Products Policy

This Policy was last updated in August 2023.

Antivirus

Antivirus for Desktop (Mac and Windows)

Official Product Name

[AVG AntiVirus for Mac](), [AVG Internet Security for Mac](), [AVG Antivirus Free](), [AVG Internet Security]()

[AVG Internet Security Business Edition](), [AVG Antivirus Business Edition](), [AVG File Server Business Edition](), [AVG Email Server Business Edition](), [AVG Remote Administration]()

(collectively as "Antivirus for Desktop")

Core Functionality

The Antivirus for Desktop provides protection against malicious software by performing key tasks, such as pinpointing specific files for the detection of malwares, scheduling automatic scans, and securing your device against malware.

What are Product's Main Features

- **CommunityIQ** is a threat monitoring service for Windows and Mac which sends information about a threat detected in your device to our server, so we can observe how the threat spreads and block it. This is vital for the functioning of our Antivirus and our ability to keep your device secure.
- **CyberCapture** detects and analyses rare, suspicious files on your Windows. If you attempt to run such a file, CyberCapture locks the file from your PC and sends it to our Threat Lab where it is analysed in a safe, virtual environment. All files are uploaded over an encrypted connection, which means your data is inaccessible to hackers.
- **File Reputation** provides a real-time comparison with an up-to-date list of malware databases of executable files sourced from users of Windows who agree to participate in the service. FileRep processes files or their

hashed versions to evaluate which are infectious and updating virus databases.

- **Online Security** is a browser plug-in which needs to be specifically activated which checks if the site isn't malicious or phishing.
- **Browser Cleanup** is a module inside Antivirus for Desktop (Windows) which inspects the browser extensions of most browsers, tries to identify malicious extensions and offers to remove them. Browser Cleanup is on by default.
- **Web Shield** scans data that is transferred when you browse the internet in real-time to prevent malware from being downloaded and run on your computer. By default, Web Shield is on and configured to provide optimal protection when switched on.
- **File Shield** scans programs and files saved on devices for malicious threats in real time before allowing them to be opened, run, modified, or saved.
- **Email Shield** scans for threats in your incoming and outgoing email messages and attachments. Scanning applies only to messages sent or received using mail management software, such as Microsoft Outlook, Apple Mail or Mozilla Thunderbird.
- **Hack Alerts** when enabled, it searches and monitors email addresses associated with your Account for data breaches to alert you when your data has been compromised in a breach and your information is exposed on the dark web. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy [here](#).

Personal Data We Process

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

Service Data	What we use it for and for how long
Identifier of the content (message) being delivered	**Service Provision** (36 months) ● To monitor service functionality **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

	Product and Business Improvement (50 months) ● To monitor messaging performance
IP address	**Service Provision** (36 months) ● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country
Samples, files	**Service Provision** (36 months) ● For protection, detection, analysis, blocking, quarantining and deleting of malicious software
Detections	**Service Provision** (36 months) ● For protection, detection, blocking, quarantining and deleting of malicious software
URLs and referrers	**Service Provision** (36 months) ● For protection, detection, blocking, quarantining and deleting of malicious software
Events and product usage	**Service Provision** (36 months) ● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product **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 **Product and Business Improvement**

	● To better understand our users' behavior (50 months) ● To introduce a new feature or product based on previous experience (36 months)
Email Shield - Detections ● email subject ● sender email address ● email content or attachment ● detection type and name	**Service Provision** (1 month) ● For protection, detection, blocking, quarantining and deleting of malicious software

Device Data	What we use it for and for how long
Internal online identifiers (GUID, Device ID)	**Service Provision** (36 months) ● For ensuring continuous functionality and breaking down entries in database **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 **Product and Business Improvement** ● To better understand our users' behavior (50 months) ● To introduce a new feature or product based on previous experience (36 months)
Information concerning computer or device	**Service Provision** (36 months) ● To check for compatibility issues in automated crash dumps **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 **Product and Business Improvement** ● To better understand users' behavior (50 months)

	● To introduce a new feature or product based on previous experience (36 months)
Location	**Service Provision** (36 months) ● To set up a proper product language version for Windows **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 **Product and Business Improvement** ● To better understand users' behavior based on approximate location (50 months) ● To introduce a new feature or product based on approximate location (36 months)
Applications - other security SW / antiviruses present	**Service Provision** (36 months) ● 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) ● 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) **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 **Product and Business Improvement** (up to 36 months) ● To improve the users' overall experience by developing new features and products ● To understand/estimate market opportunity

Our other products/licenses on the device and their status	**Service Provision** (36 months) ● To recognize what features should be enabled or disabled, what product should be installed or uninstalled **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 **Product and Business Improvement** (up to 36 months) ● To improve the users' overall experience by developing new features and products ● To understand/estimate market opportunity
Internet and connection / Network data / Number of devices on Network	**Service Provision** (36 months) ● For security prerequisites (e.g. DNS settings check, port restrictions enabling or disabling Security status check of devices on the network) **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 **Product and Business Improvement** (36 months) ● To introduce a new feature or product based on previous experience
Browsers (installed, default)	**Service Provision** (36 months) ● For opening content in given browser **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 **Product and Business Improvement** ● 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.

