General Privacy Policy

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 so we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your personal data.

This Privacy Policy was last updated in June 2021.

Who We Are

This General Privacy Policy ("Privacy Policy") applies to the Avast Group (collectively "we," "us" or "our").

If you live in the European Economic Area, the Controller of your personal data is Avast Software s.r.o., which has its principal place of business at 1737/1A Pikrtova, Prague 4, Czech Republic, 140 00.

If you live in the United Kingdom, Avast's representative established in the UK is AVG Technologies UK Ltd.,110 High Holborn, 7th Floor, London, WC1V 6JS, England.

Privacy Policy Contents

This Privacy Policy describes how we handle and protect your personal data and the choices available to you regarding collection, process, access, and how to update, correct and delete your personal data. Additional information on our personal data practices may be provided in product settings, contractual terms, or notices provided prior to or at the time of data collection.

Please refer to our Products Policy describing specifics of personal data processing within our products and services.

This Privacy Policy is intended for you if you are a user of our products and services. If you are a business partner, the privacy notice that applies to you is located here: Business partner policy.

Personal Data We Process

Personal data refers to any information relating to an identified or identifiable natural person ("Personal Data").

We may collect data or ask you to provide certain data when you visit and use our websites, products and services. The sources from which we collect Personal Data include:

- Data collected directly from you or your device relating to an identified or identifiable natural person ("Data Subject"), and may include direct identifiers such as name, address, email address, phone number, and online or indirect identifiers such as login account number, login password, marketing preferences, social media account, or IP address;

- If we link other data relating to you with your Personal Data, we will treat that linked data as Personal Data; and

- We may also collect Personal Data from trusted third-party sources such as distributors, resellers, app stores, contact centers, and engage third parties such as marketing, survey, analytics or software suppliers to collect Personal Data to assist us.

We do not process special categories of personal data or deduce in any way this type of information from data we collect within our products.

We organize the Personal Data we process into these basic categories: Billing Data, Account Data, and Product Data.

Billing Data includes your name, email address, masked credit card number, license information and in certain circumstances, your billing address and your phone number. In most circumstances, you purchase our products and services from a trusted third-party service provider, reseller, or app store. In those circumstances, your Billing Data is processed by the relevant third party and we only receive a subset of this data to keep proper business records. In these instances, see below an example of Billing Data and what we use it for:

Billing data	What we use it for
Email address	To send you purchase receipts
Masked credit card number	To process the payment and billing records
License key	To identify a specific license for a follow-up actions such as renewal or troubleshooting
License type	To enable features based on the purchased license
Renewability	To check if a given subscription can be renewed
Date of expiry	To check whether a license is valid

Account Data includes information needed to set up and customize an account, such as your name, email address and username, and information connected with our services, such as license keys. For some of our products or some of their functions creating an account is necessary. See below an example of Account Data and what we use it for:

Account data	What we use it for
Name	To customize our communications by addressing you by your name
Email address	To send you communications regarding your license and support
Username	To manage your account and facilitate your login into the service
Subscription renewal date	To tell us until when the account is valid
Trial User	To add a trial period before the account is charged

An account is also necessary for some features of our **Forum.** You have the option to provide additional information within your account 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 (including 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).

Product Data includes two sub-categories:

- **Device Data** includes information about the operating system; hardware; city/country of device; error logs; browser; network; applications running on the device, including the Avast products; and

- **Service Data** includes information about the Avast product usage and events relating to use of our product by you such as samples, detections and files used for malware protection, information concerning URLs of websites, usage statistics (activation, crashes, scans, errors), IP address.

These sub-categories differ for each product and service. If you want more detail about Device and Service Data we process on a product basis, please refer to our Products Policy.

Why We Process Your Personal Data

We use your Personal Data for the following purposes and on the following grounds:

On the basis of fulfilling our contract with you or entering into a contract with you on your request, in order to:

- Process purchase of our products or services from us, our partners or our trusted third- party service providers' online stores;

- Provision the download, activation, and performance of the product or service;

- Keep our products or services up-to-date, safe and free of errors, including implementation of new product features and versions;

- Verify your identity and entitlement to paid products or services, when you contact us for support or access our services;

- Process your purchase transactions;

- Update you on the status of your orders and licences;
- Manage your subscriptions and user accounts; and
- Provide you with technical and customer support.

