Avast Privacy Policy

partners

As the world's most trusted antivirus software company, we aim to defend you against threats in cyberspace. To do so, we may have to collect your personal data to provide you with the best weapons and the most up-to-date security. We do not take your trust for granted. As a multinational company with its headquarters in the Czech Republic, we conform our data use to the European Union's ("EU") General Data Protection Regulation ("GDPR"), with effect from 25 May 2018. Therefore, in our Privacy Policy, we explain what we do, how we do it, your choices, and how we may need your cooperation to help you stay safe. You want to visit **What Happens to Your Personal Data** and its sections:

You want to review each of these sections on this page:

If you use HideMyAss Virtual Private Network (“VPN”), please see our HMA! VPN Privacy Policy. For users of Avast/AVG VPN, please see our Avast/AVG VPN Privacy Policy. Please note that Avast Mobile Security now offers VPN as one of its features.

1. Our Policy’s Aims

1.1 The Avast Privacy Policy applies to Avast Software s.r.o. ("Avast") and unless specified, its subsidiaries, including AVG, Piriform (“CCleaner”), Privax Ltd (“HideMyAss!”), AVG Technologies Norway AS, TuneUp Software GmbH, and Jumpshot, Inc., and any contractors, representatives, agents, and resellers while they are working on our behalf (collectively “we,” “us” or “our”).

1.2 Our Privacy Policy explains the processing of your personal data by us and establishes what information we collect, or which is provided to us, and how we use and protect your personal data in compliance with applicable law.

1.3 Personal data refers to any information relating to an identified or identifiable natural person (“data subject”), where this identification can be made directly or indirectly, by means of identifiers such as your name, identification number, email address, phone number, online identifiers such as cookies in some circumstances, your location, your genetic, economic, cultural or social identity or other information that is specific to you.

1.4 We do not mean information that only refers to a business corporation or organization. We also do not mean information that has been "anonymized," either by removing or de-identifying all specific identifiers. Anonymous data is not personal data when the anonymization is irreversible. When we refer to anonymous data, we mean data that cannot be reversed into personal data.

1.5 As a data controller, we commit ourselves to protecting the privacy of our website visitors and users of our products and services with respect to the processing of your personal data.

1.6 Where we collect and process your personal data, we will limit the collection and retention to what is adequate, relevant and necessary for our purposes and it will be kept in a form which allows for your identification no longer than necessary for the purpose for which we process your personal data. We refer to this as data minimisation.

1.7 Where we store your personal data for longer periods for statistical purposes, as permitted, we will use appropriate safeguards. Applicable law defines ‘statistical purpose’ as any collection of personal data, where the result of processing is for aggregate data, so the personal data we collect from you is anonymized or pseudonymized.

For example, the processing of your personal data may be for the business-related process of counting users, products, sales and various metrics. We also share statistical data that has been anonymized and aggregated geographically and so, cannot be used to identify individuals, with third parties for trend analytics.

1.8 Our policy provides you with the legal bases for the collection of your personal data, lets you know how long personal data is stored and the reasons why, and how in some circumstances, they are necessary to retain. The length of this retention and how you may choose to request that we delete some or all your personal data and the consequences of the deletion are explained in this policy.

1.9 Some of the legal bases we rely on are contractual and service necessity, consent, legitimate interests and compliance with legal obligations.

1.10 We want you to have the necessary and relevant understanding of how and why we process your personal data so that you can make fully informed decisions on whether to allow us to retain your personal data or delete them. Section 2 explains your rights under applicable law and section 3 lets you know when the Privacy Policy applies.

1.11 We strive to keep the policy easy to understand and transparent, and so we refrain from technical information overload. If you wish to have further details on how we process your personal data, please contact us.

2. Talk to Us about Your Data

2.1 We try to ensure that the users of our products and services always have an open line of communication with us. You can contact us at any time if you any questions, queries or requests about your personal data and, if European law applies to the processing of your data, about your right to request access to, modify, remove or export your data, or object to our processing of your data. We appreciate if you reach out to us first before you approach any supervisory authorities or courts.

2.2 In order to make it easier for you to reach out to us and obtain the necessary information and action changes, corrections or deletions of your personal data, we have decided to provide you with a privacy preference portal.

2.3 Aside from the privacy preference portal, you can also submit your requests through more traditional channels. We will action your request within one month of receiving a request from you concerning any one of your rights as a data subject. Should we be inundated with requests or particularly complicated requests, the time limit may be extended to a maximum of another two months. If we fail to meet these deadlines, we would, of course, prefer that you contact us to settle the matter informally.

2.4 There could be instances where you are using our products or services, but we do not have your personal data, even though you have purchased our products or services. These include situations where you purchase our products from our service provider, a reseller, or an app store. Because your relationship in these cases is with that service provider, reseller or an app store, we do not actually have your personal data and will not be able to perform your request to access or delete your information. In such circumstances, please contact your service provider, reseller, or app store where you purchased the products or services, as this person is the primary controller of your personal data.

3. When Our Privacy Policy Applies

You should know that our Privacy Policy applies to the following situations and activities:

3.1 Online activities

Any personal data collected from you when you visit our websites or use our products or services

3.2 Phone contacts

Any personal data collected from you when you call us for sales, service, or customer support.

3.3 Offline contacts

Any personal data collected from you at a "live" or in-person event such as a trade show or promotion.

3.4 Reseller information

Any personal data, including contact information such as telephone number and email address, collected from Avast resellers or sub-resellers.

3.5 Other circumstances

Any personal data collected from you when you contact us by email or by clicking the "report a virus" link on our website or by requesting online service or support, or opening a support ticket, or through our media contact or news subscription services, or other occasions.

4. When Our Privacy Policy Does Not Apply

4.1 Third Party Sites

· Clicking on a thumbnail or profile link on our "Community" pages

This will take you to the third-party site from which the thumbnail or link was imported. By using a user ID from a third-party site, you agree to be governed by the terms and conditions, privacy policy, and data security policy of the third party. You also agree that we are not responsible for any loss or damage you may suffer from your dealings with the third party, or your use of or reliance on any of that party's content.

· Submitting a search query

When you submit a search query via an app like AVG Secure Search or through Avast Secure Browser, you are indicating that you consent to having your search query and history transmitted to third party search providers and to being redirected to third party sites, where the privacy policies of the third parties apply.

· Third party links

Third parties may also provide links to other websites and mobile applications (apps). Any sharing of data with third parties through access to and use of third party advertisements, their linked websites or mobile apps is not governed by this privacy policy, but instead is governed by the privacy policies of those third parties.

· Third party privacy practices

We are not responsible for the privacy practices of third parties. Your use of a third-party site will be governed by the terms and conditions, privacy policy, and data security policy of the third-party site.

5. Disclosing Your Personal Data to Third Parties

5.1 Disclosure to third parties

We are required to disclose your personal data to unrelated third parties in limited circumstances:

· where necessary to satisfy a legitimate government request or order;

· in compliance with a legal requirement by a court of law or in the public interest;

· in response to a third-party subpoena, if we believe on the advice of our attorneys that we are required to respond;

· where we hire a contractor to perform a service for us, such as product development or market research (but not if doing so would violate the terms of our privacy policy, or laws governing personal data);

· if we obtain your permission; or

· if necessary to defend ourselves or our users (for example, in a lawsuit).

5.2 We are also required in a few limited situations to share our users' personal information with third parties. For example, if you request a specific service or product from us, and if that product or service is administered by a third party working for us, we may share your personal information with the third party to respond to your request. This third party may also transmit back to us any new information obtained from you in connection with providing the service or product.

5.3 When you contact us or a third-party service provider working on our behalf, our service provider may suggest upgrades to our products or services. Our service provider may also suggest products or service that the service provider offers which are not Avast products or services. In this case, you will be clearly advised that the product or service is offered by the third party and not by Avast, and you will be subject to the terms and conditions, end user license agreement (EULA), and privacy policy of the third-party service provider.

5.4 We offer third party browsers to new users of certain products, such as our antivirus products. Whether you install the third party browser is in your discretion.

5.5 For certain mobile products, we offer third party ads. While we do not share your personal data with the ad network, data from your device including its IP Address, is used by the ad network to enable the delivery of the ads. If you do not want to view third party ads, you have the choice to change to a paid version of the product. If you are served a third party ad and you click on the ad, your data will be governed by the relevant third party whose ad you clicked on.

5.6 We reserve the right to store and use the information collected by our software. We may publish or share that information with third parties that are not part of the Avast Group, but we will only ever do so after anonymizing the data.

6. International Transfers of Your Personal Data

6.1 We are a global business that provides its products and services all around the world. In order to reach all of our users and provide all of them with our software, we operate on an infrastructure that spans the globe. The servers that are part of this infrastructure may therefore be located in a country different than the one where you live. In some instances, these may be countries outside of the European Economic Area (“EEA”), where the level of protection provided by the laws of these countries may be different than the high standard enshrined in the GDPR. Regardless, we provides the same GDPR-level of protection to all personal data it processes.

At the same time, when we transfer personal data outside of the EEA, we always make sure to put in place appropriate and suitable safeguards, such as standardized contracts approved by the European Commission, which legally bind the receiving party to adhere to a high level of protection, and to ensure that your data remains safe and secure at all times and that your rights are protected.

Situations where we transfer personal data outside of the EEA include provision of our products and services, processing of transactions and your payment details, and the provision of support services.

7. Sharing of Information among Avast Entities

7.1 Our data collection and management practices do not vary by location. We follow the same “data minimisation” procedure with respect to all personal data in our possession, regardless of the jurisdiction from which it was collected, and regardless of whether the data is transferred from one member of the Avast Group to another.

7.2 We reserve the right to store and use the information collected by our software and to share such information among the Avast Group to improve our current and future products and services, to help us develop new products and services, and to better understand the behaviour of our users.

7.3 Any reference in this policy to “Avast Group” means Avast, its, direct and indirect, parent companies and any company that is, directly or indirectly, controlled by or under common control with Avast or its parent companies.

8. Storage, Retention, and Deletion of Your Personal Data

8.1 Storage of Information

We store information that we collect on our servers or on the servers of our subsidiaries, affiliates, contractors, representatives, contractors, agents, or resellers who are working on our behalf.

The data on our servers can only be accessed from our physical premises, or via an encrypted virtual private network (“VPN”). Access is limited to authorised personnel only, and company networks are password protected, and subject to additional policies and procedures for security.

8.2 Access by our contractors

We or our contractors, subsidiaries, affiliates, representatives, agents, or resellers who are working on our behalf undertake regular maintenance of your personal data. All third parties must agree to observe the privacy of our users, and to protect the confidentiality of their personal information. This means your personal data cannot be shared with others, and there must be no direct marketing by the third parties.

Avast

8.3 Retention and Deletion of Your Personal Data

We retain data for limited periods when it needs to be kept for legitimate business or legal purposes. We collect data when you purchase and as you use our services. What we collect, why we collect it, and how you can manage your information are described in our Privacy Policy. If you purchased a service or registered an account with us, you may see a copy of the personal data collected from you at the privacy portal. Also, you can manage in the product settings how certain data is used.

For each type of data, we set retention timeframes based on the reason for its collection and processing. Some data you can delete whenever you like, and some data is deleted automatically as soon as we do not need it for our legitimate business or legal purposes. We do not delete data that we need for our legitimate or legal purposes, even upon request, until the purposes expire. We also take steps to anonymize certain data within set time periods. For example, we strive to anonymize IP Addresses by substituting city and country after thirty days. We may also amend the personal data we keep in such a way that you cannot be identified, for example, by hashing. We may retain a “key” to the hashing, but we will securely store it separately from the hashed data.

