

PRIVACY POLICY

*This Privacy Policy was last modified on 9th April, 2019.*

This privacy policy governs your use of the software application Secured VPN Pro ("Application") for mobile devices. Secured VPN Pro (also referred to as "we", "us" or "our") understands that you are aware of and care about your personal privacy interests, and we take that seriously. We will fully comply with all applicable Data Protection and consumer legislation from time to time in place. This Privacy Policy describes Secured VPN Pro's policies and practices regarding its collection and use of your Personal Information, and which rights you have regarding them.

User Provided Information and How We Use Them

In relation to the "Privacy Policy" the term "Personal Information" shall be regarded as the information and data that belongs to identified or unidentified person. Any personal information regarding you will be collected from different sources that are listed in the following information.

The Application obtains the information you provide when you download and register the Application. Registration with us is optional. However, please keep in mind that you may not be able to use some of the features offered by the Application unless you register with us.

When you register with us and use the Application, you generally provide:

- (a) Your name, email address, age, user name, password and other registration information;
- (b) Information you provide us when you contact us for help;
- (c) Information you enter into our system when using the Application, such as contact information etc.

Purpose

We use your information in order to:

- Create your account.
- Create things that are relevant to you.
- For statistical or survey purposes to improve this website and its services to you.
- Complete payments you make on our website with your billing information.
- Ensure you find services and information quickly.
- Ensure that you don't have to add information more than once, this makes the website easier for you to navigate through!
- Send you email about our services

device, your mobile operating system, the type of mobile Internet browsers you use, network that you use, your language, and information about the way you use the Application. This is done for the purpose of making in depth analysis, improvements on our services and troubleshooting. Our services improvement experts may require such details to be collected for marketing purposes. The IP address you use will be securely encrypted for the whole length of use of the service and will be deleted from your device afterwards when you no longer use VPN service.

When you visit the mobile application, we may use GPS technology (or other similar technology) to determine your current location in order to determine the city you are located within and display a location map with relevant advertisements. If you are subscribed to the use of the Premium package, then no single piece of information will be shared with advertisers.

We will not share your current location with other users or partners. If you do not want us to use your location for the purposes set forth above, you should turn off the location services for the mobile application located in your account settings.

When connection to our service is established and when it comes to the stage when IP address details are collected, it immediately becomes encrypted and remained so until the VPN session comes to an end. The IP address that any client uses will be deleted immediately after the session and the use of the service is finished and you are disconnected. After disconnecting from the service we will never keep your IP address in our history or log into the system under the IP number that you used. Your IP address is not regarded to be as part of your online activities by any means.

Whatever application or website is used by any of our clients, it is never attributed with a concrete user. Your activities stay intact and nobody will ever make any attempt of login into it as well as no apps or domains that are used will be associated with your gadget, email and even yourself. Whatever websites are accessed with the use of our service's servers are stored to the following: 1. For making analysis, in order to find out whether clients can easily access certain applications and websites; 2. Provided services' quality has to be improved as well as any problems and troubles will have to be eliminated.

When the service's websites are accessed:

Together with our partners, Secured VPN Pro and its service providers (Maxmind or even Google analytics) could possibly collect your details and information automatically. It is usually obtained by placing beacons, cookies or perhaps by making applications of other similar technologies in browser that clients use or with the emails that are sent to you. It could be done for the purposes of preventing frauds, determine the overall number of the app users, to make sure the application operates and functions in the most efficient way as well as for opened newsletter and other messages. If any client does not want such information to be collected via use of the cookies, there is a standard procedure in any browser to disallow this information to be collected. Cookies settings could be made so that any

Google Analytics. How it is implemented and how it is practiced in reality you can always find on the website [www.google.com/policies/privacy/partners/](http://www.google.com/policies/privacy/partners/). Google Analytics browser can also be downloaded and installed at any time you want by visiting the following page: <https://tools.google.com/dlpage/gaoptout>.

When you establish connection to our service and products, the information details that will be collected are not going to be associated with usage of such connection.

Payments

When you make payments through debit or credit card, it is the third party services that will obtain your payment details information and not us. Any payments that can be made via the use of Apple Store as well as PayPal system, any payment details that you are about to provide will be subject to the terms and conditions of the system where those payment details will be supplied. It will have nothing whatsoever to do with our service and will relate to the Privacy Policy of any of the above mentioned organizations.

