Surfshark®

SURFSHARK ISAE 3000 TYPE I INDEPENDENT REASONABLE ASSURANCE REPORT

REPORTING DATE: 30 OCTOBER 2026



Table of contents:

1. **Table of contents** 2
2. **Independent Practitioner's Reasonable Assurance Report** 3
3. **Statement by the Management** 7
4. **Description of the Subject Matter** 8

3.1. Background 8

3.2. Overview 8

3.3. Scope of the report 8

3.4. Privacy Policy 9

3.5. How Surfshark VPN servers comply with our Privacy Policy 9

3.5.1 Control Objectives 9

3.5.2 Significant processes and activities 10

3.5.3 Technology, data and supporting resources 12

3.5.4 Governance and risk management 12

3.5.5 Information and communication 12

3.5.6 Monitoring 12

3.5.7 Significant third-party dependencies 13

3.5.8 Third-party carve-out and Surfshark monitoring controls 13

3.5.9 Significant changes and subsequent events 13

4. **Appendix A - Defined Terms** 14

KPMG Baltics, UAB
Lvivo g. 101
LT 08104 Vilnius
Lithuania

+370 5 2102600
vilnius@kpmg.lt
home.kpmg/lt

Independent Practitioner's Reasonable Assurance Report

To the Management of Surfshark

Report on the description and design and implementation of controls supporting Surfshark no-logs VPN service as at 30 October 2026.

Opinion

We have performed a reasonable assurance engagement on the description of the Surfshark no-logs VPN service provided by Surfshark ("the Entity") and the related control objectives and controls identified by management as described in Section 3 Description of the Subject Matter ("the Description"), as at 30 October 2026 ("the Reporting Date"), against the criteria described in the Management Statement in Section 2 ("the Criteria"). In our opinion, in all material respects, based on the Criteria:

a) the Description fairly presents the Surfshark no-logs VPN service as designed and implemented as at 30 October 2026; and
b) the control activities related to the control objectives stated in the Description in Section 3 were suitably designed and implemented as at 30 October 2026 to achieve those control objectives.

Scope

Our opinion does not extend to the operating effectiveness of those controls over a period, to controls operated by third-party providers that are excluded from the scope described in Section 3, or to any other information accompanying the assured Description and control information and our report.

The scope of our engagement is limited to the following aspects of the Subject Matter:

- whether the Description in Section 3, together with the control objectives and controls identified by management in Section 3, fairly presents the Subject Matter as designed and implemented as at the Reporting Date; and
- the controls identified by management as necessary to achieve the stated control objectives were suitably designed and implemented as at the Reporting Date based on the criteria identified in the Management Statement in Section 2.

Our opinion is set out above and should be read and considered in conjunction with this report in full. While the controls and related control objectives may be informed by the Entity's need to satisfy legal or regulatory requirements, our scope of work and our opinions do not constitute assurance over compliance with those laws and regulations.

© 2026 KPMG Baltics, UAB, a Lithuanian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Company code: 111494971
VAT code: LT114949716

Surfshark uses third-party hosting providers and Amazon Web Services to host elements of the infrastructure supporting the Subject Matter. Controls operated by those third parties are excluded from our assurance scope. Surfshark-operated controls over the related dependencies are included only to the extent described in Section 3.

Basis for opinion

We conducted our engagement in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). Our responsibilities under this standard are further described in the "Our responsibilities" section of our report.

We have complied with the independence and other ethical requirements of the *International Code of Ethics for Professional Accountants (including International Independence Standards)* issued by the International Ethics Standards Board for Accountants (IESBA), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Each of our firms applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, issued by the IAASB. This standard requires each firm to design, implement and operate a system of quality management, including documented policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Intended users and restriction on use

Our opinion is not modified in respect of the intended use and restriction on use described below.

This report has been prepared solely for the purpose of providing assurance in relation to the VPN services of Surfshark and the controls described in this report. The intended users of this report are Surfshark, its existing and prospective customers of the VPN services to whom the report is made available in accordance with the agreed terms and conditions of use.

This report is intended solely for the intended users specified above and for the purpose described in this report. It must not be used or relied upon for any other purpose.