When the data is deleted, we remove it from our servers or retain it only in anonymized form.

The following describes why we hold onto different types of data for different periods of time.

- We keep your data for the life of your subscription or account, if it's necessary for the service (such as for activation, billing, support, communication) or if it helps us understand how users interact with our features and how we can improve our services.

- If you registered an account with us, we will keep data in your account until you choose to delete the account.

- If you subscribe to a recurring newsletter, we will keep your information to continue to fulfil your subscription request. In the case of the Forum, the Support Portal, or news and blogs, your account data is kept active until you delete it.

We have business and legal requirements that require we retain certain personal data, for specific purposes, for an extended period of time. For example, when our authorized partner processes a payment for you, or when you make a payment, your data will be retained for as long as required for tax or accounting purposes. Reasons we might retain some data for longer periods of time include:

· Security, fraud & abuse prevention

· Financial record-keeping

· Complying with legal or regulatory obligations, including for investigations, enforcement, or when legally actionable

· Ensuring the continuity of our services

· Direct communication with you and our authorized partners, such as for service activation, billing, support, and marketing.

9. Data Security

9.1 Safeguards for protection of personal information

We maintain administrative, technical, and physical safeguards for the protection of your personal data.

9.2 Administrative safeguards

Access to the personal data of our users is limited to authorized personnel who have a legitimate need to know based on their job descriptions, for example, employees who provide technical support to end users, or who service user accounts. In the case of third-party contractors who process personal information on our behalf, similar requirements are imposed. These third parties are contractually bound by confidentiality clauses, even when they leave. Where an individual employee no longer requires access, that individual's credentials are revoked.

9.3 Technical safeguards

We store your personal information in our database using the protections described above. In addition, we utilize up-to-date firewall protection for an additional layer of security. We use high-quality antivirus and anti-malware software, and regularly update our virus definitions. Third parties who we hire to provide services and who have access to our users' data are required to implement privacy and security practices that we deem adequate.

9.4 Physical safeguards

Access to user information in our database by Internet is not permitted except using an encrypted virtual private network (VPN). Otherwise, access is limited to our physical premises. Physical removal of personal data from our

location is forbidden. Third-party contractors who process personal data on our behalf agree to provide reasonable physical safeguards.

9.5 Proportionality

We strive to collect no more personal data from you than is required by the purpose for which we collect it. This, in turn, helps reduce the total risk of harm should data loss or a breach in security occur: the less data we collect, the smaller the overall risk.

9.6 Notification in the event of breach

In the unlikely event of a breach in the security of personal data, we will notify all users who are actually or potentially affected.

We may tailor the method of notice depending on the circumstances. Where the only contact information that we have for you is an email address, then the notification will necessarily be by email. We may also elect to give you notice via our in-product messaging system. Where we believe there are affected users for which we have no contact information on file, we may give notice via publication on our company website.

We reserve the right to delay notification if we are asked to do so by law enforcement or other authorities, or if we believe that giving notice immediately will increase the risk of harm to our user body overall.

10. Other Jurisdictions

Residents of the Russian Federations

We collect and process personal data on the territory of the Russian Federation in strict compliance with the applicable laws of the Russian Federation.

We collect and process personal data (including sharing it with third parties) only upon the consent of the respective individuals, unless otherwise is provided for by the laws of the Russian Federation. You will be asked to grant your consent by ticking the respective box / or clicking “I accept” button or through similar mechanism prior to having access to the site, and/or when submitting or sharing the personal data we may request. We collect and use your personal data only in the context of the purposes indicated in the consent to processing of personal data.

We (directly or through third party contractors specifically authorized by us) collect, record, systematize, accumulate, store, actualize (update and amend), extract personal data of the Russian Federation citizens with the use of databases located on the territory of the Russian Federation, except as otherwise permitted by Russian data protection legislation. We may process personal data of Russian citizens using databases located outside of the Russian Federation subject to compliance with Russian data protection legislation.

We undertake all the actions necessary to ensure security of your personal data.

You are legally entitled to receive information related to processing your personal data. To exercise this right, you have to submit a request by e-mail at: customerservice@avast.com with the headline “PRIVACY REQUEST” in the message line.

You have the right to revoke the consent at any time by sending us an e-mail at: customerservice@avast.com with the headline “PRIVACY REQUEST” in the message line. Once we receive the revocation notice from you we will stop processing and destroy your personal data, except as necessary to provision the contract or service to you. However, please note once you have revoked your consent, we may not be able to provide to you the products and services you request, and may not be able to ensure proper work of our products.

We do not transfer your personal data to the countries that under Russian law are not deemed to provide adequate protection to the individuals' rights in the area of data privacy.

We do not offer, sell or otherwise make available our products or services that have access to, collect and process (or allow us to do the same) personal data of third parties in the Russian Federation without the consent of such third parties.

If any provisions of this Policy contradict the provisions of this section, the provisions of this section shall prevail.

Your California Privacy Rights

Under California Civil Code § 1798.83, we are required to disclose to consumers the following information upon written request: (1) the categories of personal information that we have disclosed to third parties within the prior year, if that information was subsequently used for marketing purposes; and (2) the names and addresses of all such third parties to whom such the personal information was disclosed. We hereby disclose that we have not disclosed any such personal information regarding any California resident during the one-year period prior to the effective date of this Privacy Policy. California residents seeking additional information on this requirement or our privacy practices in general may write to us at customerservice@avast.com with the headline "PRIVACY REQUEST" in the message line. They may also send paper mail to Avast Software s.r.o., Pikrtova 1737/1a, 140 00, Prague 4, Czech Republic. Please write "Attention: PRIVACY" in the address.

11. Policy Changes

11.1 Updates to our Privacy Policy will occur from time to time and we will publish these changes on our website.

11.2 We suggest that you check our Privacy Policy every so often to keep yourself informed.

11.3 Where the changes are major, we will notify you by email if you have an Avast account or through posts on our website.

12. Contacting Us

12.1 We are registered as Avast Software s.r.o. and our registered address is Pikrtova 1737/1a, 140 00 Prague 4, Nusle, Postal Code 140 00, Czech Republic.

12.2 Dispute resolution

We make every effort to conduct our business in a fair and responsible manner. In the unlikely event of a disagreement or complaint about the way that your personal data is handled, please contact us.

12.3 Contact Details

· You can always reach us by email at https://support.avast.com/en-usm. Please type "PRIVACY REQUEST" in the message line of your email so we can have the appropriate member of the Avast team respond.

· If you prefer, you can send paper mail to AVAST Software s.r.o., Pikrtova 1737/1a, 140 00 Prague 4, Czech Republic. Be sure to write "Attention: PRIVACY" in the address so we know where to direct your correspondence.

13. Data Protection Officer

13.1 As required under the GDPR, we have a data protection officer (DPO) to monitor our compliance with the GDPR,

provide advice where requested and cooperate with supervisory authorities. You can contact our data protection officer via dpo@avast.com.

What Happens to Your Data

Let us take you into the intricacies of what happens to your data. You may like to navigate directly to the sections as follows:

A. How We Use Personal Data We Collect

The personal data we collect may come directly from you or we may obtain it from other sources, such as our service providers and resellers.

We want you to understand the types of personal data we process and if we do not obtain your personal data directly from you, the source we used, and the specific data collected.

We collect personal data for these reasons: to process the purchase of a product or service; to provision the product or service to you; and for the legitimate interests of us. We use no more than the minimum amount of personal data needed for the processing. We also use personal data only when the processing is necessary for our or our third party's legitimate interests.

When our use of your personal data is based on our legitimate interests and is compatible with the provision of service, you have the right to object. In some cases, you may exercise your right to object directly, for example you may unsubscribe to email marketing messages or you may choose to turn off data use in the applicable product settings; in other cases you may notify us here https://support.avast.com/en-us and we will investigate the grounds relating to your particular situation.

Avast is a global business and we have operations and personnel around the world who process personal data. We have standard contractual clauses in place among its affiliates which govern the transfer and use of personal data.

In the following sections, we explain the personal data we collect. Please be mindful that some of the categories may collect the same personal data.

B. Choice and Portal

You can make certain choices about how your data is used by us. For example, if you have purchased a product or service from us, you will be able to choose how data collected from you is used. This choice is made in the relevant product settings. Please note, if you purchased a product from us and in your product settings you do not see one or more of these choices, it means your collected data is not being used in that particular category. The choices are:

· Cross-product direct marketing: – when we offer you another product from a company within our group.

· Cross-product development – when we collect data from one product and use it for the development of another product.

· Third Party Ads – when we offer any third-party products.

· Third party analytics – when we share your data with a third party for analytics, such as purchase optimization, crash reporting, and trend analytics. *Note, all free users and paid customers can choose to turn of this feature.*

We have a portal where we will show you the Billing Data (defined below) and Account Data (defined below) we have collected from you as well as your email preferences. In general, only Billing Data and email addresses collected directly by us, AVG, and HMA!, will be currently available for viewing in the portal. If you purchased CCLeaner products and want to see the Billing Data collected from you, please contact Piriform here.

Likewise, if you purchased our products from a reseller or a distributor (e.g. business products) or you purchased a mobile product from an app store (e.g. Google Play or Apple App Store) we will not display your Billing Data in the portal because we do not have it; the reseller, distributor, or app store does. You would need to request a view of your Billing Data from your reseller, distributor, or app store. Also, for the Billing Data that we do collect, as we store it and use it separately from your Service Data, we will not display any of your Service Data in the portal.

If you have purchased a product directly from us, through one of its third party service providers, or you have requested support from one of our technical support providers, or you have registered an Account with us, you will need to use the same email address you previously provided us to login to the portal. If you have never purchased a product or provided us with your email address (e.g. you are a free user, a mobile user, or a mobile paid customer), you will not be able to access the portal, because we do not have any Billing Data or email address collected from you.

The portal is for your convenience only. It is generally read only. This means, you are able to see your choices but not able to edit your choices in the portal. To edit your choices, you need to do so in the applicable product settings.

C. Billing Data

Paid Products and Services for your personal computer

When you purchase "premium" or pay for products or services for your personal computer, the billing is handled by a third-party service provider. The service provider is acting as our agent; thus, you will be making your purchase from the service provider directly, and not from us.

If you purchase a "premium" or paid product or service, we, through our third-party service providers, will collect your name, email address, credit card number, and in certain circumstances, your billing address and your phone number (collectively “Billing Data”). Your Billing Data will be retained for as long as is necessary to complete payment, including any renewal periods.

Your Billing Data is collected by our third-party service providers only where necessary for the purposes of processing

or refunding your payments, or so that they can communicate with you. Your Billing Data may also be retained for legal reasons, for example, taxation.

The third-party service provider may transmit your Billing Data (excluding credit card number) to us. We use the Billing Data to create a record of its software installations or service requests.

We may process and store the Billing Data we receive, to verify your registration or license status, to contact you about the status of your account, or for renewal of your subscription, if applicable. We process the Billing Data as necessary for the provision of the contract and service.

In all cases where your credit card number is processed by a third-party service provider, we have determined that the service provider follows data privacy and security procedures that we deem adequate. Some of these third-party service providers are subject to the enhanced data privacy rules of the European Union. Others have self-certified annually to comply with the EU-US Privacy Shield or the Swiss-US Privacy Shield.