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

[AVG AntiVirus Free for Android](), [AVG AntiVirus Pro for Android]() (collectively as "Antivirus for Mobile (Android)")

Core Functionality

Antivirus for Mobile (Android) provides people with essential mobile security with added privacy. Block malware, check the safety of installed apps, scan public Wi-Fi networks for possible security weaknesses — all with a single app.

What are Product's Main Features

- **Device Scan** scans your device or a specific file for malware apps and files and various types of security vulnerabilities.
- **Wi-Fi Security and Speed Check** enables you to scan your network for vulnerabilities, and tests the speed of the network.
- **Web Shield** detects and notifies you when accessing a malicious website that could represent a potential security risk for you.
- **App Locking** is a paid feature, which protects your sensitive apps with a PIN, pattern, or fingerprint.
- **App Insights** consists of three features: App Usage, Data Usage and App Permissions. App Insights requires your device user permission in order to work and we ask you for this permission (if not granted yet). When you grant the permission, we keep the data from your list of installed apps stored locally in your phone's database. App Usage provides information about how much time you spend using each app.

App Permissions allows you to view which permissions are required by each of your installed apps. Data Usage monitors your data consumption and helps you avoid additional charges by notifying you when you approach the limit. This feature requires access to IMEI and IMSI.

- **Clean Junk** analyzes the space on your device and displays the amount of storage space that is being used by junk files.
- **Photo Vault** allows you to protect access to your photos with a PIN code.
- **Hack Alerts** when enabled, it searches and monitors email addresses associated with your Account for data breaches to alert you when your data has been compromised in a breach and your information is exposed on the dark web. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.
- **Privacy Audit** provides the user with an evaluation of installed apps based on data collected and permissions asked by the app compared to similar apps. The feature also compares its findings with the app's privacy policy declarations.
- **VPN** feature protects your privacy by encrypting your online communication so no one can spy on what you're doing online. It allows you to pick a specific location to be connected from.
- **Scam Protection** warns you if you tap a dangerous link from any email, SMS, or messaging app.

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) ● To monitor service functionality **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 **Product and Business Improvement** (50 months) ● To monitor messaging performance

IP address	**Service Provision** (36 months) ● To detect the approximate location of malicious software. For free Antivirus, IP address is replaced at activation with city/country. For free and paid Antivirus, it is a part of malware infection file replaced in 30 days with city/country
Samples, files	**Service Provision** (36 months) ● For the functionality of malware scanning and analysis
Detections	**Service Provision** (36 months) ● 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) ● For Web Shield feature's detection of malicious websites
Events and product usage	**Service Provision** (36 months) ● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product **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 ● Contextual promotional messaging **Product and Business Improvement** ● 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)

User's email address associated with your Account	**Service Provision (36 months)** ● To search for your credentials in data breaches. ● To send a requested report to you on whether or not their credentials have leaked. **Product and Business Improvement** (36 months) ● To improve the user's overall experience

Device Data	What we use it for and for how long
Online identifiers (GUID, Device ID (Android ID), Advertising ID)	**Service Provision** (36 months) ● To ensure functionalities of the product and its features **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 **Product and Business Improvement** ● To better understand our users' behavior (50 months) ● To recognize reinstalls of the app on the same device (36 months) **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) ● To ensure functionalities of the product and its features **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 **Product and Business Improvement**

	● To better understand users' behavior (50 months) ● To improve the user's overall experience by developing new features and products (36 months)
Location (city/country, longitude and latitude)	**Service Provision** (36 months) ● Delivering geo-specific changes to app's configuration (both local or remote) **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 **Product and Business Improvement** ● To better understand users' behavior based on approximate location (50 months) ● To introduce a new feature or product based on approximate location (36 months)
IMSI	**Service Provision** (accessed only locally) ● For App Insights's feature Data Usage to provide data consumption of installed apps based on IMSI
Applications	**Service Provision** (36 months) ● To define rules for malware protection how Antivirus should behave **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
Internet and connection	**Service Provision** (36 months) ● For security prerequisites **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 **Product and Business Improvement** ● To better understand users' behavior (50 months) ● To introduce a new feature or product based on previous experience (36 months)

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

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

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

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

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

AVG Mobile Security

Core Functionality

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

- **Web Shield** detects and notifies you when accessing a malicious website that could represent a potential security risk for you.
- **Hack Alerts** looks for leaked personal information, whether your data has been compromised in a breach and your information is exposed on the dark web. If we identify new breaches we alert you based on the email address you submitted. This is done in cooperation with our partner SpyCloud which checks your credentials against its repository of stolen accounts. For further information please refer to its privacy policy here.
- **Photo Vault** locks your photos in an encrypted vault and secure them with a PIN, Touch ID, or Face ID so that only you have access to them.
- **Wi-Fi Security** automatically scans Wi-Fi networks for vulnerabilities to verify that the network you're connected to is safe. Receive alerts if any risk is detected.
- **Secure Browsing** (available only for paid version) protects your privacy by making sure no one can spy on what you're doing online with Secure Browsing VPN feature.
- **Email Guardian** is a cloud-based service which monitors emails from supported providers, scans when they arrive in your inbox and flags them as malicious if they contain a threat. In order to deliver its functionality and allow us to improve our products and business, this feature processes personal data, such as e-mail and its content, including attachments. When enabled, it provides protection to your device even when the device is switched off. Connecting this feature to Gmail accounts requires us to ask Google for permission to use its APIs. Google allows companies to use its APIs only if they undertake to limit its use of information accessed through the APIs. As a result, the use and transfer of information received from these Google APIs to any other product will adhere to Google API Services User Data Policy, including the Limited Use requirements.

