

VPN TERMS OF SERVICE

1. General Provisions

1.1. Scope of Regulations

- (1) These terms of service (the “**Terms of Service**”) set out the terms and conditions under which Secure VPN Solutions Limited, with its registered office in Seychelles, address: House of Francis, Room 303, Ile Du Port, Mahe, Seychelles, entered into the Register of Companies under number 224005 (“**SecureVPN**”) provides a VPN service (the “**VPN Service**”) to users (the “**User**”). These Terms of Service provide detailed information about the VPN Service, the rules on which it is provided, the entities involved in its provision and the terms and conditions on which Users may use it.
- (2) The User should read these Terms of Service before using the VPN Service.

1.2. Definitions

- (1) **VPN Key** means IT solutions made available to the User to enable him or her to use the VPN Service;
- (2) **Terms of Service** means these Terms of Service;
- (3) **VPN Server** means the SecureVPN server used to provide the VPN Service;
- (4) **Website** means the website operated by AFTERMARKET.PL Limited at www.aftermarket.pl;
- (5) **VPN Agreement** means an agreement for the provision of the VPN Service on the terms and conditions specified in these Terms of Service and in accordance with the accepted or selected subscription plan, concluded by the User and SecureVPN;
- (6) **VPN Service** means the service described in clause 2;
- (7) **User** means a person buying the VPN Service from SecureVPN;
- (8) **User who is a consumer** means the User who is a natural person and who concludes the VPN Agreement for purposes not directly connected with his or her business or professional activity.

1.3. Rules of Interpretation

The section captions used in the Terms of Service are for convenience of reference only and shall not affect the interpretation or construction of the Terms of Service.

2. VPN Service

2.1. Description of the VPN Service

- (1) The VPN Service consists in providing the User with IT solutions (access data, encryption keys, IP address of the VPN Server, etc.) (the “**VPN Key**”) which enable the User to establish a connection (tunnel) with the VPN Server. This allows the User to create a virtual private network by establishing a connection between his or her equipment and the VPN Server, and to communicate with the Internet through this server, which basically encrypts the User’s activities on the Internet, hides his or her IP address and protects his or her privacy on the Internet. With the VPN Service active, the traffic and activity on the Internet generated by the User are transferred through the VPN Server, which, by transmitting further such traffic and activity, masks the User’s data, replacing them with the data of the VPN Server. Thus, to the recipient, the traffic and activity on the Internet generated by the User seem to be generated from the VPN Server with the use of the IP of the server.
- (2) The VPN Service helps to protect the User’s privacy when using the Internet but does not guarantee complete anonymity. The User should be aware of the risk that each use of the Internet may leave traces that enable identification of the User.
- (3) Provision of the VPN Service starts when the VPN Keys are made available to the User, irrespective of the time of their use by the User (activation of the VPN Service). The VPN Service is also provided if the User has not activated the VPN Service or has effectively ceased using it without terminating the VPN Agreement.
- (4) The VPN Service is provided as is at any given time, subject to efforts to make the VPN Service available on a continuous, uninterrupted and round-the-clock basis. However, the actual availability or functionality of the VPN Service, including data transmission range and speed, etc., may vary from time to time. In particular, the actual data transmission speed may vary depending on configuration, compression, network congestion, load on the VPN Server and other factors. The VPN Service may be unavailable, or its functionality may be limited in certain situations, in particular as a result of maintenance or development works, failures and their removal. Unavailability of the VPN Service may also be caused by external factors, such as failures of services necessary for the provision of the VPN Service which are provided by third parties, hardware or network failures, Internet disruptions.

2.2. VPN Service Provider

- (1) The VPN Service is provided by SecureVPN, which is also the provider of the VPN Key.
- (2) For the avoidance of any doubt, AFTERMARKET.PL Limited is not the VPN Service provider, nor is it involved in the provision of the VPN Service. AFTERMARKET.PL Limited may perform certain activities at the request of SecureVPN, which may include facilitating communication between SecureVPN and the User by providing certain Service functionalities.