In all cases such third-party service providers have executed agreements with us promising not to use your personal data for their own marketing purposes, and not to share this information with other parties for their unrestricted use.

We store your Billing Data separately from your Service Data (defined below).

We may change service providers as we carry out our business. In that case, your Billing Data will be transferred from one service provider to another. When this happens, you will be informed of such transfer.

Paid Products and Services for your mobile device

When you purchase "premium" or pay for products or services for your mobile device, the billing is handled by a third-party app store, such as Google Play and Apple iTunes. You will be making your purchase from the third party app store directly, and not from us.

Your Billing Data is collected by the third party app store and your Billing Data is not shared with us.

Paid Products and Services for your business

When you purchase "premium" or pay for products or services for your business, the billing is handled by our reseller or distributor. You will be making your purchase from the reseller or distributor directly, and not from us.

Your Billing Data is collected by the reseller or distributor. Your Billing Data, excluding your credit card number, may be shared with us. We use the Billing Data to create a record of the software installations.

We may process and store the Billing Data we receive, to verify your registration or license status. But, generally, we will not contact you. Your reseller or distributor will contact you about the status of your account, or for renewal of your subscription. We process the Billing Data as necessary for the provision of the contract and service.

The handling of your Billing Data (excluding your credit card number) shared with us by the service provider, reseller, or distributor will be governed by this Privacy Policy and the End User License Agreement applicable to the product or service from us. Your Billing Data inclusive of your credit card number collected by the service provider, reseller, distributor, or third party app store to process your payment and renewal will be governed by any privacy policy or terms of service published by the applicable third-party service provider, reseller, distributor, or the third party app store.

In some instances, we change resellers or distributors as we carry out our business. In that case, your Billing Data will be transferred from one reseller or distributor to another. When this happens, you will be informed of such transfer.

What about Free Products?

You are not required to disclose Billing Data to download our free products and services for your PC and mobile device, which includes free AntiVirus, free mobile security, and free CCLeaner for desktop. However, our free CCLeaner cloud product does require you provide your name and email address to register for the product.

D. Support

We directly or through our third party technical support service provider(s) collect your name, email address, phone number(s), home or work address, or other information by which we may identify you while providing technical support. We need this data for verification and to communicate with you about your support request.

In cases where you request individual support or assistance we may ask you to provide information about your device or computer, your means of accessing the Internet, or information about your internet service provider. To provide the technical support we also collect data that may include your email address, IP Address, information about your hardware and software, the URLs of sites you have visited, files stored on your computer (including potentially dangerous or infected files), email messages (whether stored on your computer or elsewhere), information regarding senders and receivers of email messages, and the like. If you request support, we may offer you the option of accepting a remote session in which we take control of your device or computer in order to help you resolve the issue.

Information collected while providing the support will not be used for secondary purposes, other than, we may use your email address to send you information about our other products or services. If you contact us for support, we may suggest that you upgrade or update products or services. Information and data connected to provision of support will be retained by us to have a history of support requests and for support research purposes.

E. Marketing

When we collect your email address, we may market our other products and services to you. You may choose to unsubscribe from future email marketing by following the instructions in the email.

Generally, we do not serve third party ads in its products for the personal computer. We may serve third party ads in our products for mobile devices.

To be able to offer you our services for free, we show third party ads within your mobile apps through popular ad networks, which are listed below. We display an AdChoices logo on top of every ad. You can tap the icon to learn more about the ad network.

To enable the ad, we embed a third-party software development kit (SDK) for these ads. The SDK code is provided by third party ad agencies or networks.

Data of our mobile users remain anonymous to us and to the third party ad agencies. However, the ad agencies' SDK code will collect data to tailor ads to you, such as the third-party apps you installed on your device, your Android advertising identifier, your IP Address, your device's operating system details and MAC address, and other statistical and technical information. You can find more information in each network's privacy policy, the link to which we are also including in the overview below.

Ad Network	Provider	Product	Link to Privacy Policy, Additional Information

AdMob	Google	• Avast Mobile Security • AVG AntiVirus • AVG Protection for Xperia • VPN SecureLine Proxy by Avast • Avast Wi-Fi Finder • Avast Cleanup • VPN Proxy by Avast SecureLine • Avast Battery Saver • CCleaner • Alarm Clock Xtreme • AVG Cleaner • Gallery • AVG Cleaner for Xperia™	https://policies.google.com/privacy?hl=en https://support.google.com/admob/answer/9012903?hl=en-GB https://support.google.com/admob/answer/2753860#Interest_based
Amazon	Amazon	• Avast Mobile Security • AVG AntiVirus • AVG Protection for Xperia • Avast Cleanup • CCleaner	https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=502584

		• Alarm Clock Xtreme • AVG Cleaner • AVG Cleaner for Xperia™	
AppLovin	AppLovin	• AVG Cleaner • CCleaner • Avast Cleanup • AVG Cleaner for Xperia™	https://www.applovin.com/privacy/
Facebook Audience Network	Facebook	• Avast Mobile Security • AVG AntiVirus • AVG Protection for Xperia • VPN SecureLine Proxy by Avast • Gallery • Avast Cleanup • VPN Proxy by Avast SecureLine • Avast Battery Saver • CCleaner • Alarm Clock Xtreme • AVG Cleaner • AVG Cleaner for Xperia™	https://www.facebook.com/privacy/explanation https://developers.facebook.com/docs/audience-network/policy/

InMobi	InMobi	• Avast Mobile Security • AVG AntiVirus • Avast Cleanup • CCleaner • Alarm Clock Xtreme • AVG Cleaner	https://www.inmobi.com/privacy-policy/
Ironsource	IronSource	• AVG Cleaner • CCleaner • VPN SecureLine Proxy by Avast • Avast Cleanup • AVG Sony Cleaner	https://developers.ironsrc.com/ironsource-mobile/air/ironsource-mobile-privacy-policy/
Mopub	Twitter	• Mobile Security & Antivirus • Alarm Clock Xtreme Free • AVG AntiVirus • Gallery • Avast Cleanup & Boost • AVG Cleaner • Avast Battery Saver	https://www.mopub.com/legal/privacy/ https://www.mopub.com/legal/partners/

		• AVG Cleaner for Xperia™ • CCleaner	
Unity	Unity Technologies	• AVG Cleaner • CCleaner • Avast Cleanup • AVG Cleaner for Xperia™	https://unity3d.com/legal/privacy-policy
Taboola	Taboola	• Alarm clock	https://www.taboola.com/privacy-policy

If you do not want to view third party ads, you may uninstall the free mobile product and/or choose an available paid version of mobile products, which does not serve third party ads.

F. Online Identifiers

GUID

The GUID is a randomly generated number that we assign to each installation of software. For paid customers of products and services for your personal computer, the GUID is connected to your Billing Data. For free users of products and services for your personal computer and your mobile deice, and for paid customers of business and mobile products and services, as there is no Billing Data collected by us, the GUID is disconnected from personal data.

The GUID is used for many purposes, which will be described in this Privacy Policy.

Cookies

Our websites use cookies to acquire data that may be used to determine your physical location via your Internet Protocol address (“IP Address”) and automated geolocation techniques, or to acquire basic information about the computer, tablet, or mobile phone that you use to visit us. See description below. By using our websites, you authorize the collection and use of data by cookies according to the terms of this privacy policy.

We use common information-gathering tools, such as cookies, pixel tags and Web beacons, to collect information about your general internet usage. When you visit our websites, a cookie file is stored on your browser or the hard drive of your device. Technologies such as: cookies, beacons, tags and scripts are used by us and our marketing partners, affiliates, or analytics or service providers (e.g. payment processor, etc.). These technologies are used in analyzing trends, administering the site, tracking your movements around the site and to gather demographic information about our user base as a whole. We may receive reports based on the use of these technologies by these companies on an individual as well as aggregated basis. You authorize us and agree that we may place cookies or tracking technologies on your device.

Across all of our websites, we may use the following cookies or tracking technologies:

Cookie	Purpose	Party	Cookie Provider
Google API	Functionality	3	Google
Analytics	analytics & tracking	1	us
AdWords	retargeting	3	Google
DCM	retargeting	3	Google
Optimize	analytics & tracking	1	us
Hotjar	analytics & tracking	1	us
Optimizely	analytics & tracking	1	us
Visual Website Optimizer	analytics & tracking	1	us
Facebook	retargeting	3	Facebook
LinkedIn	retargeting	3	LinkedIn
My Target	retargeting	3	VKontakte
Outbrain	retargeting	3	Outbrain
A8Fly	affiliate	1	us
AXM	retargeting	3	MediaMath
Commision Junction	affiliate	1	us
Bing	retargeting	3	Microsoft
Captera	retargeting	3	Captera
Criteo	retargeting	3	Criteo
Ginga	retargeting	3	Signal
Softonic	retargeting	3	Softonic International
SalesForce	retargeting	3	salesforce.com
Sklik	retargeting	3	Seznam

Hubspot	CMS	1	us
Twitter	retargeting	3	Twitter
SoundCloud	podcasts	3	SoundCloud
Iron Source	retargeting	3	Ironsource
apex__avastLocale	locale switcher	1	us
apex__avgLocale	locale switcher	1	us
hidemyassComLocale	locale switcher	1	us
apex__language	locale switcher	1	us
avgLocale	locale switcher	1	us
geoip	locale switcher	1	us
sat_track	analyticst & tracking	1	us
consentAccepted	cookie consent accepted by user	1	us
couponfield	coupon for cart	1	us

Please note that not all of our websites use all of these cookies.

We may partner with a third party either to display advertising on our site or to manage our advertising on this site and other sites. Our third party partner may use technologies such as cookies to gather information about your activities on this site and other sites in order to provide you advertising based upon your browsing activities and interests. By continuing to browse our websites, you are aware of the use of cookies, as described in this Privacy Policy. If you do not wish to allow the use of cookies, you can disable them through your browser settings. We do note, however, that not all browsers across all platforms may support this functionality. Furthermore, if you disable cookies, our websites may not function properly or your access to our websites and their features may be affected or restricted**.**

IP Address

We collect your IP Address to provision your product or service. We also use the IP Address with mobile products to serve ads. We strive to replace your IP Address within sixty days of collecting it with your city and country or we hash your IP Address.

G. In-Product Messaging

We sometimes communicate with you using a technique known as "in-product messaging." In-product messaging may be used in the following scenarios:

· when your license is about to expire;

· when you update or upgrade a program;

· when a virus database is updated;

· when you visit an infected webpage;

· when a monthly security report is prepared for you; or

· in other cases where user communication is necessary for provision of our products or services.

We also use in-product messaging to notify you of different products or upgrades to existing products and services. Data used for in-product messaging is connected to the GUID for in-product messaging to function. For free users, this data remains anonymous and for paid customers, the data is pseudonymized.

Billing Data is however not used for in-product messaging. In-product messaging also permits your computer or device to transmit information to our servers including technical data, virus definitions, security, and technical information about your hardware.

The data may be used to offer you a discount on a new product based on your past purchases. Data is also used for analytical and statistical purposes, product updates, quality control, and in-product and feature design. Premium or paid customers can manage In-product messaging for marketing purposes in the applicable product settings.

H. Service Data

Service Data is collected from your use of our websites, products, and services.

Service Data is used primarily to provision the products or services. Service Data is also used for the compatible and legitimate uses of research, to compile statistics, analytics, aggregated reporting, product development, In-product messaging, and direct marketing. Before Service Data is used for secondary purposes, pseudonymize or anonymize the Service Data.