On the basis of your consent, in order to:

- Subscribe you to a newsletter or the Avast forum;
- Enable the provision of third-party ads in product massages;
- Enable the provision of personalized ads in support of certain free products; and
- Allow us to record our phone conversation when you contact our tech support by phone.

We will always ask for your consent before any processing that requires it and provide you with necessary information through our Consent Policy or otherwise as applicable.

On the basis of legal obligations, we process your Personal Data when it is necessary for compliance with a legal tax, accounting, anti-money laundering, legal order, sanction checks or other obligation to which we are subject.

On the basis of our legitimate interest we will use your Personal Data to:

- Communicate about possible security, privacy and performance improvements and products that supplement or improve our purchased products and to optimize the content and delivery of this type of communication;
- Evaluate and improve the performance and quality of our products, services and websites, develop new products, train our employees and to understand usage trends, and analyze user acquisitions, conversions and campaigns;
- Allow interoperability within our applications;

- Secure our systems and applications;

- Allow effective performance of our business by ensuring necessary internal administrative and commercial processes (e.g. finances, controlling, business intelligence, legal & compliance, information security etc.); and

- Establish, exercise or defend our legal rights.

For the above mentioned processing operations, we have balanced your interests against our interests. In any case, you have the right to object, on grounds relating to our particular situation, to those processing operations. For more details please see section Your Privacy Rights.

Balancing Legitimate Interests

Before relying on our legitimate interests, we balanced them against your interests and made sure they are compelling enough and will not cause any unwarranted harm. With respect to the purposes below we consider necessary to explain what our interests are in detail.

Systems, Apps and Network Security

We process Personal Data for network and information security purposes. In line with EU data protection law, organizations have a recognized legitimate interest in collecting and processing Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security. This primarily covers the ability of a network or of an information system to resist events, attacks or unlawful or malicious actions that could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, or the security of the related services offered by, or accessible via those networks and systems.

Both as an organization in our own right, and as a provider of cybersecurity technologies and services which may include hosted and managed cybersecurity technology services, it is necessary for the functionality of our systems, products and services and in our legitimate interests as well as in our users', to collect and process Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring the security of our own, and of our users' networks, devices, and information systems. This includes the development of threat intelligence resources aimed at maintaining and improving on an ongoing basis the ability of our networks and systems, and

those of certain partners, to resist unlawful or malicious actions and other harmful events (“cyber-threats”).

The Personal Data we process for said purposes includes, without limitation, network traffic data related to cyber-threats such as:

- Sender email addresses (e.g., of sources of SPAM);
- Recipient email addresses (e.g., of victims of targeted email cyberattacks including phishing);
- Reply-to email addresses (e.g., as configured by cybercriminals sending malicious email);
- Filenames and execution paths (e.g., of malicious or otherwise harmful executable files attached to emails);
- URLs and associated page titles (e.g., of web pages broadcasting or hosting malicious or otherwise harmful contents); and/or
- IP addresses (e.g., of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching or other storage of cyber-threats such as malicious or otherwise harmful contents).

Depending on the context in which such data is collected, it may contain Personal Data concerning you or any other Data Subjects. However, in such cases, we will process the data concerned only to the extent strictly necessary and proportionate to the purposes of detecting, blocking, reporting (by removing any personally identifiable elements) and mitigating the cyber-threats of concern to you, and to secure your network, device and systems. When processing Personal Data in this context, we do not seek to identify a Data Subject.

In-product and Email Messages

We have a legitimate interest for messaging our users about possible security, privacy and performance improvements and products that supplement or improve purchased products.

If you are our customer, we feel a responsibility to inform you about security and utility improvements and possible problems to your device and software

that go beyond our product that is installed and provide you with effective solutions relevant to these problems. We thus have legitimate interest to optimize the content and delivery of this type of communication to you so that you will be most likely to find them relevant and non-intrusive at the same time.