This report constitutes a single and integral document and may only be distributed, published or otherwise provided to third parties in its entirety and without omission. Our assurance conclusion must not be disclosed, quoted, reproduced or distributed separately from the complete report. Any distribution of the report shall be subject to the applicable terms and conditions of use, which the recipient must accept.

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.

Management's responsibilities

Management of Surfshark is responsible for preparing the Description in Section 3 and the Management Statement in Section 2, including the completeness, accuracy, and method of presentation of the Description and the Management statement; operating the Surfshark no-logs VPN service covered by the Description; selecting or developing suitable criteria and appropriately referring to or describing them in the management statement; specifying the control objectives and stating them, together with the related controls in Section 3; identifying the risks that threaten the achievement of the control objectives; and designing, implementing, and documenting controls that are suitably designed and implemented to achieve the related control objectives if operated as described.

© 2026 KPMG Baltics, UAB, a Lithuanian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Management is also responsible for designing, implementing and maintaining internal control relevant to the preparation of the Description, including the control objectives and related controls, and the Management Statement such that they are free from material misstatement, whether due to fraud or error.

Inherent limitations

The Description has been prepared to meet the common information needs of the intended users and may not include every aspect of the Subject Matter that a particular user may consider relevant. Because of their inherent limitations, controls may not prevent, or detect and correct, all errors, omissions or other events relevant to the stated control objectives. Controls may also become inadequate because of changes in circumstances, processes, technology or personnel, or because the degree of compliance with policies and procedures may deteriorate.

Accordingly, our opinion relates only to the fair presentation of the Description and the design and implementation of the controls as at the Reporting Date and should not be projected to any future date or period.

Our responsibilities

Our responsibility is to express an independent opinion on the Description of the Subject Matter and on the design and implementation of controls related to the control objectives stated in that Description, based on the procedures performed and evidence obtained. We are responsible for planning and performing the engagement to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls are suitably designed and implemented as at the Reporting Date, based on the Criteria, and for reporting our opinion to the Management of the Entity. Our assessment includes the risks of material misstatement of the Description and the information about control design and implementation, whether due to fraud or error.

Summary of the work performed as the basis for our opinion

We exercised professional judgement and maintained professional scepticism throughout the engagement and designed and performed procedures to obtain sufficient appropriate evidence to support our opinion. A reasonable assurance engagement involves performing procedures to obtain evidence about the disclosures in the Description and whether the controls are suitably designed and have been implemented. The nature, timing and extent of the procedures selected depend on our judgement, including the assessment of the risks, whether due to fraud or error, that the Description is not fairly presented and that the controls are not suitably designed and implemented, informed by our understanding of the Subject Matter and the engagement circumstances.

Our procedures also included evaluating the overall presentation of the Description, the suitability of the control objectives stated therein and the suitability of the Criteria.

Consideration of the control environment

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. Our consideration of the control environment included the following procedures, to the extent we considered necessary:

1. Inspection of relevant policies and enquiry about Surfshark's organisational structure and the allocation of responsibilities between the VPN, infrastructure and Security teams;
2. Discussions with management and with the personnel responsible for designing and operating the controls;
3. Observation of personnel performing their assigned duties; and
4. Discussion with management regarding the risk management process.

© 2026 KPMG Baltics, UAB, a Lithuanian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The control environment was considered in determining the nature, timing and extent of our procedures.

Procedures performed

Management provided us with the controls it identified as necessary to achieve each control objective, as described in Section 3, and we tested the design and implementation of each of them. Our procedures comprised enquiry of Surfshark personnel, inspection of system configurations, code and records, observation of processes and reperformance of selected checks, using samples covering each server type in scope. In summary:

- **No logs of user activity on VPN servers, including DNS:** inspected the configuration of a sample of VPN servers and the deployment process, and confirmed that servers run in memory only and that DNS query logging and system logging are disabled, including for the containers running the VPN services.
- **Temporary session data on RADIUS servers:** observed how session data is held and deleted, inspected logging settings and the central RADIUS database, and reperformed a check that no session records remained more than 15 minutes after the session ended.
- **Usage data:** inspected the settings and output of the monitoring tools and confirmed that only aggregate operational metrics are collected.
- **Protection from hosting providers and from changes on running servers:** inspected outage handling, redeployment, disk encryption and server accounts, and confirmed that hosting providers have no operating system access.
- **Changes to systems and code:** observed a change from request to deployment, and inspected approval, segregation of duties and access settings.
- **Privileged access:** inspected access settings, reperformed connection attempts that should be refused, and observed how access is granted, recorded and removed.

