VPN 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 VPN 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.

VPN application

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:

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.

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.

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.

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).

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 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 policy.

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.

Where and How Long We Store Your Personal Data

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.

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.

Disclosure of Your VPN information

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

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.

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.

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.

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.

VPN extension

Personal Data Collection and Use

If you use the free VPN extension for Chrome and Firefox browsers, this is the data that we process on the client extension side:

Client data	**What we use it for**
Application Events Events, such as WebRTC blocking enabled, update event or browser type, etc. together with an internal identifier (“application event identifier”)	For user support, troubleshooting, and product development planning Example: Let us know what features are popular.
License information	For basic functionality, e.g. when the VPN is in the expired state, we show a proper message. Example: License type (trial, paid) or expiration date

We delete this data after **30 days**.

On the backend extension side, we don’t collect any data. Period.

Please note that in order to sync a VPN extension with an installed VPN application, we use native messaging.