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

Service Data	What we use it for and for how long
Information concerning URLs of websites visited (malicious and non-malicious) and referrers (previous page with link to malware-hosting site)	**Service Provision** (36 months) ● For Web Shield feature's detection of malicious websites
Timestamps of your connections for Secure Browsing	**Service Provision** (36 months) ● To manage the number of concurrent active connections, and handle abuse **Product and Business Improvement** (36 months) ● To improve the user's overall experience
The subnet of your originating IP address for Secure Browsing	**Service Provision** (36 months) ● To plan for increased network demand and capacity
IP address of the VPN server you're using for Secure Browsing	**Service Provision** (36 months) ● To troubleshoot our service and plan for new network capacity
Amount of data transmitted for Secure Browsing E.G. 5GB up or down	**Service Provision** (36 months) ● To plan for new network capacity and server improvements **Product and Business Improvement** (36 months) ● To improve the user's overall experience
User's email for Hack alerts	**Service Provision** (36 months) ● To send a requested report to you on whether or not their credentials have leaked **Product and Business Improvement** (36 months) ● 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) ● To ensure continuous functionality (installations, versions, updates, settings) **Product and Business Improvement** ● To understand the user's behavior (14 months) ● To improve the user's overall experience (36 months)
Email Guardian - Email	**Service Provision (seconds)** ● In order to check your email, we download the whole email message, including metadata and attachments. We keep it in our systems only during the processing, we don't store it
Email Guardian - Hash of email address of sender	**Service Provision (36 months)** ● To provide the functionality of malware scanning **Product and Business Improvement (36 months)** ● To evaluate senders' reputation
Email Guardian - Subject of emails, MessageIDs of emails	**Service Provision (4 weeks)** ● To be able to track users' support requests related to particular emails. Stored together with the user's email address
Email Guardian - Detections ● hash of the email ● hash of the userID ● payment card-stripped email subject ● hash of sender email address ● domain address of sender ● detection type and name	**Service Provision (36 months)** ● To provide the functionality of malware scanning and to do maintenance **Product and Business Improvement (36 months)** ● To do threat statistics and internal analysis

● payment card-stripped name of the attachments and their hashes ● country of the user	

Device Data	What we use it for and for how long
OS Version E.g. iOS 13.1	**Service Provision** (36 months) ● For user support and troubleshooting **Product and Business Improvement** ● To understand the user's behavior and product development planning (14 months) ● To improve the user's overall experience (36 months)
Mobile Security for iOS version E.G. Mobile Security for iOS version 1.2.2	**Service Provision** (36 months) ● For user support and troubleshooting **Product and Business Improvement** ● To understand the user's behavior and product development planning (14 months) ● To improve the user's overall experience (36 months)

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

- Google Firebase Analytics and Crashlytics for iOS
- AppsFlyer

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

AntiTrack

Official Product Name

AVG AntiTrack for Windows, AVG AntiTrack for Mac, (collectively as "AntiTrack")

As you browse the web, cookies and digital fingerprint-based tracking technologies collect and link information about your activities in order to create profiles of your behavior . This data is then shared, bought and sold by analytics and ad-tech firms. AntiTrack removes cookies and masks the device's "fingerprint" to prevent third- parties from identifying you and following your behavior across the web.

What are the Product's Features

- **AntiFingerprinting** stops scripts from fingerprinting the user's device and tracking their browsing behavior across the web. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale and AntiTrack version.
- **Privacy Score** provides the user with an evaluation of how private they are based on various in-app configurations. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale, AntiTrack version, In-app settings (such as features that are turned on/off).
- **Fingerprint Randomizer** will automatically change the user's digital 'Fingerprint' in regular intervals, or allow the user to manually change said 'Fingerprint'. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale and AntiTrack version.
- **Browser cleanup** helps the user manage browsing history and cookies by allowing the user to manually clear this information or schedule an automatic deletion at a specific time. In particular, this feature relies on processing of browser version, hardware data, Cookies, OS version, OS locale, AntiTrack version, In-app settings (such as features that are turned on or off).
- **Browser protection** helps users stay protected from online tracking attempts and similar threats through supported browsers. Any time a suspicious script (tracking attempt) encounters the user's 'Fingerprint', the user is notified. In particular, this feature relies on processing of browser version, hardware data, OS version, OS locale, website scripts and tracking elements, and AntiTrack version.
- **Allowed Websites and whitelisting processes** allows the user to add their favorite websites into the Allowed Websites list so that their stored browser data is not be cleared during the automatic and manual cookie

clearing process. Additionally, no anti-tracking measures will be active on these websites once they are added to the Allowed Websites list. In particular, this feature relies on processing of whitelisted websites, browser version, hardware data, OS version, OS locale and AntiTrack version.