These procedures were directed to design and implementation as at the Reporting Date, not to operating effectiveness over a period, and we do not express an opinion on operating effectiveness.

On behalf of KPMG Baltics, UAB

Rūta Kupinienė
Lithuanian Certified Auditor
Auditor's Certificate No. 000541

Håkan Svensson
Swedish State Authorized Public Accountant / CISA

11 November 2026
Vilnius, Lithuania

The electronic auditor's signature applies only to the Independent Practitioner's Reasonable Assurance Report on pages 3 to 6 of this document.

© 2026 KPMG Baltics, UAB, a Lithuanian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2. Statement by the Management

The accompanying description has been prepared for the intended users identified in this report to understand the design and implementation of the controls supporting the provision of the Surfshark no-logs VPN service (the subject matter), provided by Surfshark as at 30 October 2026 (the Reporting Date).

We confirm that, to the best of our knowledge and belief, and based on the criteria described below:

a) the description in Section 3 fairly presents the subject matter as designed and implemented as at the reporting date. The criteria used in making this statement were that the description fairly presents the Surfshark no-logs VPN service where it:

- identifies the nature, purpose and scope of the subject matter;
- describes the significant processes, activities, technologies, personnel and supporting resources relevant to the stated control objectives;
- identifies significant third-party dependencies and outsourced activities, where applicable;
- identifies relevant governance, risk management and monitoring activities;
- identifies complementary controls and assumptions, where applicable;
- includes material changes affecting the subject matter up to the reporting date; and
- does not omit or misstate information that could reasonably be expected to influence the decisions of the intended users.

b) the controls identified in Section 3 were suitably designed to achieve the stated control objectives if operated as described and had been implemented as described as at the Reporting Date. The criteria used in making that statement were that:

(i) the risks that threatened achievement of the stated control objectives were identified;
(ii) the identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

Signed on behalf of management	Dovydas Godelis
Position	Chief Executive Officer, netflow, UAB
Place	Vilnius, Lithuania
Date	11 November 2026

3. Description of the Subject Matter

The following section describes:

1. Surfshark's offered services.
2. How our Privacy Policy relates to our VPN service and no-logs feature.
3. Surfshark VPN infrastructure.
4. Surfshark's compliance with the no-logs promise.

3.1. Background

Surfshark is a major global VPN provider, helping millions of users access the internet privately and securely through servers located in more than 130 countries. Since launching its core VPN service, the company has broadened its offering to include a wider range of privacy and security tools. With just a few clicks, users can connect to the VPN and protect their online privacy and security.

3.2. Overview

Surfshark's publicly available Privacy Policy describes how information is handled, from collection through use and storage, and identifies information the company does not gather. To run its VPN service reliably at scale while prioritizing customer privacy, Surfshark limits data collection to what is necessary for the service to operate.

3.3. Scope of the report

This report examines the safeguards Surfshark uses to support the no-logs commitments in its Privacy Policy (https://surfshark.com/privacy). It covers how the company protects code as it moves through development, building and deployment, and the operating requirements applied to its servers over their service lifecycle.
Together, these measures are designed to preserve system integrity and to prevent logs of user activity from being collected.

In scope are the VPN servers (Standard, Static IP and Multiport) and the DNS processing on them, the RADIUS authentication and accounting servers, the central RADIUS database hosted in AWS, deployment code and configuration repositories, privileged access tooling, and security and operational monitoring tools, to the extent they support the control objectives in Section 3.5.1.

The scope does not extend to Surfshark systems, products, services or business processes that are not described in this Section 3 or addressed by the control objectives in Section 3.5.1. It excludes Dedicated IP servers, VPN-related API microservices, Surfshark's other products and features such as client applications and browser extensions, and the website, user account and payment systems, as well as streaming related proxy servers. This description presents the system and controls as at the Reporting Date, 30 October 2026.

