Deloitte.

Surfshark B.V.

ISAE 3000 - Independent Reasonable Assurance Report

14 December 2022

To the Board of Directors of
Surfshark B.V.
Kabelweg 57, 1014BA Amsterdam, the Netherlands

We have been engaged by Surfshark B.V. (hereinafter "Surfshark" or "Engaging Party") to perform independent assurance procedures on the configuration of IT systems and supporting IT operations used to provide the VPN services to customers, in accordance with the service description in Appendix I. Our assurance procedures concluded on 02 December 2022.

We performed our assurance procedures in between 21 November and 02 December 2022.

Responsibilities of the Engaging Party

The Management of Surfshark is responsible for preparing Surfshark's configuration of IT systems and management of the supporting IT operations and the accompanying statement, including the completeness, accuracy, and method of presentation of the description and the statement and its implementation. This is in accordance with the criteria in respect to the description of the "Surfshark's configuration of IT systems and management of the supporting IT operations" prepared by the Management of Surfshark. This responsibility includes the design, implementation and maintenance of the internal control system related to the preparation of Surfshark's configuration of IT systems and management of the supporting IT operations that are free from material misstatement, whether due to fraud or error. Furthermore, the Management is responsible for the selection and application of the criteria as set out in Appendix I.

Our Independence and Quality Control

We are independent of Surfshark in accordance with the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA Code) that are relevant to our audit of financial statements and other assurance engagements. We fulfil our other ethical responsibilities in accordance with the IESBA Code.

Our firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Responsibilities of the Practitioner

Our responsibility is to perform an independent audit and prepare a reasonable assurance report and to express a conclusion on the fair presentation of Surfshark's configuration of IT systems and management of the supporting IT operations and its implementation as set out in Appendix I.

Our audit has been conducted in accordance with the International Standard on Assurance Engagements 3000 (Revised) applicable to Assurance Engagements Other Than Audits or Reviews of Historical Financial Information (ISAE 3000 (Revised)) established by the International Auditing and Assurance Standards Board ("IAASB"). In accordance with this standard, we have planned and performed our engagement to obtain reasonable assurance whether Surfshark's configuration of IT systems and management of the supporting IT operations were prepared, in all material respects, in accordance with the criteria in respect to the description of Surfshark's no logging safeguards prepared by the Management of Surfshark as of 02 December 2022.

Summary of work performed

Based on risk and materiality considerations, we performed our procedures to obtain sufficient and appropriate assurance evidence. This report is solely regarding the system and infrastructure at the time of the audit, any later modification of the system or infrastructure may change our conclusion. Our assurance engagement is a point in time assessment. The procedures we performed do not provide any assurance for any other point in time or period of time.

As part of the procedures to create an independent reasonable assurance report, we performed the following work:

- Inquiries with responsible Surfshark employees,
- Review of the statement and description in Appendix I to verify whether the description fulfils the required relevant level of details and covers all relevant assertions made in the statement,
- Inspection of relevant IT systems (Standard VPN servers; Static IP VPN servers; Multihop servers and Multiport servers) design and configuration. The inspection and technical review was done on the IT infrastructure and configuration files provided by Surfshark
- Review of server's configuration and deployment process
- Review of privacy relevant configuration settings and procedures, inspection weather the settings are in line with the "logging policy" (Appendix I.) including, but not limited to: Configuration management system roles relevant to VPN infrastructure, VPN Server configuration, API (VPN infrastructure related Infra micro-service servers), SDN (Software Defined Network) and verification of their configuration against the description provided.

The following procedures are out of scope of this engagement:

- Data transfer security and security measures in place for the protection of data and systems of Surfshark,
- Streaming infrastructure (Haproxy servers, Sni proxy servers) and "Captcha" solution run on the same infrastructure,
- Web/API infrastructure except specific parts that connected to VPN infrastructure,
- Internal control environment for the maintenance and operation of the system environment of Surfshark,
- Physical security testing of IT infrastructure,
- Access rights testing related to VPN and IT infrastructure.

The procedures performed do not constitute a financial audit according to the International Standards on Auditing, nor an examination of compliance with laws, regulations, or other matters. Accordingly, our performance of the procedures does not result in an expression of an opinion, or any other form of assurance on Surfshark's compliance with laws, regulations, or other matters.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our independent reasonable assurance report conclusion.

Our reasonable assurance engagement is performed as of 02 December 2022. The procedures we performed do not provide any assurance about "Surfshark's No Logs Policy" for any other period.

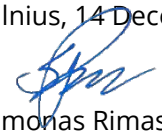
Conclusion

Based on the procedures performed and the evidence obtained, in our opinion, the configuration of IT systems and management of the supporting IT operations is properly prepared, in all material respects in accordance with the Surfshark's description set out in the Appendix I, as of 02 December 2022.

Restriction of use and distribution

Our report is solely for the purpose set forth in this report and for the information of Surfshark and their customers. It is not to be used for any other purpose or to be distributed to any other parties. We do not accept or assume any liability or duty of care for any other purpose or to any other person other than Surfshark's Management.