For all Service Data, we practice “data minimization”, which means we limit our collection and retention of your data to only what is necessary, adequate and relevant to achieve our processing purpose.

Below we list our products and the Service Data that each collects. There may be other products (current or future) that require us to collect certain types of personal data to enable full product functionality. We will always inform you prior to collecting any such information, usually in the terms of service or end user license agreement (EULA) or the privacy notice applicable to the product or service. Personal data collected as part of Service Data is necessary to the provision of the product functionality. When personal data is no longer needed we limit or stop using it in line with the minimization principle. For example, your email, the URLs of websites you have visited, your files, are scanned for malware detection and protection; then we remove your email address and other personal data or we hash any identifiers turning the Service Data into pseudonymized or anonymized data for paid users and anonymized data for free users before we re-use the Service Data for research, analytics, statistics, reporting, cross-product development, in-product messaging, and marketing..

The primary processing of Service Data will be to perform the contract to provision the product or service to you. The secondary processing of Service Data will be as compatible for our legitimate interests to provide you the benefits of research, analytics, cross-product development, and cross-product in-product messaging. If we need to process your Service Data for a purpose that requires consent, we will notify you separately of this and the general rules of providing and withdrawing consent shall apply.

Website Log Files

We collect the information in the form of server log files that tell us generally about the visitors to our site, which may include general geographic regions, length of visits, the webpages you request, the URLs of the site you were viewing before clicking on our websites, your IP Address, cookies, the type of web browser and operating system you are using, click-stream data and so forth.

If a user downloads a product from our website, we connect the installation GUID with the user's website log. We use this information to fulfil our legitimate interests, which are to analyse overall trends, administer our webpages, track users' use of the webpages, help us improve our website(s), and to better understand the users' experience on our website(s) when downloading and activating our products.

Device and Network Information

We may collect information about the computer or device you are using, our products and services running on it, and, depending on the type of device it is, what operating systems you are using, device settings, application identifiers (AI), hardware identifiers or universally unique identifiers (UUID), software identifiers, IP Address, location data, cookie IDs, and crash data (through the use of either our own analytical tools or tolls provided by third parties, such as Crashlytics or Firebase). Device and network data is connected to the installation GUID.

We collect device and network data from all users. We collect and retain only the data we need to provide functionality, monitor product and service performance, conduct research, diagnose and repair crashes, detect bugs, and fix vulnerabilities in security or operations (in other words, fulfil our contract with you to provision the service).

We also use your device and network data for in-product-messaging and cross-product development. Premium or paid customers can manage in-product messaging for marketing purposes and cross-product development in the applicable product settings.

We collect information in the form of statistics through our own or third-party analytics about which apps have been installed or uninstalled, how they are used, the number of active users, and the impact apps have on device performance and battery consumption (collectively, "AppInfo"). From this we study device and network behaviour, purchasing history and trends to measure the relative success of our products over time (in other words, serve our legitimate interests).

Analytics and Crash Reporting

We use analytical tools, including third party analytical tools, which allow us to, among other things, identify potential performance or security issues with our products, improve their stability and function, understand how you use our products, and websites, so that we can optimize and improve your user experience, as well as evaluate and improve our campaigns. While we generally prefer using our own analytical tools, we sometimes need to partner with other parties, which have developed and provide us with their own tools and expertise. Below, we list these partners, their tools which we use, as well as additional information on where and how we use them.

Tool	Product	Tool Provider	Description	Privacy Policy
Google Analytics	**Avast Omni (IoT)** **Desktop:**	Google	Our apps use Google Analytics to	https://support.google.com/analytics/answer/6004245 https://policies.google.com/privacy

	Desktop AV - Avast and AVG both CCleaner Desktop CCleaner Cloud Avast Cleanup AVG TuneUp **Mobile:** Call Blocker (Avast Call Blocker) WifiFinder (Avast WifiFinder) Passwords (Avast Passwords) Smart Home Security (Avast Skyline/Scout/IOT) Battery Saver (Avast Battery Saver) Gallery Doctor (AVG Photo Cleaner) Gallery (Flayvr Media Gallery) Mobile Security (Avast Antivirus) AntiVirus Free (AVG Antivirus) AntiVirus Pro (AVG Antivirus) AntiVirus Tablet Free (AVG Antivirus) AntiVirus Tablet		allow us to understand how our users use and interact with our products and how to improve our products. Where our apps use Google Analytics for Apps or the Google Analytics for Firebase SDKs, Google Analytics collects an app-instance identifier — a randomly generated number that identifies a unique installation of an app. Whenever a user resets their Advertising Identifier (Advertising ID on Android, and ID for Advertisers on iOS), the app-instance identifier is also reset. Where our apps have implemented Google Analytics with other Google Advertising	https://support.google.com/analytics/answer/6366371?hl=en&ref_topic=2919631

	Pro (AVG Antivirus) AntiVirus Xperia (AVG Antivirus for Sony) Cleaner (AVG Cleaner) Cleaner Xperia (AVG Cleaner for Sony) Cleanup (Avast Cleaner) CCleaner Android (Piriform CCleaner) Alarm Clock Xtreme Free (AVG Alarm Clock) Alarm Clock Xtreme Pro (AVG Alarm Clock) SecureLine (Avast VPN) AVG Secure VPN (AVG VPN) SecureMe (Avast VPN) HMA! VPN (Privax VPN)		products, like AdWords, additional advertising identifiers may be collected. Google Analytics also collects Internet Protocol (IP) addresses to provide and protect the security of the service, and to give us a sense of which country, state, or city in the world our users come from (also known as "IP geolocation"). We do implement measures and best practices in order to avoid sending personal data when collecting Analytics Data such as: Safeguarding our data, IP Anonymization, IP masking, data retention, user deletion and access management.	
Firebase Analytics	**Avast Omni (IoT)** **Mobile:**	Google	Firebase Analytics is a service that helps us	https://firebase.google.com/support/privacy/ https://policies.google.com/privacy

	Avast Mobile Security (Avast Antivirus) AntiVirus Free (AVG Antivirus) AntiVirus Pro (AVG Antivirus) AntiVirus Tablet Free (AVG Antivirus) AntiVirus Tablet Pro (AVG Antivirus) AntiVirus Xperia (AVG Antivirus for Sony) Cleanup (Avast Cleaner) Cleaner (AVG Cleaner) Cleaner Xperia (AVG Cleaner for Sony) CCleaner Android (Piriform CCleaner) Alarm Clock Xtreme Free (AVG Alarm Clock) Alarm Clock Xtreme Pro (AVG Alarm Clock) Call Blocker (Avast Call Blocker) WifiFinder (Avast Wifi Finder) SecureLine (Avast VPN)		understand our users and how they use apps including information about interactions with the user's mobile applications. Firebase Analytics uses identifiers for advertising on mobile applications (for example, Android Advertising ID and Identifier for Advertisers for iOS - IDFA), and we will collect the AAID and IDFA for these above-mentioned purposes. Users who wish to opt-out of the AAID and IDFA advertisement tracking can do so through device advertising settings for mobile apps within your device and users who wish to avoid tracking by Firebase Analytics can opt-out in application

	AVG Secure VPN (AVG VPN) HMA! VPN (Privax VPN)		settings. Data collected will be transmitted to and stored by Google on servers globally.	
Firebase Crash Reporting	**Avast Omni (IoT)** **Mobile:** Avast Mobile Security (Avast Antivirus) AntiVirus Free (AVG Antivirus) AntiVirus Pro (AVG Antivirus) AntiVirus Tablet Free (AVG Antivirus) AntiVirus Tablet Pro (AVG Antivirus) AntiVirus Xperia (AVG Antivirus for Sony) Cleanup (Avast Cleaner) Cleaner (AVG Cleaner) Cleaner Xperia (AVG Cleaner for Sony) CCleaner Android (Piriform CCleaner) Alarm Clock Xtreme Free (AVG Alarm Clock)	Google	To improve the stability of mobile applications, we use crash reporting services to collect information about the devices that you use and your use of our applications (for example the timestamp of when you launched the application and when the crash occurred) which enables us to diagnose and resolve problems. This allows us to deliver to you stable, functioning services and improve our applications in the future. The data collected does not contain any information which can personally	https://firebase.google.com/support/privacy/ https://policies.google.com/privacy

	Alarm Clock Xtreme Pro (AVG Alarm Clock)		identify you. The data will be transmitted to and stored by Google (Firebase Crash Reporting and Fabric Crashlytics) on servers globally.	
Fabric Crashlytics	**Avast Omni (IoT)** **Mobile:** Avast Mobile Security (Avast Antivirus) AntiVirus Free (AVG Antivirus) AntiVirus Pro (AVG Antivirus) AntiVirus Tablet Free (AVG Antivirus) AntiVirus Tablet Pro (AVG Antivirus) AntiVirus Xperia (AVG Antivirus for Sony) Passwords (Avast Passwords for Android) Cleanup (Avast Cleaner) Cleaner (AVG Cleaner) Cleaner Xperia (AVG Cleaner for Xperia) CCleaner Android (Piriform CCleaner) SecureLine (Avast VPN) AVG Secure VPN (AVG VPN)	Google		https://try.crashlytics.com/terms/privacy-policy.pdf https://policies.google.com/privacy

	HMA! VPN (Privax VPN) Alarm Clock Xtreme Free (AVG Alarm Clock) Alarm Clock Xtreme Pro (AVG Alarm Clock)			
AppsFlyer	**Avast Omni (IoT)** **Desktop:** HMA!VPN for desktop **Mobile:** SecureLine (Avast VPN) HMA! VPN (Privax VPN) AVG Secure VPN (AVG VPN) Avast Mobile Security (Avast Antivirus) AntiVirus Free (AVG Antivirus) AntiVirus Pro (AVG Antivirus) AntiVirus Tablet Free (AVG Antivirus) AntiVirus Tablet Pro (AVG Antivirus) AntiVirus Xperia (AVG Antivirus for Sony) Cleanup (Avast Cleaner)	AppsFlyer	AppsFlyer is a third party SDK (software development kit) embedded into our software. It allows us to analyze our marketing campaigns. We use it for the purpose of understanding through which marketing campaign you were directed to us and to evaluate the success and performance of our marketing campaigns. The data collected by AppsFlyer includes data such as IP Address, identification of the advertising campaign, app event data such as first app launch and settings	https://www.appsflyer.com/privacy-policy/

	Cleaner (AVG Cleaner) Cleaner Xperia (AVG Cleaner for Xperia) CCleaner Android (Piriform CCleaner)		and device info. Access to this data and its protection is governed by the AppsFlyer privacy policy. Data necessary for the identification of a marketing campaign and evaluation of its success is also shared with respective advertising providers. You can opt out of AppsFlyer Analytics tracking by changing the privacy settings within your app (Third Party Analytics switch) or by following the instructions available in AppsFlyer's Privacy Policy.	
Adjust	**Mobile:** Avast Family Space Avast Companion	Adjust	Adjust is a third party SDK which also provides install attribution capabilities. Like AppsFlyer, it is used to measure the performance of marketing campaigns. The service collects data	https://www.adjust.com/terms/privacy-policy/

			including IP address, the device's advertising ID, and some in-app behavior, such as product activation and purchasing. You can opt out of Adjust tracking from the Personal Privacy section of Settings in the app.	
Facebook Analytics	**Mobile:** SecureLine (Avast VPN) HMA! VPN (Privax VPN) AVG Secure VPN (AVG VPN) Mobile Security (Avast Antivirus) (deprecated in newer versions) Cleanup (Avast Cleaner) Cleaner (AVG Cleaner) Cleaner Xperia (AVG Cleaner for Xperia) CCleaner Android (Piriform CCleaner) Gallery (Flavyr Media Gallery) Battery Saver	Facebook	Facebook Analytics is primarily integrated into the older versions of our software and the newer ones no longer use it. It helps us understand the makeup of people who engage with our app by logging events from the app via Facebook's Android SDK. This tool enables us to observe how many users install the app, how frequently users activate the app, how much time users spend using it, and other	https://www.facebook.com/about/privacy https://developers.facebook.com/docs/analytics/overview