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

Personal Data We Process

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

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

Browser information (including information about extensions)	**Service Provision** (the earlier lifetime of the account and 24 months)
	• To show Browser Protection and Cookie Cleanup status in the product, and identify the default browser for opening the links from the app.
	• To check the browser extension status (only in supported browsers).
	• When Browser Protection feature from the product is ON, for AntiTrack to obfuscate the following properties of the browser under Anti-Fingerprinting:
	  ○ User-Agent
	  ○ Plugins
	  ○ HTTP Headers

Cookies	**Service Provision** (the earlier lifetime of the account and 24 months) • To identify the "Total (number of) Cookies, and Tracking Cookies" available for a browser • To perform the cookie cleanup (delete the cookies, cache, and browser history).
Whitelisted websites	**Service Provision** (the earlier lifetime of the account and 24 months) • To add websites into the Allowed Websites list
Website Tracker Details (Javascript, HTML documents)	**Service Provision** (the earlier lifetime of the account and 24 months) • To identify website trackers on the website that the user is visiting and determine if the Javascript/Html is a tracker or not. **In-product messaging** (6 months) • To update the user about tracking.

AntiTrack version	**Service Provision** (the earlier lifetime of the account and 24 months)
	  ● To provide user support, troubleshoot
	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
	Product and Business Improvement (24 months)
	  ● To better understand how users' interact with certain aspects

Install Date or Time	**Service Provision** (the earlier lifetime of the account and 24 months)
	  ● To do license management
	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
	Product and Business Improvement (24 months)
	  ● To know when to market new features and or products

Crash Incidents	**Service Provision** (the earlier lifetime of the account and 24 months) ● To ensure continuous functionality

Device Data	What we use it for and for how long

OS information (version, keys, tasks)	**Service Provision** (the earlier lifetime of the account and 24 months)
	  ● To provide user support, troubleshoot
	Product and Business Improvement
	  ● When developing new features - to adjust the scope of the feature based upon the requirements and the functionality of certain operating systems (24 months)
	  ● To better understand how users' interact with certain aspects 24 months)

OS Locale	**Service Provision** (the earlier lifetime of the account and 24 months) - To segment updates by location **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 **Product and Business Improvement** (24 months) - To determine which segments of our users to roll out a new feature or product - To better understand how users' interact with certain aspects
Hardware Data (device model, RAM, GPU, CPU)	**Service Provision** (the earlier lifetime of the account and 24 months) - To install the product, provide application updates, customer support **Product and Business Improvement** (24 months) - To better understand how users' interact with certain aspects

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

Alarm Clock

Official Product Name

[Alarm Clock Xtreme]()

Core Functionality

Alarm Clock provides an alarm clock for Android devices, using built in system features users can schedule alarms and customize their behavior in many ways.

- **Alarm Clock** schedules a one time alarm or repeated alarms, customize sound and other behavior while alarms go off and set many other parameters. This feature does not require any special permission, except when a user wants to use a local sound file for their alarms, the app asks to access device storage.
- **Timer** schedules timers that would go off after desired time is passed. On the technical level timers are just different method of scheduling alarms
- **Reminders** are a different method of scheduling alarms tailored towards use cases when one needs to remind themselves about something. Unlike regular alarms, reminders can be set with a specific date in the future and the way they go off is more subtle than alarms that are designed to wake users up.
- **Stopwatch** can measure elapsed time. Stopwatch does not need any special permission to function.
- **My Day** is a feature that can be optionally brought to the foreground after an alarm is dismissed. My Day is designed to provide useful information to users in the morning. My Day shows weather forecasts and it can be optionally more precise if the user provides permission to determine location from device. My Day also optionally provides information about upcoming events if users agree to access their device calendar.

Personal Data We Process

While using Alarm Clock, 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) ● To monitor service functionality **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 **Product and Business Improvement** (14 months) ● To monitor messaging performance

IP address	**Service Provision** (36 months) ● Replaced with city/country for delivering geo-specific changes to app's configuration (both local or remote) **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 **Product and Business Improvement** (14 months) ● To monitor messaging performance
Events and product usage	**Service Provision** (36 months) ● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product **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 **Product and Business Improvement** ● 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** (up to 36 months) ● To identify correct installation **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 **Product and Business Improvement**

	● To better understand our users' behavior (14 months) ● To recognize reinstalls of the app on the same device (36 months) **Third-party Ads** (not stored after provision) ● We process Advertising ID which allows ad placement
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) ● To ensure functionalities of the product and its features. For example to inform users about settings that make alarm scheduling more reliable on specific devices. **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 **Product and Business Improvement** ● To better understand our users' behavior (14 months) ● 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) ● Delivering geo-specific changes to app's configuration (both local or remote) ● Related to My Day feature which can show weather forecasts **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 **Product and Business Improvement** ● To better understand users' behavior based on approximate location (14 months) ● To introduce a new feature or product based on approximate location (36 months)

Calendar Events	**Service provision** (36 months) ● To provide an overview of upcoming events on My Day Screen. Specific content of users calendar is only processed locally on user device and never stored anywhere. **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 **Product and Business Improvement** (14 months) ● To better understand users' behavior
Internet and connection	**Service provision** (36 months) ● For functionality of our features, providing error messaging **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 **Product and Business Improvement** ● To better understand users' behavior (14 months) ● To introduce a new feature or product based on previous experience (36 months)