Third-party hosting providers, Amazon Web Services and other third-party service providers are addressed only to the extent that Surfshark's own controls over the related dependencies are described in this report. Controls operated by third parties are not included in the Subject Matter or the assurance conclusion.

3.4. Privacy Policy

Below are relevant passages from Surfshark's Privacy Policy, effective 12 October 2026, located on the Surfshark website.
These excerpts show the commitments the control objectives are based on. KPMG's opinion covers the description and the controls, not the Privacy Policy itself.

How do we handle your connection data?

No-logs Policy is one of the most important features of our VPN service and we keep our VPN service logs-free.
We don't store any information that could lead us to see your online activities.
Surfshark respects your privacy, therefore, we are committed to not process any information related to the online activity of our users. Surfshark is based in the Netherlands jurisdiction, which does not require information storage or reporting. We do not collect any information about what you do online (i.e., we do not collect your visited IP addresses, browsing history, session information, connection time stamps, used bandwidth, network traffic or any other similar information).
To ensure the functionality of our VPN service, our servers temporarily keep details about your connection to a specific VPN server, such as your user ID and / or your IP address and connection to VPN server time stamps.
However, this information is automatically deleted within 15 minutes after your session ends. Rest assured, we do not store any information about the websites you visit.

3.5. How Surfshark VPN servers comply with our Privacy Policy

3.5.1 Control Objectives

Surfshark's management has set the following control objectives, based on the no-logs commitments in the Privacy Policy excerpts in Section 3.4. The controls designed to achieve them are described in the rest of this section.

Control objective 1

Controls provide reasonable assurance that Surfshark VPN servers, including the DNS service that runs on them, do not record or store logs of users' activity after login: no browsing history, traffic destination, data content, DNS queries or records of individual connections.

Control objective 2

Controls provide reasonable assurance that the Surfshark RADIUS servers keep users' login session data only temporarily, and delete it no later than 15 minutes after the session ends.

Control objective 3
Controls provide reasonable assurance that usage analytics data collected from VPN servers is limited to aggregate operational metrics that do not identify individual users, in line with the Surfshark Privacy Policy (effective 12 October 2026).

Control objective 4
Controls provide reasonable assurance that Surfshark protects VPN user data on its servers from access by hosting providers, and that an unapproved change made to a running server does not remain in place beyond the next redeployment.