	(Avast Battery Saver) Alarm Clock Xtreme Free (AVG Alarm Clock) Alarm Clock Xtreme Pro (AVG Alarm Clock)		demographic information which helps us better understand how users interact with our product.	
HockeyApp	Mac and iOS products Avast Mobile Security (Avast Antivirus) SecureLine (Avast VPN) HMA! VPN (Privax VPN) AVG Secure VPN (AVG VPN) SecureMe (Avast VPN) Passwords (Avast - Mac and iOS)	Microsoft	We use this analytical tool only in older versions of some of our applications, so if you have not updated yours in a while, it is possible it is integrated in the application. We use this tool for the purposes of beta distribution, crash reporting, user metrics, feedback, and internal workflow integrations.	https://privacy.microsoft.com/en-us/PrivacyStatement
Mixpanel	**Desktop:** Avast SecureBrowser	Mixpanel Inc.	Our apps use Mixpanel to allow us to understand how our users use and interact with our products and how to improve our products, in particular from	https://mixpanel.com/legal/privacy-policy/

			a user experience and interactivity perspective. In this respect, we process data concerning events, timeframes (intervals within which the events took place), lengths of interaction, location (country-level) and similar necessary information. We do not use this analytical tool to process any information which can be used to identify you (such as your name, address, e-mail address, etc.).	
Logentries	**Desktop:** CCleaner Defraggler Recuva Speccy CCleaner Mac CCleaner Cloud	Rapid 7	Logentries is a cloud-based repository where we send multiple logs from our desktop apps to logentries such as activations and installer logs and update check pings. This allows us to search the	https://www.rapid7.com/privacy-policy

			logs and run queries on the data for the purposes of tracking errors, fixing bugs and resolving technical issues, as well as compiling generic statistics on, e.g., user, install or activation count and understanding how you use our products. We also log parameters from a device to check if they are eligible for certain installer offers, such as Chrome or Avast. This tool uses unique identifiers of the installation and device. These unique identifiers contain IP addresses, but we hash this data and do not keep it in its original form as soon as possible (usually within 30 days) when data gets stored.	

Loggly	**Avast Omni (IoT)** **Desktop:** CCleaner Cloud	SolarWinds (Loggly)	Loggly is a cloud-based repository where we send errors logs from CCleaner Cloud so that we can search, filter and query the data and receive alerts. Loggly is used to display error messages from our log files. We gather error messages from each agent log file and send them to Loggly, which analyzes it. We use this tool to find common errors in our applications, identify new errors which may occur, determine our business performance and identify geographical areas in which we can improve. Each entry in Loggly has a computer ID, but it does not contain any information which can	https://www.loggly.com/about/privacy-policy/

			personally identify you.	
Amplitude	**Avast Omni (IoT)** **Mobile:** Avast Family Space Avast Companion	Amplitude	Amplitude is a third party analytics service used to observe user behavior in the app in order to help us improve the product. We also use it to track, diagnose and improve technical performance, such as monitoring user-generated commands as they pass between various endpoints on the way to another device assigned to the same family. You can opt out from the personal privacy settings in the app. This is controlled from each device, so changing these settings on one device does not affect other devices or users in the family.	https://amplitude.com/privacy

Specific products for your PC collecting your Service Data

Avast and AVG AntiVirus & Internet security products & services

Our AntiVirus and Internet security products require the collection of usage data to be fully functional. Some of the usage data we collect include:

· potential malware threats to your device and the target of those threats, including copies of files or emails marked as potential malware, file names, cryptographic hash, vendor, size, date stamps, associated registry keys, etc.;

· information about how you use our products and their features, including data about your particular device, installation and uninstallation rates, language, technical parameters and manufacturer of a device, device security information (password attributes, encryption level), etc.;

· information about where our products and services are used, including approximate location, zip code, area code, time zone, the URL and information related to the URL of sites you visit online; and

· we collectively call this information “Clickstream Data”

We use this Clickstream Data to provide you malware detection and protection. We also use the Clickstream Data for security research into threats. We pseudonymize and anonymize the Clickstream Data and re-use it for cross-product direct marketing, cross-product development and third party trend analytics.

Avast CommunityIQ

Avast CommunityIQ is a threat monitoring service. Information about a threat detected in your device is sent to our server, so we can observe how the threat spreads and block it. This is vital for the functioning of our service and our ability to keep your device secure.

When you download our products and services, you will automatically be opted into our CommunityIQ, and your device is able to provide security-related information when needed. You may choose to opt out via product settings. By remaining in our CommunityIQ, you actively help yourself and others in the Avast community to experience a higher standard of security.

Our security experts process the data acquired by our CommunityIQ to update our databases of viruses and infected websites, and for historical and statistical purposes to understand where the threat is coming from, the levels of threat per country, how many persons visited the malicious website and the number of people we protected. We process this data for the purposes of antivirus functionality and to protect your device.

The data is collected from your entire submission process online. For both desktop and mobile users, this includes URLs of visited websites, IP Addresses, approximate geolocation of user or Internet Service Provider (ISP), device IDs together with the information on the nature of the detected threat. We collect this information to ascertain the source of the infection.

Geolocation gives the approximate location, for example, the latitude and longitude of the IP Address. However, if you access a malicious website while using Wi-Fi, then your IP Address can be location data. Depending on your ISP, your IP Address may indicate an exact location or the location of the ISP office or your location at a country level.

We may provide a method for manual submission of suspected malware, or a way to add more information about the source of an infection. Files and information submitted through this process will be retained as long as is necessary for security research and providing you protection.

Avast File Reputation Service

FileRep is a database of executable files sourced from users who participate in the service. The files (or their hashes, that is, de-identified versions of the files) are stored and evaluated for the purpose of determining which are infectious and updating virus databases.

Your participation is voluntary, and the data is stored in a way that limits its potential to be associated with individual users, for example, by hashing so the data is anonymous. This means it can be personally identifiable data if reversed by a “key”. However, the risks are lowered. In participating, you actively help yourself and others to experience a higher standard of security.

If you do not want to participate, you can opt-out by unticking the box ‘Enable reputation services’ in the general settings menu.

CyberCapture

CyberCapture is a feature in our AntiVirus that detects and analyses rare, suspicious files. If you attempt to run such a file, CyberCapture locks the file from your PC and sends it to the our Threat Lab where it is analysed in a safe, virtual environment. You are notified when the analysis is complete.

Currently, CyberCapture triggers when you run or download suspicious files from the Internet that CyberCapture has not previously encountered. We plan to expand this condition in the future to cover more sources.

CyberCapture is able to handle large files, but it may take longer to deliver such files to the Threat Lab. All files are uploaded over an encrypted connection, which means your data is inaccessible to hackers.

When CyberCapture is enabled, we collect information about you, your device IDs, your operating system, for example, whether you are using Windows 10 or XP, and we know your approximate location, usually at the country level.

CyberCapture is enabled by default in the latest version of our AntiVirus. We strongly recommend that you keep CyberCapture enabled. If you would like to disable CyberCapture, open the product user interface and go to Settings.

Avast CleanUp

CleanUp is offered as a Windows program. It removes unneeded files, registry entries, broken shortcuts and other similar items. It also provides system tuning features like program deactivator. For it to function, we process and store the following:

· originating IP Address; scanned systems history including data about operating system, patch level;

· system health, hardware information (including CPU), graphics card information, hard drive information;

· system data information, which is a list of computer software installed, directory listing of software, registry name and entries, registry hives and executables; and

· other operational data, for example, errors and error messages.

We use this data for operational purposes, and to provide you with a fully functional service.

Avast Secure Browser

In the default setting, our Secure Browser will process:

· your IP Address;

· the GUID number assigned to your installation of the Browser;

· cookies usage data; and

· browser extensions.

We use the data we collect to provide the Browser's functionality, to monitor performance and to improve our services. You can access and manage key privacy features from the Secure Browser's settings:

Browser Security & Privacy Center

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

Anti-Phishing

This blocks malicious websites and downloads to help prevent your personal computer (PC) from becoming infected with viruses, spyware, and ransomware.

Privacy Cleaner

This cleans your browser history, cached images, cookies including both first-party and third-party cookies, and other junk with just one click, to keep your activity private and free up disk space.

Stealth Mode

This 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.

Avast Secure Browser will also process the following data locally on your PC:

· your browsing history;

· personal information and passwords;

· a list of permissions;

· thumbnail-sized screenshots of websites that you visit;

· cookies or data from websites you visit;

· data saved by browser extensions and add-ons;

· data on what you downloaded from websites;

· data imported from other browsers; and

· bookmarks.

You can manage the data stored locally on your machine in the Browser settings. Data stored locally on your machine is not collected by our servers.

You can manage this information in several ways:

· you can delete your browsing history, cookies and site data by visiting the Security & Privacy Center and using the 'Privacy Cleaner' tool;

· you can stop our Secure Browser from accepting cookies from publisher websites by ensuring that 'Anti-Tracking' is turned on from within the Security & Privacy Center;

· you can modify the cookie setting policy under the us Secure Browser Settings by going to Settings/Advanced settings/Security & Personal Privacy/Content settings;

· you can review stored passwords using the Secure Browser default password manager in the Secure Browser Settings. Go to Settings/Advanced settings/Passwords and forms/Manage passwords; and

· you can view and manage your stored Autofill information in the Secure Browser Settings. Go to Settings/Advanced settings/Passwords and forms/Autofill settings.

Avast Passwords

Avast Passwords is a feature that stores user passwords and notes under a single master password or fingerprint and permits the user to log on to multiple sites using a unitary sign-on credential.

On Windows, our Passwords forms an integral part of the AntiVirus, which can be activated by the user by either performing a smart scan or by opening the feature in the product menu. On other platforms (Android, iOS and Mac) Passwords is a standalone program.

When activated, Passwords will check whether you have stored any passwords via your browser and will suggest you move these passwords to Passwords, so they can be stored securely.

When you choose to do so, Passwords will upload these passwords and remove them from your browser. Please note that the browser check happens locally on your device and none of your passwords are sent to our servers.

Your passwords and other personal data are stored locally on your devices and encrypted by the Passwords app.

However, when you choose to activate the optional feature "Synchronisation & Backup" to synchronise and backup your passwords across all your devices, you are required to create an account. Your personal data, that is, your passwords and notes, which may include credit card details, will be backed up on our remote server in a securely encrypted form, readable only via a "master key" on your device. Thus, it cannot be decrypted by us.

The data collected by our Passwords is necessary to provide the product functionality.

Identity Guard/Passwords/HackCheck

This functionality works in a number of ways. It allows you to check whether the passwords to your online accounts have been compromised. We are able to do this by searching through the database of leaks which we know about. You can do this through a number of our products which have this functionality.