Vilnius, 14 December 2022



Simonas Rimasauskas

Appendix I: Surfshark's Statement: No Logs Policy Statement

We have prepared the accompanying description on how we protect the privacy of our customers by having effective policies and controls in-place to ensure that our IT systems and underlying infrastructure regarding VPN services is designed and implemented with no-log configuration. We confirm, to the best of our knowledge and belief, that:

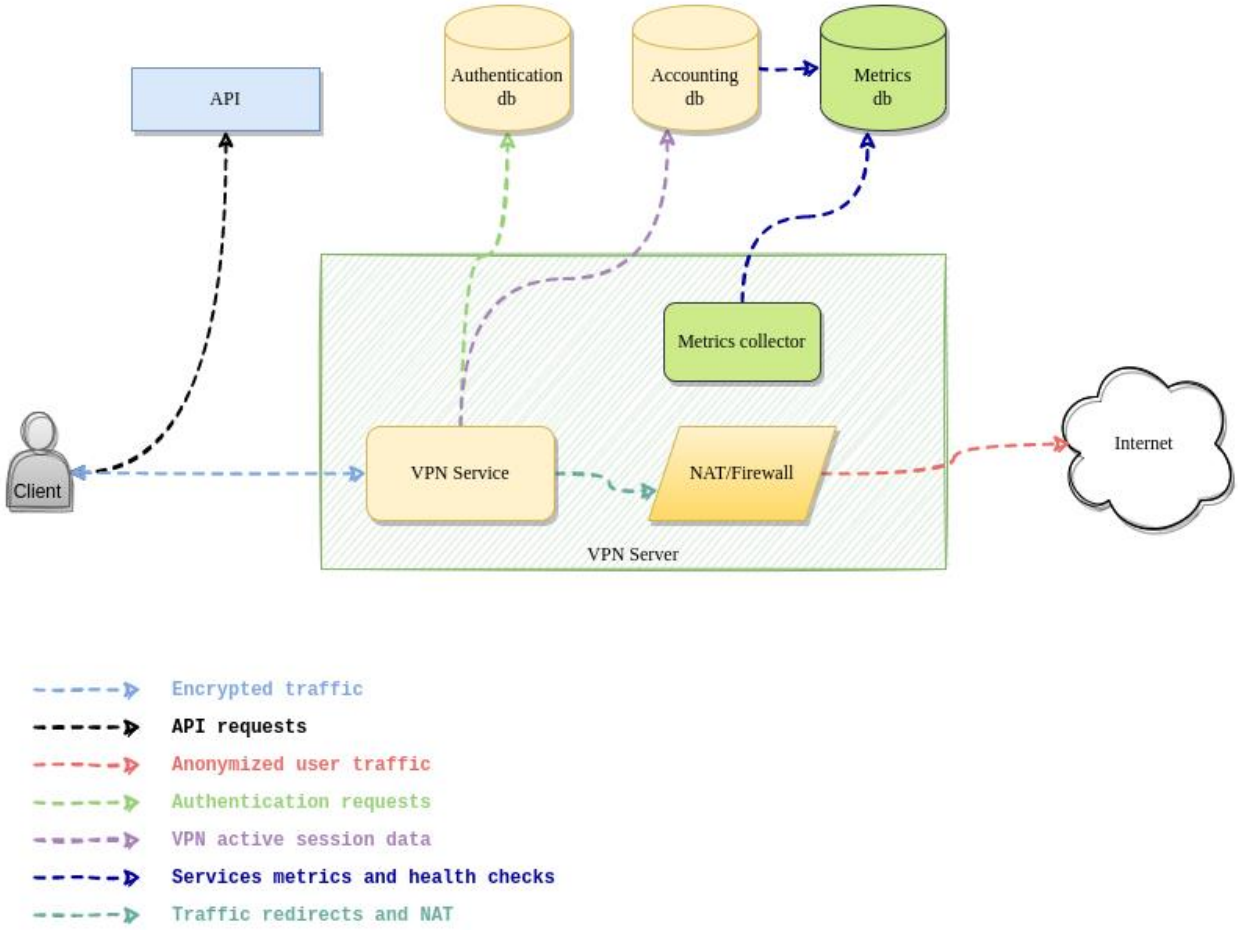
a) The accompanying description fairly presents how Surfshark configures the IT systems and manages the supporting IT operations to ascertain that no user logs are recorded and stored, related to customers' activity:

- We process only minimal user information – only as much as it is absolutely necessary to maintain our services (email address, encrypted password, basic billing information and order history)
- Our servers do store information about user's connection to a particular VPN server (user ID and connection time stamps), but this information is automatically deleted within 15 minutes after termination of user session. Please note that this information has nothing to do with the user's browsing activities
- We do not store any incoming and outgoing traffic data, including user and destination IP addresses, browsing history / websites visited, amount of data transferred, the VPN servers used, DNS queries or files downloaded
- We collect operating system diagnostics information (like ram usage, cpu usage, service health, etc.)
- The authentication servers count the total number of successful connections, but no individual data is collected. We collect only the aggregated raw number of users currently connected to the server (but not their IPs, identities, or activity)
- The containers are isolated at the network level and logging is turned off for them during the deployment process before users can even access the service
- In addition to disabling logging at the container level, logs are also turned off at the service level for all services by redirecting their output to the null device (/dev/null)
- All VPN servers run entirely on RAM disk . Once a VPN server loses power or is rebooted, all data associated with it is immediately and irreversibly deleted
- All new servers are deployed automatically via pre-defined playbooks including no-log configuration

b) the Surfshark service is implemented as described in the description as of 02 December 2022.

In a summary, our system architecture is designed so that Surfshark cannot be compelled to provide any type of information on its users' VPN activity, because that information does not exist. We do not know anything about our users' online activities while they are using our services.

Surfshark High Level Architecture



Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see https://www2.deloitte.com/lt/en/pages/about-deloitte/articles/about-deloitte.html to learn more about our global network of member firms.

Deloitte is a leading global provider of audit and assurance, consulting, legal, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 330,000 professionals make an impact that matters, visit www.deloitte.com.

© 2022. For more information, contact Deloitte Lithuania.