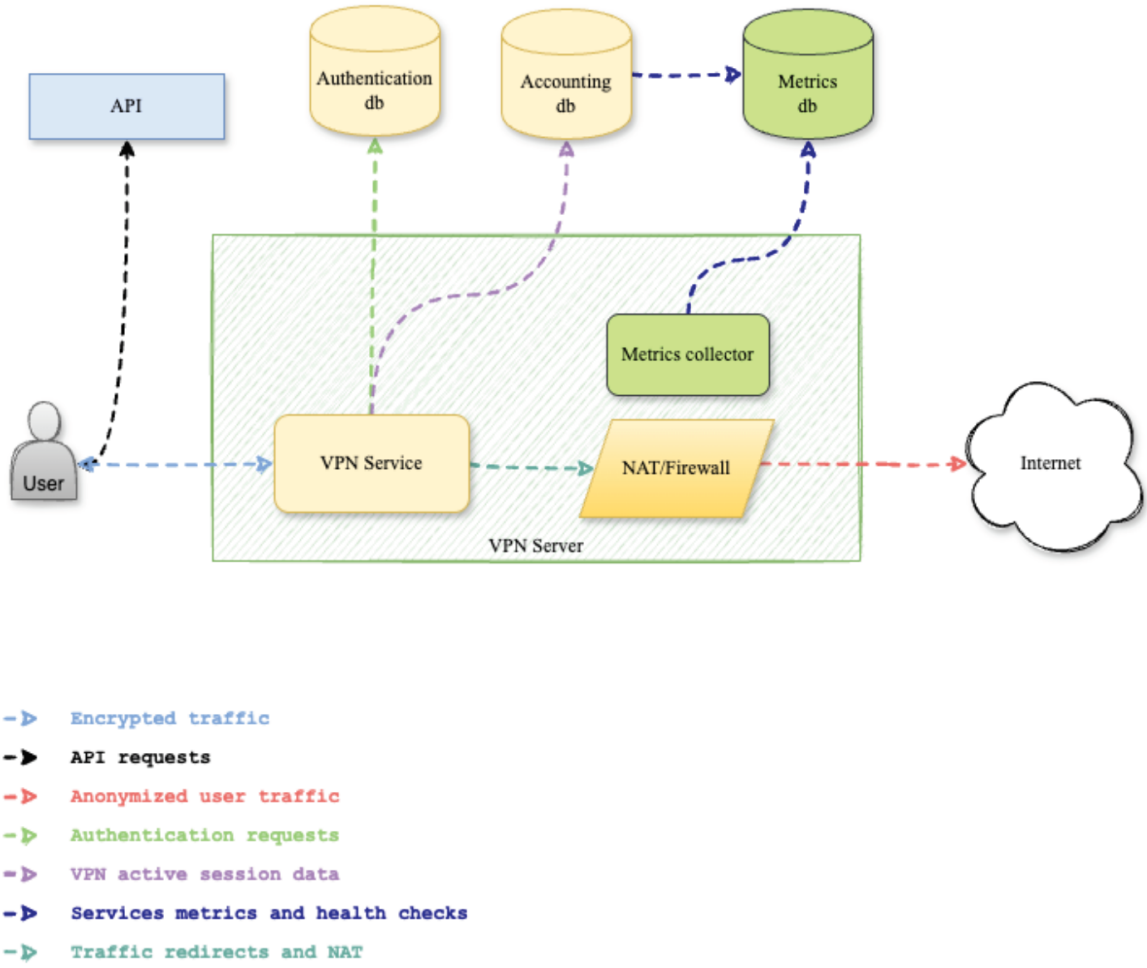
Control objective 5
Controls provide reasonable assurance that changes to Surfshark VPN's IT systems, code, and configurations are appropriately authorized, documented, and implemented in a manner that preserves system integrity and prevents unauthorized modifications.

Control objective 6
Controls provide reasonable assurance that privileged access to VPN and RADIUS servers is limited to authorised personnel using approved access paths, granted only after approval and removed when an employee leaves, and that administrator actions are recorded and monitored.

3.5.2 Significant processes and activities

Surfshark configures its IT systems and manages the supporting IT operations so that no logs of user activity are recorded or stored. In summary:

- Our servers do store information about a user's connection to a particular VPN server (user ID, IP addresses 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
- Other than the temporary session data described above, 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.



VPN service and RADIUS servers are built and configured automatically from deployment code held in version control and run through CI/CD pipelines. Every change to this code requires a Jira ticket and approval by a designated code owner other than the author before it can be merged, and only approved versions are deployed.

During deployment, system logging is disabled and log directories are emptied, existing log files are removed, and the VPN services that handle user traffic, including DNS resolution, run without activity or query logging. VPN servers run entirely in memory (RAM): on every boot, the operating system image is downloaded from the network, the local disk is not used to store data, and everything held in memory is lost on reboot. The deployment pipeline confirms that each server is running from memory and stops if it is not, and servers are redeployed from the approved build at least every 5 weeks.

Surfshark does not retain data about users' online activity. The only data held about users' connections is the session data that the RADIUS accounting servers need while a session is active, which is deleted within 15 minutes after the session ends. An automated job deletes ended sessions every minute, and sessions that have not been updated for 10 minutes. RADIUS servers do not log login requests or responses, database change logs are removed within 15 minutes, and the central RADIUS database holds only the data needed to authenticate users, with no session or connection data. Usage data is collected only as aggregate operational metrics without user-identifiable information.

3.5.3 Technology, data and supporting resources

The system consists of VPN servers on dedicated hardware in third-party data centers; RADIUS authentication and accounting servers on dedicated hardware with encrypted disks; and a central RADIUS database hosted in Amazon Web Services (AWS). After a restart, the RADIUS servers do not start until authorised Surfshark staff unlock the encrypted disks through an approved method. Deployment code, server configuration and boot images are held in Surfshark-managed GitLab repositories, with a separate repository for each service and access granted per repository and role. Privileged access is provided through Teleport and administrator jump servers.