Product and business improvement

We have a legitimate interest to use necessary Personal Data to understand user conversions, acquisitions and campaign performance through various distribution channels, and users' download, activation and interactions with our products because these analytics help us improve functionality, effectiveness, security and reliability of our products and business activities and develop new products. This processing includes using third-party tools. Please refer to our Products Policy for the list of third-party tools used for the specific products and services.

How We Process Your Personal Data

We do our best to disconnect or remove all direct identifiers from the Personal Data that we use:

- For free versions, this disconnection or removal of identifiers begins when the products and services are initially activated. For paid users we keep Billing Data in a separate database and minimize its use for anything other than handling payments and our own finances.

- For both paid and free versions, we continuously monitor for, minimize, disconnect and remove all direct identifiers during the normal performance of the products and services.

Processing of IP Addresses

For paid products including antivirus, virtual private network ("VPN"), and performance, your IP address is collected at the time at which your product or service is being provided, for the purpose of facilitating our billing process. Specifically, our third-party billing partner will collect your IP address for its billing process; we do not store the IP address from this process.

For free and paid products including antivirus, your IP address is also processed for the purpose of downloading certain products, product authorization, fraud and malware detection.

Please refer to our Products Policy for specific use of IP address by our products and services.

Personalization

We use your answers from surveys, in which you can participate, and relevant Product Data to personalize communication and recommend our relevant products for you.

We do not take any decisions solely based on algorithms, including profiling, that would significantly affect you.

How We Disclose Your Personal Data

We only disclose your Personal Data as described below, within our group, with our partners, with service providers that process data on our behalf and with public authorities, as required by applicable law. Processing is only undertaken for the purposes described in this Privacy Policy and the relevant Products Policy sections. If we disclose your Personal Data, we require its recipients to comply with adequate privacy and confidentiality requirements, and security standards.

Payment processors

If you opt to pay for use of our services, we will use a third party payment processor to take payment from you. These third parties are properly regulated and authorized to handle your payment information and are prohibited from using your Personal Data for any other purposes other than arranging these services for us. However, they are independent controllers of your data with their own responsibility.

These are our long-term payment processors:

Payment Processor	Link to Privacy Policy	Location

Digital River	https://www.digitalriver.com/privacy-policy/	US, Ireland
Softline	https://allsoftglobal.com/en/privacy-policy/	Cyprus
Nexway	https://www.nexway.com/legal-notice-privacy/	Germany, France, USA
Cleverbridge	https://www.cleverbridge.com/?scope=opprivacy	Germany, USA, Japan, Taiwan, Malta
DLocal (only for non-EEA customers)	https://dlocal.com/legal/privacy-policy/	US, UK, Malta
Net Distribution Services (only for non-EEA customers)	---	India
Paypal	https://www.paypal.com/en/webapps/mpp/ua/privacy-full	US, Ireland
Google Play Store (for mobile apps)	https://policies.google.com/privacy	US, Ireland
Apple Store (for mobile apps)	https://www.apple.com/legal/privacy/	US, Ireland

Your Billing Data is processed by the payment processor from whom you purchased the product. Your data is processed according to the relevant processor's privacy policy.

Service Providers

We may use contractors and service providers to process your Personal Data for the purposes described in this Privacy Policy and Products Policy. We contractually require service providers to keep data secure and confidential.

Such service providers may include in particular contact centers, professional consultants (including for defence or exercise of our rights), and marketing/survey/analytics/software suppliers.

Sometimes these service providers, for example, our distributors, resellers, and app store partners, will be independent controllers of your data and their terms and conditions, end user license agreements ("EULA") and privacy statements will apply to such relationships.

Advertising Companies

To be able to offer our products and services for free, we serve third-party ads of advertising companies in our products for mobile devices. To enable the ad, we embed a software development kit ("SDK") provided by an advertising company into the product, which then collects Personal Data in order to personalize ads for you.

Please note that only few of our free products serve third-party ads. You will be asked for consent during the installation process of such product. For further information, including the exact scope of processed Personal Data and names of relevant products, please refer to our Consent Policy which includes the list of our advertising partners and their privacy policy.