These are the third-party analytics tools we use for Cleaner for Android:

● Google Firebase Analytics and Crashlytics for Android
● AppsFlyer

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

The ad-supported version of Alarm Clock serves relevant third-party advertisements. These are the advertising partners we use for this product:

● Google AdMob
● Facebook Audience Network
● InMobi

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

Battery Saver

Official Product Name

[AVG 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) ● To monitor service functionality **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

	Product and Business Improvement
	● To better understand our users' behavior (12 months)
	● 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) ● To monitor service functionality **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) ● To check for compatibility issues in automated crash dumps **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 **Product and Business Improvement** (12 months) ● To better understand users' behavior

	● 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) ● To set up a proper product language version for Windows **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 **Product and Business Improvement** (12 months) ● To better understand users' behavior based on approximate location ● 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) ● To recognize what features should be enabled or disabled, what product should be installed or uninstalled **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

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

BreachGuard

Official Product Name

[BreachGuard](#)

Core Functionality

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

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

What are Product's Features

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

out forms require some of, if not all of the information to submit a valid opt-out request and verify that you are in fact in their database. As a result, we collect this basic information from you to submit the opt-out requests on your behalf.

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

Personal Data We Process

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

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

This data is not sent to our environment.

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

Service Data	What we use it for and for how long
	●
Browsing history and bookmarks (only domain name)	**Service Provision** (6 months) ● To display relevant privacy guides

	Product and Business Improvement (6 months)
	● For development of new features or products
	●
Events and product usage (app metadata, page views, clicks, installs, Number of Application Launches, updates, error logs and screen flow)	**Service Provision** (24 months) ● To improve user experience and application performance **Product and Business Improvement** (39 months) ● 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 E.g. Windows 10, BreachGuard v1.2.0	**Service Provision** (24 months) ● For users' support and troubleshooting **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 **Product and Business Improvement** (39 months) ● For development of new features or products ● To understand the users' behavior and product development planning
OS Locale	**Service Provision** (24 months) ● For users' support and troubleshooting as well as rendering the data broker removal service **Product and Business Improvement** (39 months) ● For development of new features or products
Hardware Data	**Service Provision** (24 months)

e.g. Device Model (e.g. Windows 10 (13-inch 2017), RAM (Random Access Memory), GPU (Graphical Processing Unit), and Central Processing Unit (CPU)	● For users' support and troubleshooting **Product and Business Improvement** (39 months) ● For development of new features or products

Cleaner

Official Product Name

AVG Cleaner for Android ("Cleaner for Android")

Core Functionality

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

What are Product's Features

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

While using Cleaner for 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) ● To monitor service functionality **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 **Product and Business Improvement** (14 months) ● To monitor messaging performance
IP address	**Service Provision** (36 months) ● Replaced with city/country for delivering geo-specific changes to app's configuration (both local or remote) **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 **Product and Business Improvement** ● To monitor messaging performance (14 months)
Events and product usage	**Service Provision** (36 months) ● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product **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 **Product and Business Improvement** ● 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) ● For counting users, ensuring functionality and stability **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 **Product and Business Improvement** ● To better understand our users' behavior (14 months) ● To recognize reinstalls of the app on the same device (39 months) **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) ● To ensure functionalities of the product and its features **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 **Product and Business Improvement** ● To better understand our users' behavior (14 months) ● 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) ● Delivering geo-specific changes to app's configuration (both local or remote)

	● Related to Battery Profile feature, as users can set being in a certain location as a trigger to automatically launch a Battery saving profile. **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 **Product and Business Improvement** ● To better understand users' behavior based on approximate location (14 months) ● To introduce a new feature or product based on approximate location (36 months)
Applications	**Service provision** (36 months) ● 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 **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 **Product and Business Improvement** (14 months) ● To better understand users' behavior
Internet and connection	**Service provision** (36 months) ● For functionality of our features, providing error messaging **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 **Product and Business Improvement** ● To better understand users' behavior (14 months)

	• To introduce a new feature or product based on previous experience (36 months)

These are the third-party analytics tools we use for Cleaner for Android:

- Google Firebase Analytics and Crashlytics for Android
- AppsFlyer

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

The free version of Cleaner for 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

[AVG Driver Updater](#)

Core Functionality

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

Personal Data We Process

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

Service Data	What we use it for and for how long
Identifier of the content (message) being delivered	**Service Provision** (12 months) ● To monitor service functionality **In-product Messaging** (126 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 **Product and Business Improvement** (12 months) ● To monitor messaging performance
Events and product usage	**Service Provision** (12 months) ● To ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product **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 **Product and Business Improvement** (12 months) ● To better understand our users' behavior ● 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) ● For ensuring continuous functionality and breaking down entries in database **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 **Product and Business Improvement** (12 months) ● To better understand our users' behavior ● To introduce a new feature or product based on previous experience
Information concerning device (type, vendor, model, manufacturer, version)	**Service Provision** (12 months) ● To check for compatibility issues in automated crash dumps **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 **Product and Business Improvement** (12 months) ● To better understand users' behavior ● To introduce a new feature or product based on previous experience
Information concerning drivers (driver version, updated date, name, matching device id, driver rank, driver flags)	**Service Provision** (12 months) ● To monitor service functionality **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 **Product and Business Improvement** (12 months) ● To better understand our users' behavior ● 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) ● To set up a proper product language version for Windows **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 **Product and Business Improvement** (12 months) ● To better understand users' behavior based on approximate location ● 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) ● To recognize what features should be enabled or disabled, what product should be installed or uninstalled **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

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.