· Hack Check – Hack Check is our website where you can check your leaks simply by entering your email. You will then be sent the results of the check to your email. Our service will then also send you periodical emails as to whether

we have learned that your credentials have leaked. You can unsubscribe from receiving these messages by clicking the unsubscribe link in the footer of these emails.

· Identity Guard – Identity Guard is a function within Avast Mobile Security where you can enter an email address and get back feedback on whether or not your credentials have leaked. The functionality also stores e-mail addresses with respect to which no leak was detected, and will notify you if we learn that your credentials leaked at a later date.

· Password Guardian – Password Guardian is a function within the Passwords product. When you store your credentials in the Passwords product, in an encrypted vault, we will notify you if we learn that your credentials have leaked elsewhere.

Antispam

Antispam is a product functionality that is designed to protect you against unwanted emails (spam). The software may collect information contained in emails reported by you as spam or identified as spam by a third-party tool (Mailshell). When you report an email as spam, the email is sent to the third party. Your consent is required for each of these submissions if you use the default setting.

We do not collect, use or store your personal data. We do not share your software or device ID or any of our generated IDs with the third party. In general, Mailshell does not have information about individual users or devices and is not able to connect any information to you. If you wish to know in detail what data Mailshell collects from you, please go to their website.

Avast SafePrice

When you use SafePrice, information related to certain shops or products, URLs, the installation GUID, a timestamp of the offer, purchase, product name and number, merchant's name, product links, prices and the categories of your purchased items, location at country level will be collected or transferred to us.

This information is used to retrieve available offers, for example, coupons or cheaper prices from third parties partnering with us. We request offers anonymously from those third parties and will not transfer or disclose your personal data to them.

At this stage, you do not communicate with the third party, only with us, and we do not forward any information to the third party except your country level geolocation and language. We do not give them your personal identifiers, so no emails and no names.

The third parties may use cookies in relation to the services they provide on or via SafePrice. For example, when you click on an offer presented within the product, a cookie may be placed on your computer. Third party/third party's partner/service provider sites, offers and/or cookies are not controlled by us and are not subject to this privacy policy.

In the end, you buy directly from the seller. We do not have access to your credit card details as you deal directly with the third-party companies.

Avast BackUp

The Avast BackUp service is provided by a third party under contract with us, and the privacy policy, terms of service, and EULA of the third party apply to any information that users provide in connection with the Avast BackUp service.

Avast BackUp provides backup and storage capabilities for personal data that otherwise would reside only on your computer's hard drive. For the BackUp to work, data on your hard drive must be transferred to a centrally hosted site

so that it can be "backed up."

If your hard drive contains personal information, that information will be transferred to the host site for storage and subsequent retrieval. Techniques used to protect this information during storage and transmission are described below.

Avast Omni

Avast Omni is a connected device and suite of products aimed at providing you comprehensive security in your home and for your entire family. It has the following features:

(i) Home Network Security - this is the feature aimed at protecting your whole home network as well as your individual devices from threats such as various types of malware, DDoS attacks or smart home hacking. Upon activation, OMNI will become a hub of your device network next to your router, through which all traffic from your connected devices will be redirected. In order for it to work, it needs to process device data and service data about the network and devices connected to it and data concerning traffic, including but not limited to: information concerning your devices (such as device ID, OS and its version, model and manufacturer), the network and connections made (are you connected to WiFi or broadband, connection speed, etc.), URLs of the websites you visit, as well as certain metadata concerning the files you download or some fragments of the underlying network traffic (although we will, under no circumstances, access the contents or decrypt it); and

(ii) Parental Controls, which is a feature that functions in the same way as our standalone "Family Space" product.

We process this data in order to provide you with the Omni's functionality, in particular, to detect threats to your network and devices. We further use this data in order to understand how users use and interact with our product through analytics conducted either by us or by our analytical tool providers.

In order to use Omni, it is necessary that you create and manage your Omni through an Avast Account. All of the above device data and service data will then be linked to your Avast Account.

Service Data specific to CCleaner Desktop Apps and Other Products

All Piriform desktop apps receive usage data via log files. We collect usage data such as your device ID, your browser type and version, your operating system, your IP Address and information on software you have installed as necessary for the functioning of your Piriform desktop apps and to check if you qualify for any installer or in-app promotions we may market. The collecting and processing of your usage data is automatic once you install the app.

Desktop apps

CCleaner Mac

CCleaner for Apple Mac cleans and de-clutters your hard drive, makes your operating system run faster and helps make your browsing on the internet more private and secure.

Recuva

Recuva is a windows app that allows you to search your hard drives and USB drives and recover any deleted files (if deleted with standard windows deletion).

Speccy

Speccy is a windows tool that allows you to receive an audit of your computer hardware and software. You may publish this information to an online page if you wish to share. The audit does not include IP Addresses (http://speccy.piriform.com/results/HSP0RYoxXz3SniCDtOLxcJN).

Defraggler

Defraggler allows you to optimise your older hard drives so they run faster.

Software as a Service (SaaS) Product

SaaS products allow you to connect to and use cloud-based apps via the Internet.

CCleaner Cloud

CCleaner Cloud is offered as both a free and paid version. The platform allows users and businesses to remotely manage their computers centrally from the platform.

For free users, we collect personal data including your name, email address, IP Address and computer events, for example when you install software. This data is necessary to provide and improve our services by connecting this data with the usage logs. For Professional and Business users, we collect the same personal data as for the free user and additionally, we may collect your company name, billing information and mobile number. The data is necessary to complete the contract when you subscribe to our services.

Business-only Product

CCleaner Network

CCleaner Network is a business-only product that is installed locally on your server and allows you to manage and clean your company's computers. We do not receive any data as this is a local-only closed network product.

Service Data Specific to Your Mobile

Avast and AVG Products & Services

In the sections below, we look at what data is collected when you use AMS, AVG AntiVirus and AVG Protection for Xperia, in addition to variations of these apps developed specifically for tablets or alternative app stores.

When you first run these apps following installation, you have the option to subscribe to use the paid version. If you stay on the free version, we will serve third party ads; if you do not want to view third party ads, you may choose the paid version. Whatever your choice, your service data is not connected to your Billing Data, because there is no Billing Data for free users and for paid customers, as described above, your Billing Data is collected only by the app store where you purchased the product.

If you use the free version of our apps, the services are supported by third party ads. Choosing to install the free version means data such as your IP Address will be provided to the third party ad server.

In some instances, Avast Mobile Security (AMS) or AVG AntiVirus may come preinstalled on your mobile device upon purchasing it from the store and you can deactivate them within the product Settings – Personal Privacy.

Web Shields

Web Shield Lite is on by default and is only effective on some browsers and Android operating system versions. When enabled in a supported configuration, the app reads URLs from the browser in realtime and sends them to our server via the URL information service. We check the URL against our database of known threats and then display an alert if the URL is a known threat.

Web Shield with Accessibility is off by default. You need to grant Accessibility permission to activate this feature. While it is the same service as Web Shield Lite, it is capable of checking URLs in more browsers and operating systems. The list of supported browsers and operating systems sometimes changes due to the development of or changes to third party services.

We may use anonymous browsing data for third party trend analytics. All users may turn off data sharing in product Settings – Personal Privacy.

Avast AntiTheft for Android

AntiTheft is a function within AMS. It is off by default. When you choose to turn it on, you can request location on demand from my.avast.com or through SMS commands from another phone. AntiTheft is designed to protect data residing on your mobile phone in the event of theft.

For AntiTheft to function, we must collect and store information about your phone and its approved users. The types of data we collect include the following:

· a list of approved SIM cards;

· a phone number to notify you in the event of unauthorized SIM card replacement;

· a number where calls and messages can be forwarded in the event of theft;

· your mobile's unique identifier or International Mobile Equipment Identity (IMEI) when you activate AntiTheft.

We use this data to locate and identify your lost device, and to help you report the lost device to police and cell phone carriers. If the phone was stolen, it may block the thief from using the device. The collected data is used to provide you the functionality.

Last Known Location is a feature within AntiTheft, also off by default. When you activate the feature, we send more frequent location updates to the server to help you track your device's last known location.

Avast Call Blocker

The Call Blocker feature is only available on Android versions below 9.0. This paragraph does not apply to Android 9.0 and above. Call Blocker is a feature of AMS which allows you to block unwanted callers. It is off by default. When on, we build a database of SPAM callers by analysing patterns of high volume callers across our user base.

When you (an AMS user) call a third party, or a third party calls you, we will have the following record in our database: the third-party phone number, the time of the call, and an anonymous key code number assigned to this particular record. This allows us to count the number of calls made to a specific recipient in order to evaluate whether the call is a spam or not. Your GUID is disconnected from this data.

We do not collect the phone numbers of our users. Therefore, the data we collect from you is anonymized and we are not able or intending to trace the call record to you.

However, we are able to see the phone numbers of third parties who called our AMS users in general or which phone

numbers were called by our AMS users.

The purpose of this data collection is to identify high volume callers; therefore, we look at aggregations, not at individuals. You may shut off this feature in your discretion via the product Settings.

Avast Wi-Fi Finder

Avast Wi-Fi Finder for Android provides information about free hotspots. It is based on crowdsourced data, meaning that every user has to willingly contribute to the database.

We use the data collected for sharing with other Wi-Fi Finder users. You may turn off data collection by not using the WIFI sharing feature. We collect this data:

· the location of the device when you use “submit a hotspot”;

· names of hotspots you submit to the database;

· some technical information about the network (speed, signal strength, security assessment, and frequency

· mac address and IP Address of the device;

· the install GUID and hardware identifier; and

· hotspot passwords.

In some Android versions, we need your location permission to scan Wi-Fi networks for security threats. Any time we’re given the location permission, we may use it to refine our databases of Wi-Fi networks, including the locations of Wi-Fi hotspots and dangerous networks.

Avast Battery Saver

The Battery Saver is an app that helps you monitor what apps are running in the background, speed up your mobile device, and save the battery. We collect AppInfo for the purpose of delivering this feature.

Battery Saver has a functionality, Smart Profile that can switch your device setting automatically to preserve the battery upon an event you set up, for example, when you come home. In doing this, you have to reveal your location Wi-Fi or give us permission to use your Android mobile operating system’s location so that the event can be triggered. This data is stored locally on your device and is not transmitted to us.

We track the usage of this feature via Google Analytics, so we would know the demographic and geographic statistics of our users who have enabled Smart Profile. We do not have information on the individual user. As Google is a third party, the third-party privacy policy applies.

Smart Profile is enabled by default, but you may disable this via product settings.

AppInfo

AppInfo is an Avast library used in our product features such as App Insights, for the purposes of displaying how much time is spent on the device, broken down by app, by total data, and by day; enhancing our cloud based threat detection; improving other Avast products; for Avast marketing; for third party ads; and for analytics. To this end, it analyzes device information such as: language; make and model; operating system version; telecom provider; and city and country. Additionally, we observe the list of currently installed apps; the time when an app is installed or removed; the source of an installed app; Wi-Fi and carrier data consumption per app; time that an app is in the foreground;

battery and CPU consumption per app; and which permissions are granted to each app. The specific scope of information collected is dependent on permissions granted to the app. We may share statistical data that has been anonymized and aggregated geographically and so, cannot be used to identify individuals, with third parties for trend analytics. You can always turn off the specific features which use data from the AppInfo library in your settings, or change your preferences for the processing of this data in the privacy settings.