Distributors, Resellers

We may provide your Personal Data to our partners for the purpose of distribution, sale or management of our products. Our partners may use your Personal Data to communicate with you and others about Avast products or services. In addition, you purchase our products directly from our distributor, a reseller, or an app store. Because your relationship in these cases is with that distributor, reseller or an app store, such third party will also process your Personal Data.

Cookies Providers

Our websites use cookies to personalize your experience on our sites, tell us which parts of our websites people have visited, help us measure the effectiveness of campaigns, and give us insights into user interactions and user base as a whole so we can improve our communications and products.. While using our websites,

you will be asked to authorize the collection and use of data by cookies according to the terms of the Cookie Policy.

Analytics Tool Providers

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. We use Service and Device data for analytics.

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 and tools and their privacy policies.

Tool (provider)	**Type of Analytics**	**Link to Privacy Policy**	**Location**
Google Analytics (Google)	user behaviour	https://support.google.com/analytics/answer/6004245 https://policies.google.com/privacy https://support.google.com/analytics/answer/6366371?hl=en&ref_topic=2919631	US, Ireland
Firebase Analytics (Google)	user behaviour (advanced features like A/B testing, predictions)	https://firebase.google.com/support/privacy/ https://policies.google.com/privacy	US, Ireland

Firebase Crashlytics (Google)	crash reporting	https://try.crashlytics.com/terms/privacy-policy.pdf https://policies.google.com/privacy	US, Ireland
AppsFlyer (AppsFlyer)	user acquisition	https://www.appsflyer.com/privacy-policy/	Germany
Adjust (Adjust)	user acquisition	https://www.adjust.com/terms/privacy-policy/	Germany
Facebook Analytics (Facebook)	user behaviour	https://www.facebook.com/about/privacy https://developers.facebook.com/docs/analytics/overview	US, Ireland
HockeyApp (Microsoft)	crash reporting	https://privacy.microsoft.com/en-us/PrivacyStatement	US, Ireland
Mixpanel (Mixpanel Inc.)	user behaviour	https://mixpanel.com/legal/privacy-policy/	US
Loggly (Solar Winds/Loggly)	server side logging - troubleshooting issues	https://www.loggly.com/about/privacy-policy/	US
Amplitude (Amplitude)	user behaviour	https://amplitude.com/privacy	US
Kochava	user acquisition and behaviour	https://www.kochava.com/support-privacy/	US
VWO	user behaviour (A/B testing)	https://vwo.com/privacy-policy/	India

Please note that not all of our products use all of these third-party analytics tools. Analytics tools that we use for diagnosing your product are necessary for service provision. You will find relevant tools listed under each product in our Products Policy.

Public Authorities

In certain instances, it may be necessary for us to disclose your Personal Data to public authorities or as otherwise required by applicable law. No Personal Data will be disclosed to any public authority except in response to:

- A subpoena, warrant or other process issued by a court or other public authority of competent jurisdiction;
- A legal process having the same consequence as a court-issued request for data, in that if we were to refuse to provide such data, it would be in breach of local law, and it or its officers, executives or employees would be subject to liability for failing to honor such legal process;
- Where such disclosure is necessary for us to enforce its legal rights pursuant to applicable law; or
- A request for data with the purpose of identifying and/or preventing credit card fraud.

Mergers, Acquisitions and Corporate Restructurings

Like any other company, we too go through its own cycle of growth, expansion, streamlining and optimization. Its business decisions and market developments therefore affect its structure. As a result of such transactions, and for maintaining a continued relationship with you, we may transfer your Personal Data to a related affiliate.

If we are involved in a reorganization, merger, acquisition or sale of our assets, your Personal Data may be transferred as part of that transaction. We will notify you of any such deal and outline your choices in that event, when applicable.

Cross-Border Transfers of Personal Data among Avast Entities and to Third-Party Vendors

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"). Regardless, we provide 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, 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. Further, an outside-EEA transfer may also occur in case of a merger, acquisition or a restructuring, where the acquirer is located outside of the EEA (see the Mergers, Acquisitions and Restructurings section).

