

# VPN Policy

This policy applies solely to our VPN services and must be read together with the general data processing information. Please read [General Privacy Policy](#) for overall information about who we are.

This policy does not apply to service data which may be collected by different products, such as an antivirus app, or to the operation of cookies on our website. Please read [Products Policy](#) or [Cookies Policy](#) for such information.

## What data our VPN processes?

Generally speaking, we need some personal data particularly to provide you our products and services, optimize and improve our products and services, to send you direct marketing, or to comply with our legal obligations. We try to minimize the collection of any data, we aggregate or delete it as soon as possible, and if it is not necessary we don't collect it at all. We will describe how we process the data in the following sections. But let's start with what we don't collect.

### Data we don't send to our servers. Period.

- Originating IP address.
- Any DNS queries while connected. We rely on our own secure DNS servers, so your queries are also protected from exposure to 3rd parties.
- Browsing history.
- Transferred data meaning files such as emails, pictures or other data which you download/upload from the internet.

### Personal Data 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 personal data about you in the following situations:

## Product functionality

## Service Data from our VPN servers

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

<b>Service Data</b>	<b>What we use it for</b>
	To calculate peak times of service demand in order to plan the network capacity.
Timestamps of connections	To manage the number of concurrent active connections, and handle abuse. To troubleshoot our service.  Example: We use them to detect sudden disconnects of multiple connections and correlate it with other monitoring data in order to resolve the issues.
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 server’s service data for 35 days**, after which time it is deleted on a rolling basis — data created on Jan 3rd, 2020 gets deleted on Feb 7rd 2020, for example.

## Service Data from our VPN clients

In order to make sure our VPN clients do their job properly and without errors we have to know how many specific errors we have. This data pertains to interactions taken in the app, and cannot be used to uncover what you’re using the VPN service for.

<b>Client Data</b>	<b>What we use it for</b>
Connection events	To operate and provide VPN service with high quality.
Events such as the attempt to connect, disconnection, connection error, etc.	Example: How many unknown users get the same error?
Application Events	To plan product development and analytics
Events such as auto-connection, uninstall event, etc.	Example: How many users do we have? Is a new client-side feature we introduced popular? Are users uninstalling after our latest release?
Crash reports generated and sent by the user	Please note that if you provide us together with information above also your personal data, e.g. within an ad hoc crash report that you decide to send to us, we could add this information to the service data and might be able to connect it with you.
We might collect data like your e-mail, app version or	

internal identifiers described above. Example: App is crashing on some specific device. This is how customer care support can help with device-specific issues.

**We store client’s service data for 2 years**, after which time it is deleted on a rolling basis — data created on Jan 3rd, 2019 gets deleted on Jan 3rd, 2021, for example.

## **Account creation and management**

When you create an account with us (note: this is necessary in order for you to use the VPN service), we will need some information about you. This is the personal data that is created and stored for the management of your account:

<b>Account data</b>	<b>What we use it for</b>
Email address	To send you purchase receipts, communications, and occasional product news
Activation Code	To activate your subscription
Subscription renewal date	To tell us until when the account is valid

Account data is stored for the lifetime of your product plus 2 years. You can see all of this data by logging into our [Privacy Preference portal](#).

## **Billing and Payment**

We rely on our payment providers to handle your product purchases. You can find out which provider we are working with for the point of purchase you chose (for example our website, an app store, etc) by looking at your transactional email or receipt. The list of all payment providers we use can be found in our [General Privacy Policy](#). Please consult the website of the relevant payment provider for more information on their privacy practices.

## **Third-party tools used for analytics**

To analyze application events from our VPN clients in order to understand how our services function, or how stable or successful they are, we rely on our own analytics tools as much as possible. Here are the third-party tools we use, how we use them, and their privacy policies:

### **Google Firebase Analytics on iOS and Android**

Firebase helps us to understand how people interact with certain aspects of our service. While Firebase normally relies on Android Advertising ID or iOS Identifier for Advertisers, this is not the case of our service because we’ve opted to use our own anonymizing identifiers instead.

As this tool is not necessary for service functioning, you can opt-out of providing us with this performance data in our application settings.

## Google Fabric Crashlytics on iOS and Android

This Google tool helps us to improve application stability, pinpoint things that don't work, and improve your experience.

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](#).

## App Center on macOS

This is used for crash reporting. This tool belongs to Microsoft and you can find their privacy policy [here](#).

## Deprecated Analytics

If you're still on older versions of our service, the following analytics are embedded in them:

- 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](#).

We highly recommend that you upgrade to [later versions](#).

## VPN Extension Privacy Policy

We offer the browser extension as an addition to the desktop product. This extension only manages the installed VPN application. This means that there is no more additional data collected than is described below.

If you use the 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

To plan product development and analytics

Events such as update, uninstall or version of the browser, etc.

Example: How many users do we have? Is a new client-side feature we introduced popular? Are users uninstalling after our latest release?

**We store client's service data for 2 years**, after which time it is deleted on a rolling basis — data created on Jan 3rd, 2019 gets deleted on Jan 3rd, 2021, for example.

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