2.3. VPN Application

- (1) The use of the VPN Service requires third-party vendor software (the “**VPN Application**”). The list of VPN Applications recommended by SecureVPN that support the VPN Service is available at: <https://faq.securevpnsc.com/download> . Other VPN Applications are not recommended and may cause a failure or malfunction of the VPN Service.
- (2) VPN Applications are provided by third-party vendors. SecureVPN does not modify, edit, customise or affect the VPN Applications or the manner of their functioning.
- (3) The manufacturer of the VPN Application is fully responsible for the functioning of the VPN Application, including its malfunction and the consequences of this circumstance.
- (4) The VPN Application is used under the terms of a licence agreement between the User and its manufacturer. SecureVPN is not a party to such a license agreement.

2.4. Monitoring of the VPN Service

- (1) Individual actions of the User during the use of the VPN Service are not monitored, recorded, processed, stored or transmitted to third parties. SecureVPN does not store logs. In particular, it does not store information about the start and end date and time of the session, the duration of the session, the User’s IP addresses and ports and the IP addresses and ports to which the User connects via the VPN Service, information about the bandwidth used or traffic logs.
- (2) SecureVPN may monitor Users’ activity while they are using the Internet with the VPN Service active. Monitoring may justify the use of traffic and activity management measures referred to in clause (4). Monitoring is quantitative and not qualitative, which means that only the number of open sessions outgoing from the VPN Server to Internet resources initiated by a given User is monitored in real time, without interference or analysis of data sent or received by the User.
- (3) The collection of information on the number of open sessions under clause (2) provisions is done for statistical purposes and to prevent overload of the VPN Server. It is performed in real time, and the collected information is generally not saved or otherwise recorded. During such monitoring, the User’s name and the number of simultaneously active sessions may be temporarily stored. However, these data are deleted at the end of the session at the latest and cannot be restored.
- (4) As part of the monitoring, traffic and activity on the Internet generated by the User may be shaped, queued and limited by any methods, including in particular prioritisation, rate limiting, QoS, traffic shaping, policing, drop, to maintain the high quality of the VPN Service and to comply with the requirements of third parties which provide services necessary for the provision of the VPN Service. Traffic and activity management measures are intended to promote efficient use of the VPN Server and optimise the overall quality of the VPN Service provided to all users, are applied on a non-discriminatory basis and are based on objective criteria designed to meet the above-mentioned objectives. Their application may result in a temporary reduction in the level of provision of the VPN Service, which is not a violation of the standards for the provision

of the VPN Service but merely a mechanism to maintain the quality of the VPN Service. Traffic and activity management measures may be applied in particular when it is necessary for:

- (a) ensuring compliance of the VPN Service with applicable laws, regulations or decisions of competent authorities,
- (b) maintaining the security of the VPN Server,
- (c) preventing an overload of the VPN Server or mitigating its effects.

2.5. Technical Conditions

- (1) To use the VPN Service, the User needs to:
 - (a) have internet access,
 - (b) have an active user account on the www.aftermarket.pl website (the “**Website**”),
 - (c) order the VPN Service via the Website,
 - (d) have the VPN Application,
 - (e) configure the VPN Service and activate it in accordance with the SecureVPN guidelines.
- (2) The VPN Server may automatically block specific network ports. Receiving and sending data from or to these network ports with the VPN Service enabled is not possible.
- (3) Detailed information about the requirements and a list of blocked network ports are available in the description of the VPN Service at <https://faq.securevpns.com/tech> .

3. Ordering the VPN Service and Payment

3.1. Ordering the VPN Service

- (1) The VPN Service is ordered via the Website after logging into the User’s account on the Website. When ordering the VPN Service, the User accepts (if only one is available) or chooses (if there are several options) a subscription plan in accordance with the current price list available on the Website.
- (2) As a result of placing an order, the User enters into an agreement with SecureVPN for the provision of the VPN Service under the terms and conditions set forth in these Terms of Service and in accordance with the accepted or selected subscription plan (the “**VPN Agreement**”).
- (3) Once an order has been placed, SecureVPN shall make available to the User, via the Website or by e-mail to the User’s address provided on the Website, the VPN Key together with instructions on how to configure and activate the VPN Service.