How We Protect Your Personal Data

We maintain administrative, technical, and physical safeguards for the protection of your Personal Data.

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.

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.

Physical Safeguards

Access to user information in our database by Internet requires using an encrypted VPN, except for email which requires user authentication. 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.

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.

Children's Privacy

We have products and services designed specifically to assist you as a parent by providing child online protection features. In such cases, we will only collect and process Personal Data related to any child under 13 years of age, which you choose to disclose to us or otherwise instruct us to collect and process. Details about this processing is included in our Products Policy. Please refer to the specific applicable notices for this information.

How Long We Store Your Personal Data

We will hold your Personal Data on our systems for the following periods:

- For Billing Data, for as long as we have a legal obligation or for our legitimate interests in establishing legal rights;

- For Account Data, for as long as you maintain your account;

- For Product Data, only as long as necessary for the purposes of a particular product or service. We use rolling deletion periods which means we regularly delete collected data in the given periods starting from the collection of that respective data. The rolling deletion periods for Product Data are not longer than six years. You can find specific rolling deletion periods for each of our products and their purposes in our Products Policy. Please note that when you uninstall our product, processing for service provision, in-product messaging, analytics and third-party ads, if applicable, dependent on the installed product shall cease. After the uninstallation, we will continue to process your Product Data for statistical purposes for up to six years, however, we have appropriate measures in place, including pseudonymization.

Storage of Your Personal Data

The data we collect from you may be stored, with risk-appropriate technical and organizational security measures applied to it, on in-house as well as third-party servers in the Czech Republic, in the United States, as well as anywhere we or our trusted service providers and partners operate.

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.

Your Privacy Rights

You have the following rights regarding the processing of your Personal Data:

- Right to information - Right to receive information about the processing of your Personal Data, prior to processing as well as during the processing, upon request.

- Right of access - Aside from the information about the processing of your Personal Data, you have the right to receive a copy of your Personal Data undergoing processing.

- Right to rectification - We should process accurate Personal Data; if you discover inaccuracy, you have the right to seek rectification of inaccurate Personal Data.

- Right to erasure ("right to be forgotten") - You have the right to erasure of your Personal Data, but only in specific cases stipulated by law, e.g., if there is no legally recognized title on our part for further processing of your Personal Data (incl. protection of Avast's legitimate interests and rights).

- Right to data portability - The right to receive Personal Data which you have provided and is being processed on the basis of consent or where it is necessary for the purpose of conclusion and performance of a contract, in machine-readable format. This right applies exclusively to Personal Data which processing is carried out by automated means.

- Right to object - Applies to cases of processing carried out in legitimate interest. You have the right to object to such processing, on grounds relating to your particular situation, and we are required to assess the processing in order to ensure compliance with all legally binding rules and applicable regulations. In case of direct marketing, we shall cease processing Personal Data for such purposes after the objection.

- Right to withdraw consent - In the case of processing based on your consent, as specified in our Consent Policy, you can withdraw your consent at any time, by using the same method (if technically possible) you used to provide it to us (the exact method will be described in more detail with each consent when you provide it). The withdrawal of consent shall not affect the lawfulness of processing based on your consent before its withdrawal.

- Right to restriction of processing - You have the right to restriction of processing of your Personal Data if: You are contesting the accuracy of your Personal Data, for a period enabling us to verify the accuracy of your Personal Data; the processing is unlawful and you oppose the erasure of the Personal Data and request the restriction of its use instead; we no longer need the Personal Data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims; or you have objected to processing of your Personal Data, and there is a pending verification whether our legitimate grounds override your interests.

- Right to contact supervisory authority, court - You may contact and lodge a complaint with the supervisory authority – The Office for Personal Data Protection (Czech: Úřad na ochranu osobních údajů – www.uoou.cz) or your local authority or a relevant court.

The fulfillment of data subject rights listed above will depend on the category of Personal Data and the processing activity. In all cases, we strive to fulfill your request.

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 resolve the situation informally.

Where requests we receive are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

For the free versions, we do not and will not maintain, acquire or process additional information solely in order to identify the users of our free products and services. This is simply not necessary for the free versions of our products to be provided to you and function.