Management Console

Official Product Name
AVG Cloud Management Console

Core Functionality

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

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

- **Monitor Device Security** uses the console to monitor the health of all managed devices from one place, reviews the number of blocked threats, schedules regular scans, and more.
- **Management Dashboard** activates devices, adds devices to groups, configures antivirus settings, and views blocked threats from an easy-to-read dashboard.
- **Master Agent** selects a device as the Local Update Server where all updates can be downloaded and saves bandwidth by scheduling and distributing updates to all endpoints in your network when it's convenient.
- **Tasks** sets up security tasks for all managed endpoints, such as scans, messages, updates, and shutdowns to ensure optimal security for the entire network.
- **Updates** remotely downloads and distributes virus and program updates to all devices from one console to save time and bandwidth.
- **Notifications** receives instant email notifications on any security threats or network issues that need your attention, including outdated antivirus applications, extended device inactivity, and additional device update.
- **Reporting** views detailed reports that include blocked threats, task lists, and protected devices, making it simple to improve security and customize protection.
- **Subscriptions Overview** lists all valid subscriptions and licenses.
- **Network Discovery** scans your network for connected devices to bring visibility over what devices should be taken care of.
- **Cloud Backup** securely stores selected data in the cloud as backup in case of data loss or disaster resulting in data loss/damage.
- Remote Control enables IT admins to quickly and securely connect to a user's device, access files and applications, and help troubleshoot issues in real time.
- **Patch Management** - scans for missing operating system updates and third-party application patches and enables remote installation of those patches to resolve application vulnerabilities of endpoints.
- **Content Filtering** boosts productivity and security by controlling your employees' internet usage and allowing to restrict their access to specific sites.
- **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.

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** ● For ensuring continuous functionality and breaking down entries in database **Product and Business Improvement** ● To better understand our users' behavior ● 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 Provisioning** - To better identify and manage devices detected on the network - To determine whether it supports installation of Avast services
Information concerning computer or device (OS build, display)	**Service Provision** ● To check for compatibility issues in automated crash and agent log dumps **Product and Business Improvement** ● To better understand users' behavior ● To introduce a new feature or product based on previous experience
Applications	**Service Provision** ● To determine which application needs to be updated, to provide support and troubleshooting
Files, content	**Service Provision** ● To provide cloud backup, email archive
Internet and connection / Network data / Number of devices on Network	**Service Provision** ● For security prerequisites (e.g. DNS settings check, port restrictions enabling or remote deployment) **Product and Business Improvement**

	∉ To introduce a new feature or product based on previous experience
Location, IP and MAC addresses	**Service Provision** ● For admins to have a possibility to localize their devices
Device status (last connection to Avast)	**Service Provision** ● For admins to see which devices were active and when and determine the risk profile
Location	**Service Provision** ● To set up a proper product language version **In-product Messaging** ● 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** ● To better understand users' behavior based on approximate location ● To introduce a new feature or product based on approximate location
Language, time zon0065	**Service Provision** ● To set the right language settings **In-product Messaging** ● To send campaigns localized based on users' language

Service Data	What we use it for
Identifier of the content (message) being delivered	**Service Provision** ● 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** ● For protection, detection and blocking of malicious or restricted content
Our other products/licenses on the device and their status	**Service Provision** ● For administrators to have an overview of running services and expiration dates
Events and product usage	**Service Provision** ● To provide reporting capability for admins and to ensure continuous functionality (installations, versions, updates, settings) and map how users interact with our product **In-product Messaging** ● 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** ● To better understand our users' behavior ● To introduce a new feature or product based on previous experience
Audit Logs	**Service Provision** ● To provide record of changes in application and endpoints

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

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

Company Data	What we use it for
Name, business, finance and tax details and contact information	**Service Provision** ● To provide support and to contact the company when needed ● To process product purchases ● To renew & license products
Business type	**Service Provision** ● 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 Business Management Console is Google Analytics, Hotjar, Medallia. For further information regarding our third-party analytics partner, including its privacy policy, please refer to our Privacy Policy.

Online Security & Privacy

Official Product Name

[Online Security](#) **& Privacy**

Core Functionality

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

What are Product's Features

- **Antivirus** checks the links in search results so the user knows if the page is trying to spread malware.
- **Anti-phishing** identifies and blocks phishing sites trying to steal your data.
- **Anti-tracking** blocks annoying tracking cookies that collect data on your browsing activities.
-
- **Marking Search Results** shows if the site is safe or not even before the user visits it.
- **Advertising Data Collection** opts out from ads based on user personal interests. By opting out of interest-based advertising it means the company or companies from which you opt out will no longer show ads that have been tailored to your interests.
- **Privacy Advisor** allows optimizing privacy settings on the most popular online platforms via step-by-step guidance.
- **Global Privacy Contro**l is a [3rd party solution](#) we have implemented in the settings, the user can send web companies he visits a 'GPC' signal that he wants to opt out of website selling or sharing his personal information