3.2. Fees for the VPN Service

- (1) Subscription fees for using the VPN Service are specified in the subscription plan accepted (selected) by the User upon placing an order.
- (2) Subscription fees are cyclical and are charged in advance for each billing cycle. The billing cycle is defined in the subscription plan. If the VPN Agreement is not concluded for an entire billing cycle, the subscription fee is calculated proportionally to the duration of the VPN Service. Where the VPN Agreement is terminated before the end of a billing cycle or the provision of the VPN Service is suspended in a given cycle, the subscription fee for a given billing cycle shall be reduced proportionally to the period during which the VPN Service was not provided.
- (3) Subscription fees shall be documented by VAT invoices. The User agrees to receive VAT invoices in electronic form via the Website or by e-mail to the User's address given on the Website.
- (4) The date of payment of the subscription fee shall be specified in the VAT invoice, and this date shall not be earlier than 14 (fourteen) days from the date of issue of the invoice. The subscription fee shall be paid by a bank transfer to the bank account specified in the VAT invoice or by other payment methods specified on the Website, and if SecureVPN has funds previously paid by the User, by deducting the subscription fee from such funds.

3.3. Promotional Period

SecureVPN may decide to provide the VPN Service for free during the promotional period.

4. Using the VPN Service

4.1. Terms of Use

- (1) The User may use the VPN Service only for lawful purposes and in compliance with good practice. The User is prohibited from providing unlawful content.
- (2) The User is not entitled to make the VPN Service available to third parties in any way, in particular for commercial purposes.
- (3) When using the VPN Service, the User shall be solely liable for all of his or her acts and omissions in connection with the use of the service, including violations of the laws of the jurisdiction to which he or she is subject and of the rights of third parties. Specifically, the liability covers any data transmitted through the VPN Service.
- (4) The use of the VPN Service in certain countries, locations, destinations, or instances may be restricted, excluded, or violate the law. Therefore, before ordering and using the VPN Service, the User should check if he or she can use the VPN Service in accordance with the applicable laws and regulations to which he or she is subject and if the use of the VPN Service will not result in any liability, in particular criminal or administrative liability. The User may not use the VPN Service if this is prohibited by applicable laws or

regulations to which the User is subject. The User should immediately notify SecureVPN of such a circumstance.

4.2. Prohibited Activities

The VPN Service may not be used to:

- (1) provide content that is unlawful, pornographic, defamatory or slanderous to specific persons, institutions, communities, nationalities or nations, contrary to accepted principles of morality, violates third party rights, incites or facilitates the commission of criminal acts,
- (2) violate any applicable law, regulation or decision of a competent authority,
- (3) conduct a legally regulated activity without obtaining the appropriate concession, licence, permit or fulfilling any other conditions under applicable laws, regulations or decisions of competent authorities,
- (4) carry out criminal activities,
- (5) launder money or finance terrorism,
- (6) attack other computers, systems or networks,
- (7) generate artificial traffic which is not for the purpose of transmitting, receiving or transferring data,
- (8) generate traffic intended to block the VPN Service, VPN Server or other services, servers or systems,
- (9) gain unauthorised access to data, systems or networks, including attempts to probe or test for security holes or to breach or bypass security or authentication measures on such systems or networks,
- (10) violate any third party rights, including its intellectual property rights,
- (11) interfere with other services, including the VPN Services provided to others,
- (12) distribute unsolicited commercial communications, as well as content constituting spam or chain letters,
- (13) take any action to encourage or promote any activity prohibited under these Terms of Service.

5. Liability

5.1. Liability of SecureVPN

- (1) SecureVPN shall provide the VPN Service with due diligence.
- (2) SecureVPN shall not be liable for lost, undelivered, delayed or misdelivered data, regardless of the reason for any interruptions or problems with the VPN Service or

communication services or networks. SecureVPN does not save or archive such data, and any recovery of such data by SecureVPN is not possible.