Avast ApkRep

We use the ApkRep to build a database of Android apps sourced by users of AMS. We collect and store hashes of app files together with the installation GUID, as well as metadata about the apps (e.g. application package name, application signing certificate information, source market identifier and file size). We process this on the legal basis of our legitimate interests in analysing your data to find infectious apps and to update our virus databases, which is necessary to continuously improve AMS to keep you secure.

Avast Android CleanUp, AVG Cleaner, AVG Cleaner for Xperia, and CCleaner for Android (Piriform)

Avast Android CleanUp, AVG Cleaner, AVG Cleaner for Xperia, and CCleaner for Android (Piriform) access your device storage to delete data that is not in use. You will be asked to allow your Android operating system to access your device storage. The feature sees what's in your device, for example the apps and files you have downloaded, ranging from your music playlist to photos. However, everything takes place locally on your device and nothing is transmitted to our servers.

Since we do not collect or store any personal data, any data collected is anonymous.

We also offer you a Cloud service connection for you to back up your files so nothing important gets deleted. You may sign-in to Google Drive, Dropbox or Microsoft OneDrive directly from CleanUp. This feature is optional. If you use this feature, you will be storing your files with a third party and thus this is subject to the third party's terms of service and privacy policy.

Avast Family Space

Avast Family Space (for parents) and Avast Companion (for children) are mobile applications available for Android and iOS. Family Space provides the following functionality:

(i) location monitoring - this feature monitors the location of connected devices using their GPS location. The administrator (parent) can create and save locations such as "home", "school", "gym", "friend's house", etc., and receive alerts when the connected device (child's device) arrives or departs a saved location. This feature also allows the parent to see the child's location on demand, receive scheduled updates about their current location, and see their location history. The connected device also has the option to share its location with the administrator's device and with other connected devices. The connected device may also request the information of other users in the family. The parent may set permissions in the connected device, which will enable or disable the sharing of information from the child's device. This particular feature and its functionality may, however, be affected by the scope of permissions granted by the specific user. For example, if the parent does not grant the permission to access their location, the ability to share this information would be limited.

(ii) content filters - this feature blocks the connected device from accessing blocked content (apps and websites). This setting is set by the parent (administrator) through the application in their device.. Filter defaults are suggested based on the age range of the users of the connected device, which can be selected and further modified by the administrator.

(iii) insights - this feature allows the administrator to monitor the connected device's access of named apps or devices. The feature also provides activity summaries from the connected device and location history. Additionally, administrators can set pause on internet access and set time limits on the connected device.

Avast processes only the data necessary to provide this functionality. This data is processed in Avast's cloud service environment. This processing includes the following categories of data for both the administrator's device and the connected device: (i) Account Data of the parent (administrator), (ii) Information about the users of the connected device which the administrator chooses to input into the application, such as names, age range or photos, (iii) location data of the devices; (iv) information concerning app usage history and content engagement, including names of apps, names or categories of blocked content and time limits; (v) device and network information.

Avast Mobile Campaign and News Feed

From time to time, we will run mobile campaigns. The goal of our campaigns is to show messages to you to promote various features of our apps and offer discounts on paid features. We use three kinds of messaging formats:

· Notifications

· Overlays

· Purchase screen

Here are some examples of general events which we use to trigger messaging:

· First launch

· App installation

· Subscription changes

· Features changed

· Trial changed

· Seasonal events (such as national holidays)

Each app can also define its own events, for example:

· EULA accepted

· AV scan threats found

· App update

· Safe clean

· Low battery

Apart from campaigns, when you use our apps on your Android, you will receive news feed from us, for example, once you complete a virus scan or CleanUp process, you are directed to a result screen that offers a Facebook-news-feed-like experience.

Each feed has multiple cards. You can scroll the feed vertically. Each card has its own function. We may offer information or tips, promote our apps or guide you to a screen, application, Google Play or web page when you tap on the card. We also display third party advertisement cards to free users.

We use our servers to download relevant content for you, so we will transmit some of your data in the request, for example, your hardware ID, the install GUID, and device information like language, vendor, model, and android version. Your data is used to deliver content, which is relevant to you.

AVG Alarm Clock, Open Weather and Taboola

AVG Alarm Clock

When you install Alarm Clock, which is an app that you can set to wake you up, you will also receive by default, weather (via Open Weather), news (via Taboola), and third party ads via regular ad SDKs. You may opt out of receiving news and weather reports via Settings – My Day Dashboard.

Through Alarm Clock, we collect and process anonymous statistical data in our own analytics system and we share pseudonymized or anonymised data with third-party analytics and crash reporting. We collect only the personal data necessary for us to enable our third-party providers to send you relevant information. You may opt out of third party analytics through Settings – Personal Privacy.

Open Weather

You receive weather information from Open Weather, our third-party service provider. This service is on by default and we share your approximate location data, so you will receive relevant weather forecasts, for example, East Coast, USA. However, if you wish to have the weather forecast for a specific location, for example, Brooklyn, New York, you have to turn on this setting. Apart from Alarm Clock, you can receive Open Weather on your charge screen when you install AntiVirus, Cleaner and Battery Saver.

Taboola

Alarm Clock will also show you news articles from Taboola, our third-party news aggregator. We share some of your data with Taboola, such as your IP Address, your device, browser and operating system, your hardware ID, news websites you visited and your preferred language, for you to receive locale specific news.

AVG Gallery, Gallery Doctor and Photo Cleaner for iOS

AVG Gallery

Gallery is a smart app that you can install in your Android to help you organise your photos and videos into significant moments. Through Gallery, we collect analytics data in our internal analytics system, and through third party analytics like Google Analytics and third party crash reporting (Crashlytics).

AVG Gallery Doctor

Gallery Doctor is a free app that helps you free up storage space in your mobile by identifying bad & similar photos in your Android gallery. It does not collect any personal data.

I. Accounts

There are a variety of accounts you can create with us.

Account data is the data you give when you open an account or request a service from us and may including your

name, address, email address, phone number, photo, date of birth, gender, and interests (collectively, “Account Data”). Account Data may include the same data as in your Billing Data (such as name and email), but Account Data is not connected to your credit card number and, except in a few instances described below, is not connected to your Service Data. We process this data in order to provide you with the relevant account.

Examples of Accounts and Services

Avast and AVG Accounts

Avast Account (id.avast.com) and AVG account (my.avg.com) are tools which permit you to register multiple products using a single registration and authentication system. If you use these Accounts, you will be asked to provide your email address directly or indirectly via social media login. This is used for authentication.

Opening an account is voluntary. For paid and trial customers, there is the convenience of managing your licenses and seeing your connected devices in My Avast portal.

Once you delete your account, your Account Data will be deleted, but this will not delete other records of your name or your email address stored with us.

Some products may require you to establish an Avast Account for the provision of the service or to provide the product functionality. For example, Avast anti-theft products will sync your personal computer and your mobile device, so if you lose your mobile device, you can track it on your personal computer. For forum.avast.com and business.avast.com, you likewise need an account. For product features to be enabled and functioning, you must have an Avast Account.

For myaccount.avg.com, this is a legacy account that was used for subscription handling and had features such as permitting users to download copies of their invoice(s).

For HMA!, users can manage a list of their product subscriptions, as well as some specific VPN features, and see a list of VPN servers.

Website Product Registration

To register as a customer of our paid AntiVirus products, you are required to provide your email address and select a password. For desktop users, you may register online on the website. We process this information to validate and verify the number of current licenses in existence. We may also use it to verify that copies of our product are legitimate, and not counterfeit. You may voluntarily submit additional information such as your name, demographic information, or other personal information.

In-Product Registration

Instead of website registration you may select "Registration form" from within the product interface. On the registration form, you provide your email address and select a password. We may also ask general demographic questions such as your level of computer experience or your prior AntiVirus program. You may voluntarily submit additional information such as your name, demographic information, or other personal information.

Registration and Log-in via Other Mediums

It is possible to use Facebook or Gmail to register the Free AntiVirus and to log-in to your Avast Account.

If you choose Facebook or Gmail for registration and sign-in, you will be asked to share certain personal data from

your Facebook or Gmail account with us. We collect and store personal data you provide such as your email address, name, avatar (main profile picture) and the identifier of your Facebook or Gmail account.

One of our website features is the "Community" section, which includes a comments area, links to user pages, links to blogs, links to the Avast Forum, and links to third-party sites such as Twitter and Facebook.

You may post a general comment in the "Overview" section of the "Community" pages using your Avast Account or via Facebook or Gmail. The user ID that appears beside your comment will be the user ID from your Facebook or Gmail. If you have a profile photo connected with this user ID, that photo will appear beside your user comment.

Avast Forum

The Avast Forum is accessible from the AVG Support Community pages or via a link on the "Support" section of our website. Certain features require registration by you.

If you decide to register by creating an Avast Account, you will be asked to select a username, password, provide an email address and physical location. Disclosing your physical location is optional. You may allow other users to send you messages and you can log in to your account via Facebook or Gmail.

Once registered for the Forum you may control your privacy settings when using the Forum by visiting your "Profile" page. You can modify your settings at any time. You can also view your past posts, usage stats, password settings, and user profile as seen by others.

You have the option to provide additional information such as personal texts, disclose your birth date, identify your gender, instant messaging number, messenger username, or website name and address, disclose your physical location, and select an avatar or personalized picture. Any information you provide here will be visible to other users.

The following minimum items of information will be available to all users, regardless of your profile settings: your username, your total number of posts, and posts per day, the date and time you registered, your local time, and the date and time of your last activity.

Where you submit your personal data for publication, for example, via the Avast Forum or our Community pages, such data will be made available publicly.

Facebook Posts

If you choose Facebook as your registration or sign-in method, your permission will be sought for us to take certain actions on your behalf.

Specifically, we will request permission to post on your behalf where:

· you register or install a product;

· you update a program; or

· a program protects you from visiting an infected website.

Examples of what might be posted may include the following, or similar messages:

(1) “Avast AntiVirus just saved my computer from infection! Try it now. It’s free.”

(2) “My us AntiVirus just updated, with powerful new security features. Download it for FREE. You’ll love it.”

(3) “I just installed us AntiVirus for free. I really like it. If you want the best protection, download us like I did.”

You are not obliged to agree to allow us to post on your behalf and you may “skip” this state during registration.

You can modify your posting preferences at any time via my Avast Account (https://my.avast.com/en-us/facebook).

Contact Us

There are many opportunities to contact us via our website. There are links that allow you to reach us by email via the Support page, by clicking our media contact or news subscription buttons, or by requesting online service or support. In general, the amount of information that we collect when you contact us will be in proportion to the nature of the contact. For example, if you contact us by email, we will require your email address to reply.

Newsletters and Blog Notifications

We offer news and information on our website, including email newsletters and blog notifications of current news items. This is a free service we provide to you. You may receive an ad banner on our website promoting a news story. However, you must subscribe if you wish to read it.

We may use your email to send you information on other publications or our other products or services.

When you subscribe, we request your first and last names, email address, and country of residence. We process your personal information to help develop content that is interesting to our audiences and to send you relevant blog notifications and/or newsletters.

You are free to cancel your news subscription(s) at any time by visiting www.avast.com/news-subscription.php?page=unsubscribe

"Refer A Friend"

There may be times when we post a "refer a friend" link that allows a site visitor to send a message to a friend about an Avast product or service. We will never request that our users provide a friend's phone number or other contact information. We do not have any record of the email address that you use to send the message. It is up to the friend to install.

Sometimes the friend referral takes place when you install a product. When the friend installs, we collect the GUIDs and information that your two installations are connected.