Personal Data We Process

While using Online Security & Privacy, we process the following Service and Device Data:

Service Data	What we use it for and for how long

URL	**Service Provision** (24 months) ● To check if URLs and the preceding referral domains or URLs (as applicable) are malicious or not to identify its source for threat analysis
Usage data (open extension, rated site, disabled trackers, change settings, site blocked)	**Service Provision** (24 months) ● 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) ● 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) ● To distinguish unique malware hits and evaluate it in our systems **Product and Business Improvement** (24 months) ● To measure product telemetry and calculate statistics
Information on computer or device (browser, OS)	**Product and Business Improvement** (24 months) ● To obtain usage statistics
Extension information (installation source and time, version and campaign ID)	**Product and Business Improvement** (24 months) ● To obtain usage statistics, evaluate our messages and perform feature A/B testing
Location / Country	**Service Provision** (24 months) ● To detect country specific malware campaigns **Product and Business Improvement** (24 months) ● To measure product telemetry and calculate statistics
Language	**Service Provision** (24 months) ● To make sure we communicate in right language

	Product and Business Improvement (24 months) ● To measure product telemetry and calculate statistics
Antivirus Status	**Service Provision** (24 months) ● To being able to turn on Bank Mode which works only when Antivirus is installed and offers to user to open page in a safe sandbox environment on sensitive sites (banking)

Online Security & Privacy does not process Account or Billing Data.

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

SafePrice

Official Product Name

AVG SafePrice

Core Functionality

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

What are Product's Features

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

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

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

Personal Data We Process

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

Service Data	What we use it for and for how long
URL and referrers	**Service Provision** (36 months) ● To display discount coupons and price comparison offers relevant to the website that you are visiting
Search query	**Service Provision** (36 months) ● If submitted by you, to search for relevant products and discount coupons
Product name and price	**Service Provision** (36 months) ● To display price comparison offers relevant to the product that you are shopping for
User's feedback (ratings, comments)	**Service Provision** (36 months) ● To tell whether the offers you received are relevant and up-to-date, and collect product feedback **Product and Business Improvement** (36 months) ● 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) ● For ensuring continuous functionality and breaking down entries in database **Product and Business Improvement** (36 months) ● To measure product telemetry and calculate statistics

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

Secure Browser
Secure Browser for Desktop

Official Product Name

AVG Secure Browser ("Secure Browser for Desktop")

Core Functionality

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

What are Product's Features
- **Browser Security & Privacy Center** is built in Security & Privacy Center which is a curated collection of some key security and privacy features, tools and settings, organized into one management console making it easier for you to control and manage your online privacy and security.

- **WebShield** protects you from accessing dangerous websites, such as fake sites, sites that have harmful programs such as adware, spyware, ransomware, viruses, all types of other malware that aim at stealing your information. It includes https scanning that decrypts and scans encrypted traffic of selected websites to 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.
- **Privacy Cleaner** cleans all your browser history, all cookies including 3rd party, cached images, and other tracking scripts with just one click, to ensure that your online activity is private as well as free up space on your device.
- **Privacy Guard** is a built-in extension that helps make your online experience cleaner, faster, safer, and more private. It comprises Adblocker (stops ads from loading), Anti-tracker (blocks tracking scripts and cookies), and Anti-Fingerprint (disguises your browser fingerprint to help 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) that creates an encrypted connection between your device and the internet, securing your browsing data against eavesdroppers, trackers, and hackers. This VPN feature does not track or store connection timestamps, session information, bandwidth usage, traffic data, IP addresses, or other similar data. Using a VPN helps keep you more private and secure but you are still accountable for everything you do online.
- **Avast Addons Store** is an online store created and maintained by Avast that allows you to view and install a wide range of extensions. On installation of each extension, you will be asked what data you can share with the extension. Extensions are addons that are built to extend the functionality of the browser itself or integrate an existing service with the browser.
- **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.
- **CouponFollow extension** (only for US-based users) – 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 and in accordance with their [privacy policy](#). In order to provide this service, the extension may analyze and collect certain information related to your browsing activities, specifically the webpages you visit and device information to determine which coupons to show you. The extension may also process coupon and shopping cart related data (e.g., if and how you used a coupon, cart amounts, discount value) and information regarding any technical issues encountered by the extension. For more information, please refer to NextGen Shopping's [privacy policy](#).

Personal Data We Process

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

- Browsing history information; for example Secure Browser for Desktop may store the URLs of pages that you visit, a cache of text, images and other resources from those pages. If the pre-rendering feature is turned on, a list of IP addresses linked to those pages may also be stored for some period of time;
- Name, surname, email or passwords to help you fill out forms or signs in to sites you visit;
- Permission that you have granted to websites;
- Cookies or data from websites that you visit;
- Data saved by add-ons;
- Record of what you downloaded from websites;
- IP addresses are not stored, only used for product localization and analytics purposes based on approximate location (city/country level);

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) - To ensure functionality (installations, versions, updates, settings), map how users interact with the application and improve its design or flows **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 **Product and Business Improvement** - To better understand our users' behavior (up to 60 months)

