Deloitte.

nordvpn s.a

Independent Reasonable Assurance Report

December 13th, 2023

To the Board of Directors of
nordvpn s.a.

Fred. Roeskestraat 115, 1076 EE Amsterdam;

We have been engaged by nordvpn s.a. (hereinafter "NordVPN" 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 were concluded on December 7th, 2023.

We performed our assurance procedures between 30th November and 7th December 2023.

Responsibilities of the Engaging Party

The Management of NordVPN is responsible for preparing NordVPN's configuration of IT systems and management of the supporting IT operations. Also to prepare 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 of the description of "NordVPN's configuration of IT systems and management of the supporting IT operations" prepared by the Management of NordVPN. This responsibility includes the design, implementation and maintenance of the internal control system related to the preparation of NordVPN'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 NordVPN 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 fulfill our other ethical responsibilities in accordance with the IESBA Code.

Our firm applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality management, 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 reasonable assurance report and to express a conclusion on the fair presentation of NordVPN'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 NordVPN'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 of the description of NordVPN's no logging safeguards prepared by the Management of NordVPN as of 07th December 2023.

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.

As part of the procedures to create an Independent Reasonable Assurance Report, we performed the following audit procedures:

- Inquiries with responsible NordVPN employees;
- Review of the statement and description in Appendix I to verify whether the description fulfills the required relevant level of details and covers all relevant assertions made in the statement;
- Inspection of relevant IT systems (Standard VPN servers, Double VPN servers, Obfuscated servers, Onion Over VPN (TOR) servers and P2P servers) and verification of their configuration against the description provided. The inspection and technical review were done on the IT infrastructure and configuration files provided by NordVPN;
- Review of the aforementioned server's configuration and deployment process;
- Review of privacy relevant configuration settings and procedures, inspect whether the settings are in line with the "Privacy VPN service NordVPN" (Appendix I) including, but not limited to: SmartPlay Redirects; CyberSec/MalwareSec Blocks, SaltStack and verification of their configuration against the description provided.

The following procedures are out of the scope of this engagement:

- 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.
- Data transfer security and security measures in place for the protection of data and systems of NordVPN.
- We are not performing any audit procedures covering dedicated IP servers.
- We are not performing any audit procedures covering SmartDNS, including BIND, HAProxy or SNI Proxy.
- We are not performing any audit procedures covering the assessment of the internal control environment for the maintenance and operation of the system environment of NordVPN.
- We are not performing any audit procedures around security measures in place for the protection of data and systems of NordVPN.
- We are not performing any physical security testing or access rights testing of the related IT infrastructure. We are not testing the SLAs with other providers.

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 NordVPN'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 07th December 2023. The procedures we performed do not provide any assurance about "Privacy VPN service NordVPN" 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 NordVPN's description set out in the Appendix I, as of 07th December 2023.

Restriction of use and distribution

Our report is solely for the purpose set forth in this report and for the information of NordVPN 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 NordVPN's Management.