This concludes the description of personal data collected by us when you purchase products and services or when you register for an account or request services. The next section covers the data collected by us from the installation and during the running of our products and services. We call this Service Data.

J. Live Events and Competitions

Aside from interacting with you by way of your use or purchase of our products and services, we may collect your personal data from you directly, when we attend trade shows or when you participate in our promotional events or competitions.

When you interact with us at trade shows and provide us with your personal data on a business card or through other means (for instance, through registering for an event we are holding at such trade show), we will be processing your personal data for the purposes of building and expanding our database of existing or prospective business partners. We will use this contact information in order to communicate with you about possible business partnerships or other

similar opportunities, and to promote our brand across the industry (serve our legitimate interests).

Live events and competitions held and organized by us generally require that you register first. To complete a registration, you provide us with your name, your e-mail address and other relevant information, which is marked as “Required” (this could, for instance, include information about your technical background, if you are registering for one of our competitions). We may also take photos or videos of the competition.

Provision of live event(s) and competition(s) data is voluntary. However, if you do not provide us with the information marked in the form as “Required”, you will not be able to participate. We will also sometimes process information about your social media accounts (links to your Twitter, Facebook or other social media accounts), should you choose to provide them. Avast will process the “Required” as well as other voluntary information in order to assess your application, register you for the event and to communicate with you about it. We may use your image in photos or videos on our website or as part of our general promotion and marketing efforts. We will also use your email address to communicate with you about our new events and about other products and services from us.

Some of our competitions are carried out through social media or networks. In that case, the privacy policy of that particular social network will apply.

VPN Products Privacy Policy

Using a virtual private network (“VPN”) is like going undercover while you are on the Internet. We provide VPN services that allow you to be on the Internet anonymously and securely from anywhere in the world. While we respect your privacy and take strenuous measures to protect it, it does not mean that you are totally anonymous to us.

In this section of the Privacy Policy, we would like you to know what kind of personal data we collect from you or that you provide to us when you use our VPN services.

We treat this data differently than we do for other applications as it can be of such a sensitive nature, so we want you to understand clearly how we process it, on what legal bases, whether we transfer or disclose it, and how long we retain it, in accordance with relevant laws.

1. Personal Data Collection and Use

Personal data is understood as any information that relates to an identified or identifiable natural person, and includes the information you provide to us while using our VPN services.

More specifically, we may collect and process data about you in the following situations:

1.1 Account Creation and Management

If you create an account with us (note: this is necessary in order for you to use some of our applications or some of their functions), we will need some information about you. This is the data that is created and stored for the management of your account:

Account data	**What we use it for**
Email address	To send you purchase receipts, communications, and occasional product news

Username	To manage your account and facilitate your login into the service
License Key	To activate your subscription
Subscription renewal date	To tell us until when the account is valid
Trial User	To add a trial period before the account is charged

All of the above data is stored for as long as you use our service, as it is necessary for us to provide it. You can see all of this data by logging into our Privacy Preference portal.

1.2 Service Data from our VPN Servers

If you use our VPN service, we strictly collect the minimum amount of information needed to provide and operate our VPN service, as well as keep it running safely and efficiently. This is the data we collect to make sure our VPN infrastructure works ("Service Data"):

Service data	**What we use it for**
Timestamps of your connections	To manage the number of concurrent active connections, and handle abuse. Example: We use them to stop brute force password cracking attempts on user accounts.
The subnet of your originating IP address. E.g. We anonymize the last octet to protect your privacy: 92.143.234.000 We don't collect exact IP addresses that could ID you.	To plan for increased network demand and capacity. Example: Help us decide to add servers in a region if we see a rise in demand there, or help troubleshoot issues with a specific ISP.
IP address of the VPN server you're using.	To troubleshoot our service and plan for new network capacity. Example: Identify when an IP address suddenly doesn't work for accessing certain services, and act to resolve the issue.
Amount of data transmitted E.G. 5GB up or down	To plan for new network capacity and server improvements. Example: We may deploy more capacity to meet demand and make sure speeds stay up for all users.

We store this data on servers for 30 days, after which time it is deleted on a rolling basis — so data created on Jan 3rd gets deleted on February 2nd, for example.

1.3 Data we don't collect on our VPN service. Period

We do not collect, store or log any of the following data:

· Any complete originating IP address that could identify you.

· Any DNS queries while connected. We rely on our own secure DNS servers, so your queries are also protected from exposure to 3rd parties.

· Any activity logs: the applications you use, the services you use, the websites you connect to — basically anything you do online.

1.4 Service Data from our VPN Clients

In order to make sure our VPN clients do their job properly and improve them, we have to know how people, as a whole, interact with them. This data pertains to interactions taken in the app, and cannot be used to uncover what you're using the VPN service for.

Client Data	**What we use it for**
OS Version E.g. Windows 10	For user support, troubleshooting, and product development planning Example: Which platforms do our users most like to use?
Avast SecureLine VPN version E.G. SecureLine for Android version 4.1	For user support, troubleshooting, and product development planning Example: Is our latest update deploying well?
Application Events E.g. Turned on auto-connection, Uninstalled, etc. You can opt out of this in the settings.	To plan product development Example: Is a new client-side feature we introduced popular? Are people uninstalling after our latest release?

We delete this data on a rolling 2-year basis (i.e. data created on Jan 2, 2019, will get deleted on Jan 2, 2021).

1.5 Third-party Analytics In Our VPN Products

To analyze the application events mentioned section 1.4, and understand how our services function, or how stable or successful they are, we rely on our own analytics tools as much as possible. But sometimes, we need to rely on third-party tools that address specific issues in ways we don't have the ability to replicate. Whenever possible, we anonymize, masque, or in other ways try to limit your exposure.

Here are the third-party tools we use, how we use them, and their privacy policies. You will find that these tools are also listed under the broader section H. Service Data of this privacy policy which covers all Avast products, however in the interest of full transparency, we cover here in detail how the relevant ones are used for our VPN products:

Google Firebase Analytics on iOS and Android

Firebase helps us to understand how people interact with certain aspects of our applications. While Firebase normally relies on Android Advertising ID or iOS Identifier for Advertisers, we've opted to use our own anonymizing identifiers instead. Therefore it doesn't contain any information that could personally identify you. Still, you can opt out of providing us with this anonymized application performance data in our application settings.

Still, you can opt out of providing us with this anonymized application performance data in our application settings.

Google Fabric Crashlytics on iOS and Android

This Google service helps us to improve the application stability, pinpoint things that don't work, and improve your experience. Its implementation doesn't contain any information that can personally identify you.

Both Firebase Analytics and Crashlytics are subject to Google's privacy policies.

AppsFlyer Analytics on iOS and Android

AppsFlyer helps us understand how effective our marketing campaigns are by letting us know which ones directed you to us. The data collected here is subject to AppsFlyer's privacy policy.

You can opt out of AppsFlyer Analytics in the settings of our applications, or by opting out by following the instructions in their privacy policy.

Deprecated Analytics

If you're still on older versions of our applications, the following analytics are embedded in them. We highly recommend that you upgrade to later versions as they no longer use these:

· Facebook Analytics on older versions of our Android apps: we used to use this to know how many people opened an app, how much time they spent in it, and other information about how they interacted with them. You can find Facebook's privacy policy here.

· HockeyApp on older versions of our macOS and iOS apps: This was used to do beta distribution, crash reporting, user metrics, feedback, and more. This tool belongs to Microsoft and you can find their privacy policy here.

2. Where and how long we store your personal data

2.1 Where we store your data

When you use our service, you may be using servers located in a variety of different countries. However, there is a difference between use and storage. What little information that gets generated by your use of our infrastructure does not get stored outside of the Czech Republic.

There may be some instances where, as a matter of necessity, we need to transfer data outside of these two jurisdictions. When we process the data within our group, regardless of where we are, we always implement the same level of data protection afforded by the European General Data Protection Regulation to all personal data we process. Where we cooperate with third parties which are involved in data processing, we legally bind any party we deal with to adhere to those high levels of protection with standardized contracts approved by the European Commission, and to ensure your rights are protected in accordance with this privacy policy.

In all cases, we follow generally accepted standards and security measures to protect the personal data submitted to us, both during transmission and once we receive it. We always strive to protect your data to the maximum extent we can.

By using the service, you acknowledge this transfer, storing or processing

2.2 How long we store your data

Concerning storage or retention periods, the specific terms applicable to the various types of data used for various purposes are noted in their respective sections. After these periods elapse, we will delete this data and no longer use

it for that specific purpose.

These retention periods may be longer where it is necessary for us to comply with our legal obligations or legal orders, resolve disputes, and enforce our agreements, including in the court of law.

3. Disclosure of your VPN information

As a rule, we do not disclose any information to other commercial parties, with the following exceptions:

3.1 The Avast Group

As we are part of the Avast Group, information may be shared with members of the Avast Group in order to execute on the provisions of this service, for direct marketing, or to help our product development. In all cases, they are subject to the terms of this Privacy Policy.

3.2 Provision of services

It may be necessary to share some data with select parties to deliver the product or service you require — such as with a payment card provider who we use to process your credit card transaction, or to do perform website analytics. The information that is collected and shared with those parties is outlined above.

3.3 Legal requirements

In the event we are served with valid subpoenas, warrants, or other legal documents (for example, documents concerning the sale of all or part of our business or a merger), or where applicable law compels us to comply, or when we are required to defend the rights or property of the Avast Group, including the security of our products and services, and the personal safety, property, or other rights of our customers and employees — we may share your personal data as collected above.

3.4 Whatever the circumstance

“Avast does NOT store the originating IP addresses of our users when connected to our VPN service, and thus cannot identify users when provided the IP address of one of our servers. We are also completely unable to disclose any information about the applications people use, the services they employ, or the websites they visit while using our VPN. We simply do NOT store this information.”

Are you our business partner or a public relations contact? Find out more about how we use your personal data here

Worldwide (English)

Useful links

- Support
- Business Support
- Forum
- Affiliates
- Security news
- Paid Online Interview
- EU projects

The company

- Contact us
- Investors
- Careers
- Press center
- Technology
- Responsibility

- Avast Foundation
- Avast Blog

- Facebook
- Twitter
- LinkedIn
- YouTube

Privacy policy Legal Modern Slavery Statement

This might suit you better

AMERICAS

- Argentina
- Brasil
- Canada (English)
- Canada (français)
- Chile
- Colombia
- EE.UU. (español)
- México
- USA (English)

- América Latina (español)

EUROPE, MIDDLE EAST & AFRICA

- België (Nederlands)
- Belgique (français)
- Česká republika
- Danmark
- Deutschland
- España
- France
- Italia
- Magyarország
- Nederland

- Norge
- Polska
- Portugal
- Schweiz (Deutsch)
- Slovensko

- South Africa
- Suisse (français)
- Suomi
- Sverige
- Türkiye
- United Arab Emirates
- United Kingdom
- Ελλάδα
- ישראל
- Казахстан
- Россия
- Україна (українська)
- Украина (русский)
- المملكة العربية السعودية
- الدول العربية

- Europe (English)

ASIA & PACIFIC

- Australia
- India
- इंडिया (हिंदी)
- Indonesia (English)
- Indonesia (Bahasa Indonesia)
- Malaysia (English)
- Malaysia (Bahasa Melayu)
- New Zealand
- Philippines (English)
- Pilipinas (Filipino)
- Singapore
- Việt Nam
- 日本語
- 대한민국
- 中华人民共和国
- 臺灣
- ประเทศไทย

- Worldwide (English)