Legitimate Interest

We will share your information with third parties only in the ways that are described in this privacy statement.

We may disclose User provided and Automatically Collected Information:

As required by law, such as to comply with a subpoena, or similar legal process;

When we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request;

With our trusted services providers who work on our behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth in this privacy statement;

If Secured VPN Pro is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our Web site of any change in ownership of this information, as well as any choices you may have regarding this

What are my opt-out rights?

You can stop all collection of information by the Application easily by uninstalling the Application. You may use the standard uninstall processes as may be available as part of your mobile device or via the mobile application marketplace or network.

Data Retention Policy, Managing Your Information

We will retain User provided data for as long as you use the Application and for a reasonable time thereafter. We will retain Automatically Collected information for up to 24 months and thereafter may store it in aggregate. Please note that some or all of the User Provided Data may be required in order for the Application to function properly.

Security

We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees and contractors who need to know that information in order to operate, develop or improve our Application.

When a certain user uses the service on encrypts, all exchanged traffic information between your domain and Secured VPN Pro servers will use TLS 1.2 along with outstanding level of secrecy (ECDHE) as well as in terms of encryption 128-bit/256-bitAES data will apply, along with HMAC identification for messaging will be provided.

Generally, whenever users use public wireless service to connect to the internet, including at the airports, restaurants, hotels, train stations etc., it can be definitely said that received signal will be protected by Secured VPN Pro. While you use the service, there is one hundred percent guaranty that nobody, including internet provider will be able to hack or snoop into the traffic you use as well as the webpages you need to open. Whoever makes an attempt to hack and watch what you are up to will only be able to see that the traffic is going in and out of your device but the details will never be seen.

The service ensures every aspect of physical, administrative and technical safety, so that no sensitive and private information is leaked. Maximum protection in terms of unlawful access, collection, maintenance as well as distribution of your personal information and data is ensured, with respect to accidental loss, unauthorized disclosure.

Data is stored / processed by our cloud providers in all countries they operate. However, we assure you that we will take steps to ensure that your privacy is protected.

Changes

This Privacy Policy may be updated from time to time for any reason. We will notify you of any changes to our Privacy Policy by posting the new Privacy Policy here and informing you via email or in-application message. You are advised to consult this Privacy Policy regularly for any changes, as continued use is deemed approval of all changes.

Your Rights

By virtue of the General Data Protection Regulation (GDPR) our users have, with certain statutory exceptions, multiple rights with regard to Secured VPN Pro's processing of personal data. Users have:

- (1) The right to request access to their personal data and to find out how they are processed;
  - (2) The right to correct or complete incorrect or incomplete information;
  - (3) The right to delete personal data for data processed illegally where the lawful basis is consent;
  - (4) The right to restrict personal data processing;
  - (5) The right to transfer personal data in electronic format (data portability);
  - (6) The right to object to personal data processing based on the legitimate interest of Secured VPN Pro.
- Users have the right at any time to withdraw a consent previously given regarding Secured VPN Pro's processing of users personal data.

Links to Third Party Site

These links will let you leave Secured VPN Pro. The linked sites are not under the control of Secured VPN Pro and Secured VPN Pro is not responsible for the contents of any linked site or any link contained in any linked site, or any changes or update to such sites. Secured VPN Pro is not responsible for any webcasting or any other form of transmission received from such linked site. Secured VPN Pro is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement by Secured VPN Pro of the site.

Data Breach

Secured VPN Pro has taken strong measures to protect the security of your personal information and to ensure that your choices for its intended use are honoured. We take strong precautions to protect your data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

However, in the event of unforeseeable circumstances leading to data breach, you will be informed of such data breach within 72 hours of identifying the breach.

Your Consent

By using the Application, you are consenting to our processing of your information as set forth in this Privacy Policy now and as amended by us. "Processing," means using cookies on a computer/hand held device or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information.

Contact Details, Complaints and Questions

If a client has any questions or queries regarding the policy, the contact should be made in writing to the following email address: [support@contrast.name](mailto:support@contrast.name)