard - Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |

| | |
|---|---|
| Email Guard - 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 Guard - 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<br>• IP addresses of mail servers (SMTP servers) | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance of detections<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |
| Email Shield - Detections<br>• email subject<br>• sender email address | **Service Provision** (1 month)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |

| | |
|---|---|
| • email content or attachment<br>• detection type and name | |

| **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** |

| | |
|---|---|
| | ● 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
- Singular

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) includes a comprehensive set of features that provide protection against potential online security and privacy threats, and features for optimizing device's performance.

## What are Product's Features

- **VPN** feature helps protect your online privacy by encrypting your online communication. The paid version of Avast One Premium allows you to pick a specific location to be connected from.
- **Web Shield** helps detect and notify you when accessing a malicious website that could represent a potential online security risk for you.
- **Photo Vault** locks your photos in an encrypted vault and helps secure 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 Guard** is a cloud-based service which monitors emails from supported providers for potential threats. By default, we don't store the emails, but we create and store non-personal numeric representations of the text to detect potential scam and other unwanted messages. You can allow us to store the whole email message (EML file with message metadata) we identified as suspected malicious by consenting to it in the product. This helps us keep better detections and improve the protection against scams. Our human reviewers may check the email message in case it is needed to investigate the accuracy of our detections (esp. in case of false negatives or false positives). Suspicious messages in the raw form are stored for 30 days and then we remove personal identifiers and keep them in our malware database. 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.

## 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 and source of malicious software - IP address is part of malware infection file |
| 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 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) |

| | |
|---|---|
| | ● 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) |

| | |
|---|---|
| | ● To improve the user's overall experience by developing new features and products (36 months) |
| Email Guard - Email | **Service Provision**<br>● In order to check your email and detect threats, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it except the non-personal numeric representation of it. (seconds)<br>● If you consent, we can store suspicious email messages for in-depth analysis and to keep our detection models up to date (30 days in raw form, 60 months in de-identified form) |
| Email Guard – malicious identifiers (URL, phone, email, crypto, or other identifier types that may be identified as significant for threat detection) | **Service provision** (60 months)<br>● We extract malicious identifiers from emails to maintain our threat detection models up to date |
| Email Guard - Snippets of email around detected phone numbers | **Service provision** (30 days)<br>● To detect malicious phone numbers, we analyse snippets of the message around detected phone numbers (few words before and after). These snippets are not connected to you. |
| Email Guard - Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guard - Subject of emails, MessageIDs of emails | **Service Provision** (4 weeks) |

| | |
|---|---|
| | ● To ensure proper functionality and fix bugs. Stored together with the user's email address |
| Email Guard - 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<br>• IP addresses of mail servers (SMTP servers) | **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 | **Service Provision** (1 month)<br>● For protection, detection, blocking, quarantining and deleting of malicious software |

| | |
|---|---|
| • email content or attachment<br><br>• detection type and name | |

| **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** |

| | |
|---|---|
| | ● 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
- Singular

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

## Avast One for Desktop (Windows, Mac)

### Official Product Name
Avast One, Avast One Free (collectively as "Avast One")

### Core Functionality
Avast One offers a comprehensive set of features that provide protection against potential online security and privacy threats, and features for optimizing device's performance. Concrete set of features available to you may differ based on the version of the product.

### What are Product's Features
- **Cybersecurity**

- **Smart Scan** is a comprehensive scan that helps detects browser threats, outdated applications, hidden viruses, system issues, online privacy threats and other issues depending on the provided features.
- **Protection features** provide core defenses for blocking malware and other threats including protection against malicious files, QR codes, suspicious applications, web attacks and unsafe downloads, unauthorized remote access attempts or dangerous email attachments. Based on the features available, we also provide protection for your browser data, passwords, sensitive documents, webcam, microphone or other assets against malware and unauthorized access. To do this, we scan files, programs, applications, attachments, URLs or other sources for potential threats. Sometimes, we may directly analyze suspicious files in our safe environment to make sure you are protected.
- **Network inspector** scans for vulnerabilities and potential security issues in your network (including for example router and connected devices).
- **Firewall** helps control what data goes in and out of your computer to block traffic from malicious sources and prevent unauthorized access to your device.
- **Sensitive data shield** checks your hard drive and looks for files that contain sensitive data. It helps secure your private data by controlling which applications and users have access to selected files.
- **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.
- **Scam Guardian and Assistant** features help block potentially dangerous websites and analyze texts, emails, messages or other media to avoid scams. It can also respond, if possible, to questions related to cybersecurity or our products.
- **Email Guard** (on the web) is a cloud-based service which monitors emails from supported providers for potential threats. By default, we don't store the emails, but we create and store non-personal numeric representations of the text to detect potential scam and other unwanted messages. You can allow us to store the whole email message (EML file with message metadata) we identified as