Records relevant to the controls are change tickets in Jira, code review approvals in GitLab, deployment pipeline logs, Teleport audit logs and session recordings, and access requests in Jira Service Desk. The VPN team owns server configuration and deployment, supported by the infrastructure team, and the Security team manages privileged access tooling, security monitoring and incident response.

3.5.4 Governance and risk management

A dedicated risk team maintains an internal risk register, risks are reported, triaged and reviewed with senior management on a regular basis. Risk treatment methods are selected and tracked. Access follows the principle of least privilege. Privileged access requires a request approved by the employee's manager and the Security team, uses multi-factor authentication, and is possible only through Teleport and approved jump servers, where administrator activity is recorded. Server access allows only public key authentication, password login is disabled, and login is restricted exclusively to designated jumpbox servers. Access is removed when an employee leaves. Security monitoring is maintained continuously using internal security software, and hosting providers are strictly restricted to physical/out-of-band IPMI hardware management with no root or OS-level access. Privacy policies are maintained by in-house legal counsel and updated whenever data processing practices change.

3.5.5 Information and communication

Internally, Wazuh security alerts are sent automatically to the Security team, server outages automatically raise tickets, and monitoring and deployment alerts are sent to the responsible teams. Changes are documented in Jira tickets linked to the code changes, and access requests and leaver access removals are tracked in Jira Service Desk. Externally, Surfshark communicates its no-logs commitment to users through its published Privacy Policy, which in-house legal counsel reviews and updates regularly when data processing practices change and/or new products and/or features are introduced.

3.5.6 Monitoring

Server health and operational metrics are monitored continuously including security events. Deployment pipelines automatically check that VPN servers successfully boot exclusively into RAM; any failure during this verification halts the deployment process.

3.5.7 Significant third-party dependencies

Surfshark relies on third-party hosting providers for server hardware, physical facilities, network connectivity, and out-of-band (IPMI) access. Traffic between users and the VPN servers is encrypted. Hosting providers can observe connection metadata and traffic leaving the servers, and Surfshark does not control logging on provider networks. The protection of user data relies on encryption and memory-only servers rather than on provider contracts. Surfshark also relies on Amazon Web Services (AWS) to host the central RADIUS database.

3.5.8 Third-party carve-out and Surfshark monitoring controls.

Third-party hosting providers and Amazon Web Services are carved out of the scope of this report. Surfshark relies on third-party hosting providers for server hardware, physical facilities, network connectivity and out-of-band IPMI access; however, the providers' own controls are not included in the scope of the assurance conclusion. Surfshark's protection of user data relies on encryption, memory-only VPN servers and Surfshark-operated access, deployment, monitoring and incident follow-up controls, rather than on the design and implementation of hosting provider controls. Surfshark continuously monitors server health, operational metrics and security events, automatically raises tickets for server outages, investigates unexpected restarts or outages, and does not redeploy affected services until investigation has been completed.

3.5.9 Significant changes and subsequent events

The Privacy Policy was updated with an effective date of 12 October 2026, clarifying the analytics and diagnostic data processing scope. No other material changes occurred up to the Reporting Date, and no significant events have occurred between the Reporting Date and the date of this report.

Appendix A - Defined Terms

Surfshark, Entity	Netflow, UAB, the legal entity that engaged KPMG, to whose management this report is addressed and which operates the Surfshark no-logs VPN service described in Section 3.
Control objectives	The objectives stated by management in Section 3.5.1 that the controls are designed to achieve.
Controls	The controls identified by management as necessary to achieve the stated control objectives.
Criteria	The criteria set out in the Statement by the Management in Section 2, against which the Description and the controls are assessed.
Description	Management's description of the Subject Matter in Section 3, including the control objectives and controls.
Design and implementation	Whether the controls were suitably designed to achieve the control objectives and had been implemented as at the Reporting Date. It does not cover whether the controls operated effectively over a period.
Intended Users	The users identified in Intended users and restriction on use in Section 1.
Reporting Date	The 30 October 2026.
Subject Matter	The Surfshark no-logs VPN service, as described in Section 3.