	• 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) • To improve the product or its feature based on the user's feedback
User's feedback comments	**Service Provision** (36 months) • To ensure functionality and prevent crashes based on the user's feedback **Product and Business Improvement** (36 months) • 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) • 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) • 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 **Product and Business Improvement** (36 months) • If you enable the VPN feature, for product improvements, and

	development planning as we aim at developing best-in-class products

Device Data	**What we use it for and for how long**
Online identifiers (GUIDs, Account ID, Device IDs)	**Service Provision** (36 months) • For ensuring continuous functionality and breaking down entries in database **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 **Product and Business Improvement** • To better understand our users' behavior (60 months) • To introduce a new feature or product based on previous experience (36 months)
Information concerning computer or device	**Service Provision** (36 months) • To check for compatibility issues in automated crash dumps **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 **Product and Business Improvement**

	• To better understand users' behavior (60 months) • 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 **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 **Product and Business Improvement** • To better understand users' behavior (50 months) • To introduce a new feature or product based on country (36 months)
Extensions installed in the browser	**Service Provision** (36 months) • To define rules of how the Browser should behave in relation to extensions installed (e.g. exceptions in scanning, filtering, notifications, whitelisting, blacklisting) **In-product Messaging** (6 months) • To inform users about extension features and other available solutions **Product and Business Improvement**

	• To better understand users' behavior (60 months) • 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) • To recognize what features should be enabled or disabled, what product should be installed or uninstalled **Product and Business Improvement** (60 months) • To better understand users' behavior
Browsers (installed, default)	**Service Provision** (36 months) • To provide import functionality, improve user onboarding and product experience **Product and Business Improvement** • To better understand users' behavior (60 months) • 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

[AVG Secure Browser for Android](#) and [AVG Secure Browser for iOS](#) (collectively as "Secure Browser for Mobile")

Core Functionality

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

What are Product's Features

- **Browser Security & Privacy Center** is built in Security & Privacy Center which is a curated collection of some key security and privacy features, tools and settings, organized into one management console making it easier for you to control and manage your online privacy and security.

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

- **Secure & Private Mode** creates an encrypted tunnel between your device and the internet, encrypts your DNS queries, stops ads being shown in your browser, prevents your browsing history from being stored, and removes any tracking cookies (both first-party cookies and third-party cookies) or web cache you pick up during that browsing session.
- **PIN Protection** secures your device against real world threats from local attacks by locking access to the browser application on your device with a unique code only you know. Your PIN Code is encrypted on disk and is not stored on any servers.
- **Privacy Statistics** are showing the users' the advantage of our AdBlock and VPN through numbers, by presenting the number of ads blocked, number of malware blocked by our Web Shield, amount of browsing data protected by our VPN.

Personal Data We Process

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

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

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

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)
	● Replaced with country for delivering geo-specific changes to configuration (both local or remote)
	● For prerendering feature functionality, if activated
Events and product usage	**Service Provision** (36 months)
	● To ensure functionality (installations, versions, updates, settings), map how users interact with the application and improve its design or flows
	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
	Product and Business Improvement
	● To better understand our users' behavior (up to 24 months)
	● Findings about product have an effect on the design or layout of the new one (24 months)

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

Online identifiers (GUIDs, Device IDs)	**Service Provision** (24 months) • To ensure functionality (installations, versions, updates, settings) and to track users subscription trials and purchases **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 **Product and Business Improvement** • To better understand our users' behavior (24 months) • To introduce a new feature or product based on previous experience (24 months)
Information concerning computer or device	**Service Provision** (36 months) • To check for compatibility issues in automated crash dumps • **Product and Business Improvement** • To better understand users' behavior (24 months) • 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

AVG Secure Identity

Core Functionality

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

Personal Data We Process

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

Secure VPN

[AVG Secure VPN](#)

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

TuneUp

Official Product Name

[AVG TuneUp for Windows](#), [AVG TuneUp for Mac](#) (collectively as "TuneUp")

Core Functionality

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

What are Product's Features

TuneUp for Windows:

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

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

TuneUp for Mac:

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

<mark>Personal Data We Process</mark>

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

Service Data	What we use it for and for how long

Events and product usage (such as product version, product language, license type, days to expiration, number of potential problems or detected junk)	**Service Provision** (up to 12 months) ● To monitor service functionality **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 **Product and Business Improvement** ● To better understand our users' behavior (12 months) ● To improve users' overall experience by developing new features or products (up to 12 months)

Device Data	What we use it for and for how long
Internal online identifiers (GUID, MIDEX, UUID, Device ID)	**Service Provision** (up to 12 months) ● To identify correct installation **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, types of cleaning objects, objects size, app name, vendor, version, rating, certification)	**Service Provision** (up to 12 months) ● To check for compatibility issues in automated crash dumps **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 **Product and Business Improvement** (up to 12 months) ● To better understand users' behavior ● 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) ● To set up a proper product language version for Windows **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 **Product and Business Improvement** (12 months) ● To better understand users' behavior based on approximate location ● 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 36 months) ● Our other apps to know which products users already have on their computer ● Third-party applications or programs installed on users' computers to improve Cleanup Sleep Mode, Software Cleanup and Software Updater functionality **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 **Product and Business Improvement** (up to 36 months) ● To improve the users' overall experience by developing new features and products ● To understand/estimate market opportunity for new products and new features

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