suspected malicious by consenting to it in the product. This helps us keep better detections and improve the protection against scams. Our human reviewers may check the email message in case it is needed to investigate the accuracy of our detections (esp. in case of false negatives or false positives). Suspicious messages in the raw form are stored for 30 days and then we remove personal identifiers and keep them in our malware database. 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.

- **Email Guard** (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.**Privacy features** provide an extra layer of protection for your online privacy. Based on the features available, it can include services such as VPN, dark web leak monitoring and tracking prevention. Dark web 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 features** help optimize your PC by removing duplicate or junk files, optimizing apps, or updating drivers and software.

- Selected versions of the product include Secure Identity features such as credit monitoring, transaction monitoring, social media monitoring, alerts to help you determine if your identity has been compromised and specialist support. These features are 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.

**Personal Data We Process**

While using Avast One, 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 and source of malicious software - IP address is part of malware infection file |
| Samples, files | **Service Provision** (36 months)<br>● For the functionality of malware scanning and analysis<br>● For protecting files containing sensitive information (not stored) |
| Detection metadata | **Service Provision** (36 months)<br>● For the functionality of malware scanning |

| | |
|---|---|
| Information concerning URLs of websites visited (malicious and non-malicious) and referrers (malicious URL information may also include search terms or cookie information associated with the malware) | **Service Provision** (36 months)<br>● For 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 Guard - Email | **Service Provision**<br>● In order to check your email and detect threats, we download it whole, together with metadata and attachments. We keep it in our systems only during the processing, we don't store it except the non-personal numeric representation of it. (seconds)<br>● If you consent, we can store suspicious email messages for in-depth analysis and to keep our detection models up to date (30 days in raw form, 60 months in de-identified form) |

| | |
|---|---|
| Email Guard – malicious identifiers (URL, phone, email, crypto, or other identifier types that may be identified as significant for threat detection) | **Service provision** (60 months)<br>● We extract malicious identifiers from emails to maintain our threat detection models up to date |
| Email Guard - Snippets of email around detected phone numbers | **Service provision** (30 days)<br>● To detect malicious phone numbers, we analyse snippets of the message around detected phone numbers (few words before and after). These snippets are not connected to you. |
| Email Guard - Hash of email address of sender | **Service Provision** (36 months)<br>● For the functionality of malware scanning<br>● To evaluate senders' reputation |
| Email Guard - 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 Guard - 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 | **Service Provision** (36 months)<br>● For the functionality of malware scanning and maintenance of detections<br>**Product and Business Improvement** (36 months)<br>● Threat statistics and internal analysis |

| | |
|---|---|
| • name of the attachments and their hashes<br>• country of the user<br>• IP addresses of mail servers (SMTP servers) | |
| Email Shield - 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 |
| Email Guard (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 |
| Scam protection – texts, images, emails, messages or other similar samples submitted for scam check | **Service Provision** (30 days)<br>For detecting scams, evaluating potential cybersecurity risks, and helping to assess risks involved in the submitted information. |

| | |
|---|---|
| Scam Assistant - user conversations, questions or anything you submit | **Service Provision** (30 days)<br>● For effective functioning and for the purpose of responding to the questions or other inputs<br><br>**Product and Business Improvement** (30 days)<br><br>For improving the quality of future conversations |
| Scam Assistant – samples and conversations with personal identifiers removed, detected malicious identifiers used in scam attempts (URLs, phone numbers, emails etc.) | **Service Provision**<br>● For effective detection of scams (as long as necessary to ensure effective protection but not stored in connection to users)<br><br>**Product and Business Improvement**<br><br>For improving the scam detection rate (as long as necessary to ensure effective protection but not stored in connection to users) |
| Scam Assistant - Reporting data based on metadata collected by product (limited to number of users by general geolocations/regions, and operating systems) | **Product and Business Improvement** (25 months)<br><br>For further developing and improving the product performance. |

| **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><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><br>**Product and Business Improvement**<br><br>● To better understand our users' behavior (50 months)<br><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><br>● To ensure functionalities of the product and its features<br><br>**In-product Messaging** (6 months)<br><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><br>**Product and Business Improvement**<br><br>● To better understand users' behavior (50 months)<br><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><br>● Delivering geo-specific changes to app's configuration (both local or remote)<br><br>**In-product Messaging** (6 months)<br><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) |

| | |
|---|---|
| | • 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.