Vilnius, 13th December 2023

Rimasauskas, Simonas

Appendix I: NordVPN Statement Privacy VPN service NordVPN

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

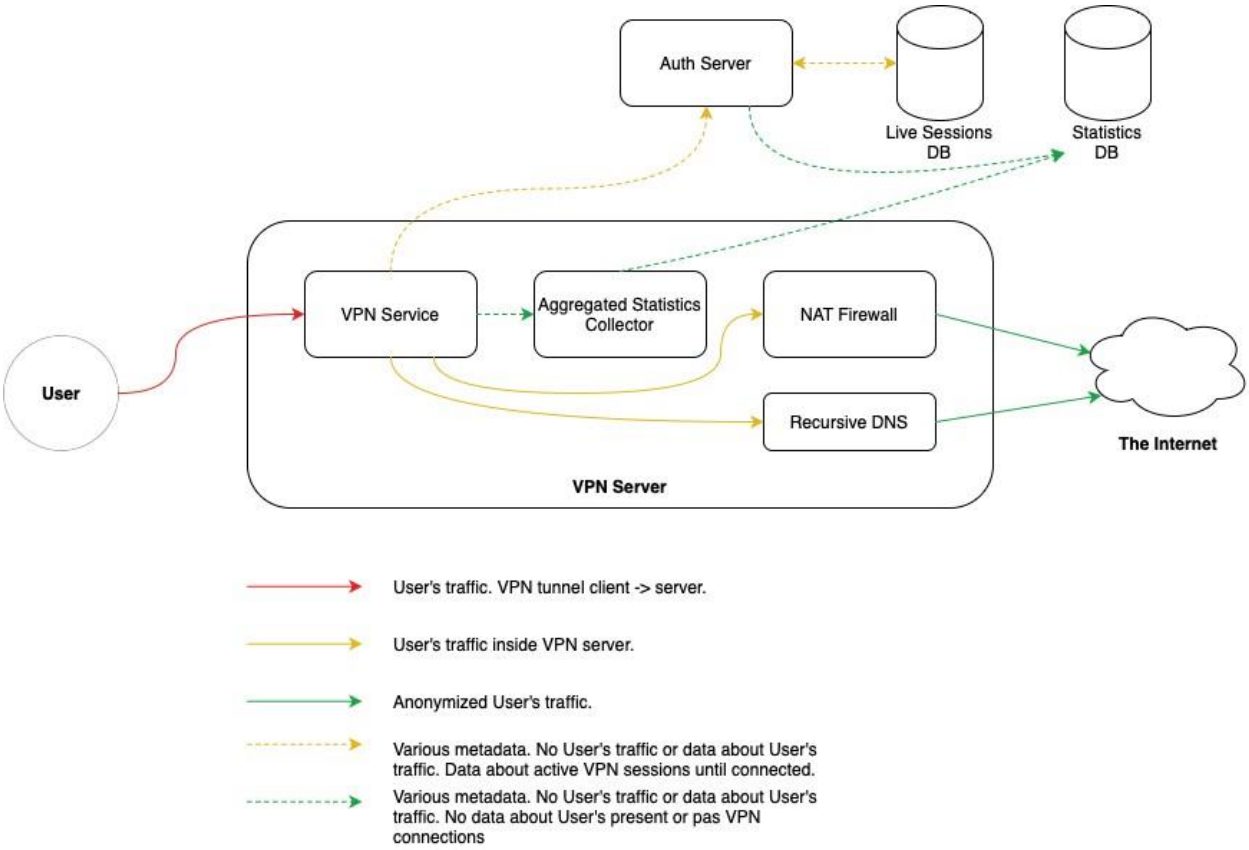
a) The accompanying description fairly presents how NordVPN configures the IT systems and manages the supporting IT operations to ascertain that NordVPN does not record and store any user logs related to customers' activity:

- 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).
- In order to authenticate a user, the NordVPN authentication server verifies the user credentials, subscription status (checks whether the user is active or not) and whether the user has not reached the limit of concurrent active user sessions. The authentication servers count the total number of successful connections, but no individual data is collected — only the aggregated raw number of users currently connected to the server (but not their IPs, identities, or activity).
- Session information is periodically sent to the NordVPN authentication server for as long as the session is active. The information contains the username and the timestamp of the last session status. The aforementioned information is used to limit the amount of concurrent active user sessions and is deleted within 15 minutes after a session is terminated.
- NordVPN authentication and VPN servers collect different anonymous, aggregated statistical information:
    - The authentication servers count the total number of all successful connections per user per month. However, they collect no information about the servers the user was connected to or the time of any of these connections.
    - The VPN servers collect the total number of all connected users and some system metrics (network traffic, CPU, memory and disk usage data, as well as running processes).
- We do not store any incoming or 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.
- When a user connects to any NordVPN VPN server, all communication between the user and the server is encrypted.
- 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 on RAM. Once a VPN server loses power, all data associated with it is immediately lost.
- All new servers are deployed automatically via pre-defined playbooks including no-log configuration

b) The NordVPN service is implemented as described in the description as of 7th December 2023.

In summary, our system architecture is designed so that NordVPN 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.

NordVPN High-Level Architecture



Deloitte.