- (3) SecureVPN shall also not be liable for:
- (a) the occurrence of force majeure, which is understood as an event beyond the control of the parties to the VPN Agreement, which is external, impossible to predict and prevent, in particular wars, natural disasters, strikes, cyber attacks (including DDoS) and acts issued by public authorities,
 - (b) decisions or rulings of public authorities, in particular decisions ordering the removal of the VPN Server,
 - (c) temporary or permanent unavailability of the VPN Service or the VPN Server,
 - (d) temporary or permanent malfunction of the VPN Service or the VPN Server,
 - (e) defects or malfunctions of the VPN Key and the consequences of such defects or malfunctions, in particular damage to Users' hardware and software or loss of data,
 - (f) permanent or temporary inability to provide the VPN Service and improper provision of the VPN Service for reasons attributable to third parties by means of which the VPN Service is provided,
 - (g) operation of malicious software (trojans, viruses, etc.),
 - (h) improper use of the VPN Service by the User,
 - (i) the use of encryption data, login data or passwords by third parties, if such third parties obtained such data as a result of their disclosure by the User or due to the User's failure to adequately protect the information against access by such third parties,
 - (j) data and content sent and received via the VPN Service,
 - (k) violation by the User of the provisions of the VPN Agreement or these Terms of Service.
- (4) SecureVPN's liability to the User in connection with the VPN Service provided at the User's request shall be limited to the sum of the subscription fees paid by the User for the provision of the VPN Service.
- (5) The provisions of clauses (2) – (4) shall not apply to SecureVPN's liability to the User who is a consumer, to the extent that it is not possible to apply such provisions in relation to a consumer. In particular, the limitations of SecureVPN's liability provided for in clause (3) letter (c) – (f) and clause (4) do not apply to the User who is a consumer.

5.2. Liability of the User

- (1) The User is obliged to cooperate with SecureVPN in combating unlawful actions of persons to whom the User has made the VPN Service available, for example, by

providing data enabling the identification of such persons to appropriate authorities or institutions.

- (2) The User shall be liable for the use of the VPN Service by third parties to whom the User has made this service available contrary to the provisions of clause 4.1.(2).
- (3) The User is obliged to remedy any damage caused to SecureVPN by the fault of the User.
- (4) If a third party, authority or institution makes a claim or demand against SecureVPN related to the VPN Service provided to the User, the User is obliged to cooperate with SecureVPN to the extent necessary. The User, who is not a consumer, is also obliged to participate in any arbitration, complaint, court, security or enforcement proceedings pending against SecureVPN in connection with the VPN Service provided to the User and to indemnify SecureVPN in this respect and to cover all costs and expenses incurred by SecureVPN in connection therewith.

5.3. Suspension of the Provision of the VPN Service

- (1) SecureVPN may suspend the provision of the VPN Service if the User or the entity to which the User has made the VPN Service available:
 - (a) violated the provisions of these Terms of Service, or there is a justified suspicion of their violation,
 - (b) has not paid the subscription fee if the delay in the payment exceeds 7 (seven) days and the User has been summoned via the Website or by e-mail to the User's address given on the Website to pay it under pain of suspension of the VPN Service provision.
- (2) SecureVPN shall immediately inform the User about the suspension of the provision of the VPN Service via the Website or by e-mail to the User's address given on the Website.
- (3) The provision of the VPN Service may be resumed after the reasons for which the service was suspended have ceased to exist.

6. Complaints

- (1) The User may file a complaint relating to the non-performance or improper performance of the VPN Agreement via the contact form available at <https://faq.securevpnsc.com/contact> .
- (2) SecureVPN will handle the complaint within 21 (twenty-one) days from the date of its receipt and will send a response to the complaint via e-mail to the address provided in the contact form referred to in clause (1) or, if no such address is provided, via the Website or by e-mail to the User's address provided on the Website.
- (3) SecureVPN shall not be obliged to provide the User with a response to the complaint, its duplicate or copy again if the circumstances of a given case clearly indicate that the response to the complaint was delivered to the User.