# Online Security & Privacy

**Official Product Name**

Online Security & Privacy

**Core Functionality**

Online Security & Privacy is a browser extension (or plug-in). that helps check if the site isn't malicious or phishing.

**What are Product's Features**

- **Antivirus** checks the links in search results for potentially malicious webpages.
- **Anti-phishing** helps identify and block phishing sites trying to steal your data.
- **Anti-tracking** helps block tracking cookies that collect data on your browsing activities.
- **Marking Search Results** works to determine if the site is safe or not even before the user visits it.
- **Advertising Data Collection** helps opt out from ads based on user personal 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 settingsthat is designed to send websites a "GPC" signal

requesting to opt out of selling or sharing personal information on that website. See the specifics here.

- **Cookie Manager** works to automatically accept or decline 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, change settings, site blocked) | **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<br>**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) |

| | |
|---|---|
| | ● 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) |

# Password Manager

## Official Product Name

Avast Password Manager

## Core Functionality

Password Manager manages usernames, passwords, credit cards, user notes and other information useful for performing online activities. The information is stored in an encrypted storage. Password Manager will also send you 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.

The product consists of several components that differ by platform:

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

## Personal Data We Process

| Service data | What we use it for and for how long |
|---|---|
| Usernames, passwords, credit card information, notes, URLs connected with passwords stored by user (encrypted) | **Service Provision** (while the account is active)<br>• To ensure the functionality of the service |

| | |
|---|---|
| Events and product usage (app metadata, usage of features (such as data leak checks, number of accounts stored, error logs) | **Service Provision** (24 months)<br>• To encrypt data synchronization<br><br>**Product and Business Improvement** (39 months)<br>• For understanding product usage to further develop and improve the product performance as well as telemetry and 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 and internal identifiers | **Service Provision** (24 months)<br>• For users' support and troubleshooting<br><br>**Product and Business Improvement** (39 months)<br>• For development of new features or products |
| Information concerning computer or device (Operating System Version, Location data, (city/country), Avast Antivirus / Avast Passwords application Version, | **Service Provision** (24 months)<br>• For users' support and troubleshooting<br><br>**Product and Business Improvement** (39 months) |

| | |
|---|---|
| Browser Version, Extension Version) | • 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 |

The monitoring of potential passwords leaked online 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.

# 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** receives a notification if any of your stored passwords are found leaked online to help protect your identity. 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.
- **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. That means we cannot decrypt and read passwords, credit cards or notes.

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 |

| | |
|---|---|
| | **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 CouponFollow or 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 CouponFollow/NextGen Shopping (in accordance with their privacy policy) or 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 |

| | |
|---|---|
| | **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) |

| | |
|---|---|
| | • To make sure our offers are relevant, and collect statistics on SafePrice usage by language |

SafePrice does not process Account or Billing Data.

# Safe Search

## Official Product Name

Safe Search

## Core Functionality

Avast Safe Search is a browser extension which overrides the browser's default search engine to use Avast Safe Search. It comes bundled with Avast Home Page, which makes the Avast Safe Search web page your default home page when opening a new tab.

## What are Product's Features

- Safe Search provides website safety ratings to the User to provide a safer web browsing experience
- Home Page sets your home page to Avast Safe Search

## Personal Data We Process

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

| Service Data | What we use it for and for how long |
|---|---|
| URL | **Service Provision** (24 months)<br><br>To check if URLs in search results are malicious and to identify its source for threat analysis |
| Events and product usage (extension installation, disablement) | **Service Provision** (24 months)<br><br>To ensure functionality (installations, versions, updates, settings), map how users interact with the app and improve its design or flows |

| | |
|---|---|
| | **Product and Business Improvement** (24 months)<br><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><br>To distinguish unique malware hits and evaluate it in our systems<br><br>**Product and Business Improvement** (24 months)<br><br>To measure product telemetry and calculate statistics |
| Information on computer or device (hardware ID, browser, OS) | **Product and Business Improvement** (24 months)<br><br>To obtain usage statistics |
| Extension information (installation source and time, version and campaign ID) | **Product and Business Improvement** (24 months)<br><br>To obtain usage statistics, evaluate our messages and perform feature A/B testing |
| Location / Country | **Service Provision** (24 months)<br><br>To detect country specific malware campaigns<br><br>**Product and Business Improvement** (24 months)<br><br>To measure product telemetry and calculate statistics |

| | |
|---|---|
| Language | **Service Provision** (24 months)<br><br>To make sure we communicate in right language<br><br>**Product and Business Improvement** (24 months)<br><br>To measure product telemetry and calculate statistics |