This means, when you use a free version of our products and services, you may contact us with a request concerning your Personal Data. Please note, consistent with our privacy by design, privacy by default and minimization practices, we may not be able to identify you in connection with your Product Data about your specific free products and services. If such a situation occurs, please go to your product settings and explore your options.

Your Choices in products

You can make certain choices about how your data is used by us by adjusting the privacy settings of the relevant product. Please check your product settings to set your privacy preferences there.

Privacy Portal

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 portal, which can show you the Billing

Data and Account Data we have collected from you as well as your email preferences.

Non-EU Jurisdictions

Residents of the Russian Federation

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 to contacts indicated below in the Contact Us section.

You have the right to revoke the consent at any time by sending us an e-mail at contacts indicated below in the Contact Us section. 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.

California Privacy Rights

This section applies to California, USA residents:

Information Notice

Categories of collected personal information

You can see all categories of collected personal information listed in the section Personal Data We Process.

Sources from which the personal information is collected

You can find information about the sources of data in the section Personal Data We Process.

Business or commercial purpose for collecting or selling personal information

You can find all purposes of processing your personal information listed in the section Why We Process Your Personal Data.

Categories of third parties with whom the business shares personal information

You can find all categories of recipients of personal information listed in the section How We Diclose Your Personal Data. Avast does not and will not sell (as such term is defined in the California Consumer Privacy Act) your personal information we collect without providing a right to opt out or your direct permission. See more about your right to opt out of sale below.

Our products are not targeted at minors under 16 years of age. We therefore have no knowledge of any sale of data concerning them.

Your Rights
You have the right to:

- know what personal information is being collected about you;
- know whether your personal information is sold or disclosed and to whom;
- say no to the sale of personal information (right to opt out);
- request deletion of your personal information; information will be deleted if no exception applies (including our right to defend our lawful interests);
- access your personal information; specific information shall be provided in a portable and, to the extent technically feasible, in a readily useable format but not more than twice in a 12-month period;
- equal service and price, even if you exercise your privacy rights (right to non-discrimination).

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 personal information was disclosed.

We hereby disclose that we have not disclosed any such personal information as defined by the California Civil Code § 1798.83 regarding any California resident during the one-year period prior to the effective date of this Privacy Policy with the exception of:

- third-party advertising cookies stated in our Cookie Policy.
- third-party ads in products listed in our Consent Policy.

Right To Opt Out Of Sale
If your personal information is subject to a sale you have the right to opt out from that sale.

A few of our free products serve third-party ads. You will be asked for consent during the installation process of such a product. For further information, including the exact scope of processed Personal Data and names of relevant products, please refer to our Consent Policy which includes the list of our advertising partners and their privacy policy. You can opt out from this processing by upgrading to a paid version of the same product or by uninstalling the product.

Please note that we do use third-party cookies for our advertising purposes as further described in our Cookie Policy where you can also find instructions on how to opt out of these cookies.

We will respect your decision to opt out for at least 12 months before asking you again to authorize the sale of your personal information.

Request Submission
You can submit your requests using contacts indicated below in the Contact Us section. If you are a California resident under the age of 18, you may be permitted to request the removal of certain content that you have posted on our websites. We will verify your request by matching your email address and, if necessary, other information you provide in your request against the email address and other information we have in our system. You can also designate an authorized agent to exercise these rights on your behalf. We may require that you provide the authorized agent with written permission to act on your behalf and that the authorized agent verify their identity directly with us.

Contact Us

To exercise any of your rights, or if you have any other questions or complaints about our use of your Personal Data and its privacy, write our Privacy Team through the most convenient channel below:

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. You can always reach us by email at customerservice@avast.com. 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.

If you live in the United Kingdom, you can contact our representative AVG Technologies UK Ltd., 110 High Holborn, 7th Floor, London, WC1V 6JS, England.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Data Protection Officer

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.

Changes to this Privacy Policy

We reserve the right to revise or modify this Privacy Policy. In addition, we may update this Privacy Policy to reflect changes to our data practices. If we make any material changes we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.