- (4) Users who are consumers may also use the online dispute resolution platform available at:
<https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=PL>

7. Duration of the VPN Agreement

- (1) The VPN Agreement is entered into for an indefinite period.
- (2) SecureVPN and the User may terminate the VPN Agreement by 7 (seven) days' notice.
- (3) SecureVPN and the User may also terminate the VPN Agreement without notice in the event of a gross breach by the other party of the provisions of these Terms of Service, in particular the provisions of clause 4.2.
- (4) Upon expiration of the VPN Agreement, the User shall be obliged to cease using the VPN Key and remove it from the data storage media in the User's possession.

8. Final Provisions

8.1. Right of Termination of the VPN Agreement

- (1) The User who is a consumer is entitled to terminate the VPN Agreement within 14 (fourteen) days without giving any reason. The time limit for termination of the VPN Agreement expires after 14 (fourteen) days from the date of conclusion of the VPN Agreement.
- (2) To exercise the right to terminate the VPN Agreement, the User who is a consumer must inform SecureVPN of the decision to terminate the VPN Agreement by an unequivocal statement sent via e-mail to hello@securevpnc.com. The User who is a consumer may use a model form of termination of the VPN Agreement available at: https://securevpnc.com/download/resignation_form.pdf, however, this is not obligatory. SecureVPN shall immediately send an acknowledgement of receipt of the notice of termination of the VPN Agreement by e-mail to the address provided by the User who is a consumer or, if no such address is provided, via the Website or by e-mail to the User's address provided on the Website. To meet the deadline for the termination of the VPN Agreement, it is sufficient for the User who is a consumer to send information regarding the exercise of the right to terminate the VPN Agreement before the expiry of the deadline for the termination of the VPN Agreement.
- (3) In the event of termination of the VPN Agreement, SecureVPN shall refund to the User who is a consumer all payments received from him or her immediately and, in any event, no later than within 14 (fourteen) days from the day on which SecureVPN receives notice from the User who is a consumer of the decision to exercise the right to terminate the VPN Agreement. The payment will be refunded by transfer to the bank account of the User who is a consumer from which the last payment was made. The User who is a consumer will not incur any charges in connection with the return. However, if the User who is a consumer has requested the commencement of the provision of the VPN Service before the expiry of the period for termination of the VPN Agreement, he or she

will be obliged to pay a subscription fee proportional to the period of provision of the VPN Service up to the time when he or she informed SecureVPN of the termination of the VPN Agreement.

- (4) The right to terminate the VPN Agreement shall not apply, inter alia, in the following cases:
 - (a) when the VPN Service has been performed in full with the express consent of the User who is a consumer and who was informed prior to the performance that after SecureVPN's performance, he or she would lose the right to terminate the Agreement,
 - (b) when the delivery of digital content, which is not recorded on a tangible medium, has begun with the express consent of the User who is a consumer before the expiry of the time limit for termination of the VPN Agreement and after SecureVPN has informed the User about the loss of the right to terminate the Agreement.

8.2. Governing Law and Jurisdiction

- (1) The VPN Agreement and these Terms of Service are governed by Polish law.
- (2) All disputes arising out of or in connection with the VPN Agreement or provision of the VPN Service shall be settled by the common court for the Śródmieście District of the Capital City of Warsaw. The provisions of the preceding sentence shall not apply to the User who is a consumer.

8.3. Contact

In matters related to the VPN Service, SecureVPN can be contacted via the contact form available at <https://faq.securevpnsc.com/contact> .

8.4. Amendments to the Terms of Service

- (1) SecureVPN reserves the right to amend these Terms of Service for important reasons, in particular, related to changes in legal provisions and changes in technical conditions of providing the VPN Service.
- (2) SecureVPN shall inform the User about amendments to the Terms of Service by sending a specification of the amendments or a new consolidated text of the amended Terms of Service via the Website or by e-mail to the User's address provided on the Website. The User has the right to terminate the VPN Agreement upon notice within 7 (seven) days of receiving the above documents. In the event of giving notice of termination, the User shall be bound by the existing Terms of Service. If the User does not give the notice, the amended Terms of Service shall be binding upon the expiry of the aforementioned seven-day period.

8.5. Entry into Force

These Terms of Service shall enter into force on 01.08.2021.