# 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 cybersecurity 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.
- **WebShield** helps protect you from accessing dangerous websites, such as fake sites, phishing sites, sites that have harmful programs such as adware, spyware, ransomware, viruses, or other malware that aim at stealing your information. It includes https scanning that decrypts and scans encrypted traffic of selected websites to help detect potential malware contained on sites using https connections. All scanning occurs

locally on your PC during the HTTPS connection, and no one outside of your device can read or decipher the connection.

- **Phishing protection** helps detect potential new scam attempts by analyzing visited URLs and features related to website's visual appearance for suspicious indications (brand impersonation prediction and other phishing threats).
- **Privacy Cleaner** works to clean your browser history, cookies including 3rd party, cached images, and other tracking scripts to help ensure that your online activity is private as well as free up space on your device.
- **Privacy Guard** is a built-in extension that helps make your online experience cleaner, faster, safer, and more private. It comprises Adblocker (helps stop ads from loading), Anti-tracker (helps block tracking scripts and cookies), and Anti-Fingerprint (helps disguise your browser fingerprint to prevent websites from tracking you) features all in one. Privacy Guard collects and displays the number of blocked 3rd party calls from external sources.
- **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) creates an encrypted connection between your device and the internet, helping secure your browsing data. This VPN feature does not track or store connection timestamps, session information, bandwidth usage, traffic data, IP addresses, or other similar data.
- **Avast Addons Store** is an online store that allows you to view and install a wide range of extensions.
- **Extension Guard** is a built-in extension that helps protect against spammy, fake, or malware browser extensions.
- **Webcam Guard** helps protect against unauthorized access to your device camera.
- **Video Downloader** is an extension that allows you to convert and download videos from YouTube and other social media platforms.
- **HackCheck** – see the HackCheck section.
- **Accuweather widget** – used to display weather information on the new tab page based on the approximate location (derived from the IP address) and device model/OS.

- **Coupons** – used to track and offer coupon codes and deals from online merchants to help you save money. The service is powered by our partner NextGen Shopping, LLC.

## 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;
- Records of what you downloaded from websites;
- IP addresses are not stored, only used for product localization and analytics purposes based on approximate location (city/country level);
- Passwords and associated information within the Password Manager feature.

This data is not sent to our environment. You can manage this data within Secure Browser for Desktop in the Settings page.

However, if you enable the Sync feature, we will process relevant browsing 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** |
|---|---|
| Subset of URLs and referrers | **Service Provision** (36 months) |

| | |
|---|---|
| | • For the WebShield feature, a subset of URLs is processed in our backends for protection, detection, blocking, quarantining and deleting of malicious software or attacks. |
| 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 | **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 |

| | |
|---|---|
| | **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. If you disable the Sync feature, data is deleted within 3 months. |
| 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 |
| Basic information about your shopping cart (cart amount subtotal and total, discount value and applied promo code details) for websites on which you applied Coupons, including the merchant's domain. | **Service Provision** (36 months)<br>• This data is needed for the Coupons feature to work properly and offer coupon codes and deals from online merchants. |

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

| | |
|---|---|
| Online identifiers (GUIDs, Account ID, Device IDs) | **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 (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 (on a city/country level) | **Service Provision** (36 months) |

| | |
|---|---|
| | • 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) |
| 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)<br>**In-product Messaging** (6 months)<br>• To inform users about extension features and other available solutions<br>**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) |

| | |
|---|---|
| Our other products/licenses on the device and their status (e.g. our antivirus product) | **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 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 cybersecurity and privacy features, tools and settings, organized into one management console making it easier for you to control and manage your online privacy and cybersecurity.
- **Adblock** helps stop ads being shown in your browser using publicly available blocking lists..
- **Anti-Tracking** helps prevent the user from being tracked across websites by avoiding tracking cookies to be created. This is done using publicly available blocking lists.
- **Anti-Fingerprinting** helps prevent the user from being tracked across websites using browser fingerprinting techniques. As fingerprinting itself

cannot be prevented or avoided, this feature alters the digital fingerprint of the user's browser in a way that third-party sites should not be able to re-identify it.

- **Web Shield** helps protect you from accessing dangerous websites, such as fake sites, phishing sites, sites that have harmful content such as adware, spyware, ransomware, viruses, all types of other malware that aim at stealing your information.
- **Phishing protection** helps detect potential new scam attempts by analyzing URLs and features related to website's visual appearance for suspicious indications (brand impersonation prediction and other phishing threats). The information is only collected for URLs/webpages that exhibit characteristics suggestive of potential phishing threats.
- **Built-in VPN** (virtual private network) creates an encrypted tunnel between your device and the internet, making your browsing data safer.
- **Security Scanner** feature will scan the device, its internet connection and browser configuration for threats and vulnerabilities, process the findings, and display a result screen with potential improvements.
- **Nuke** works to clean your browser history, cached images, cookies including both first-party and third-party cookies, and other junk.
- **Remove Site Data** helps clean your browser history, site cookies, and offline data with the current site.
- **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, helps stop ads being shown in your browser, prevent your browsing history from being stored, and remove 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, helps stop ads being shown in your browser, prevent your browsing history from being stored, and remove any tracking cookies (both first-party cookies and third-party cookies) or web cache you pick up during that browsing session.
- **PIN Protection** helps secure your device by locking access to the browser application on your device with a unique code. Your PIN Code is encrypted on device 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.
- **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.
- Passwords and associated information within the Password Manager feature.

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 advanced identity protection. Depending on the region and product version, Secure Identity – may include features such as credit monitoring (only US), alerts to help you determine if your identity has been compromised and specialist support.

If you are located in the US, 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. If you are located outside the US, the following sections are applicable to you.

## What are Product's Main Features

- **Dark Web Monitoring** helps monitor the dark web and notify you if we find your information**.**
- **Social Media Monitoring** helps keep your social media accounts safer. We monitor your accounts on popular social media sites and notify you if we think your account may be compromised or if we find potentially risky links.
- **Restoration:** Identity Restoration Specialists are on-hand to evaluate your fraud claim, work with you and parties relevant to your case and advise on external services that can help resolve your claim.

- **Stolen Wallet Assist:** If your wallet is stolen, we'll provide you with guidance on how to cancel or replace credit cards, driver's licences, insurance cards and more.
- **Financial Monitoring:** Helps protect your finances against fraud with alerts that notify you of cash withdrawals, balance transfers and large purchases.
- **Identity Theft Insurance** helps with specific losses and expenses should you become a victim of identity theft.

## Personal Data We Process

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** |
|---|---|
| • Identity-related information incl. email, phone, address, credit card, bank account, gamertags, insurance ID, driver's license, mother's maiden name, passport, verbal passcode<br>• Social Media Platform username & password<br>• Financial transactions (last 4 of account number, FI name and transaction information), name, username & password | **Service Provision**<br>• To provide dark web monitoring services (credit card, bank accounts, mother's maiden name, driver's license, passport is deleted no later than 6 months after the termination of the service, other data no later than 36 months)<br>• To provide restoration, identity theft and stolen wallet services (name, address, email, phone) (84 months)<br>• To provide social media and financial monitoring services (username & password not stored, activity/transaction data - 6 months) |
| Events and product usage (applications error reports, crash dumps logs, app-related usage data) | **Product and Business Improvement (36 months)**<br>• To help us to further understand the usage and develop and improve the performance of our products |
| Internal online identifiers (user IDs) | **Service Provision (36 months)** |

| | |
|---|---|
| | • To deliver the service and ensure continuous functionality and breaking down entries in database |
| Information concerning computer or device (Device ID, Operating system version and settings, Device manufacturer and model, Device names and/or assigned names, Preferred language, Web browser name and version) | **Service Provision (36 months)**<br>• To deliver the service and ensure continuous functionality and breaking down entries in database<br><br>**Product and Business Improvement (36 months)**<br>• To help us to further understand the usage and develop and improve the performance of our products |

# SecureLine

Avast SecureLine VPN (collectively as “VPN”)

We are a leading provider of cybersecurity 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.