netskope

Compliance Series

Using the Netskope Platform to

Support Compliance with the Australia Privacy Act and Privacy Principles

TABLE OF CONTENTS

INTRODUCTION	3
NETSKOPE PRODUCTS OVERVIEW	6
HOW TO USE THIS GUIDE	7
NETSKOPE PRODUCTS	7
AUSTRALIAN PRIVACY ACT 1988	8
AUSTRALIAN PRIVACY PRINCIPLES	13

INTRODUCTION

In Australia, the main data privacy law is the Privacy Act 1988 (“Act”). This Act governs how personal information is collected, used, and disclosed by organisations and agencies. It includes the Australian Privacy Principles (APPs) which set out standards for handling personal information. Additionally, there are specific provisions related to health information and credit reporting. The Act is overseen by the Office of the Australian Information Commissioner (OAIC), which handles complaints and provides guidance on privacy issues.

Australia is undergoing a significant overhaul of its data privacy laws to align more closely with global standards, particularly the EU's GDPR. The government has accepted or conditionally supported 106 of 116 recommendations from its Privacy Act Review, focusing on enhancing individual protections and corporate accountability. Key reforms include granting individuals the right to sue for privacy breaches and seek compensation, expanding protections to employee data while removing exemptions for small businesses, imposing tougher penalties and stricter breach notification requirements, and introducing special provisions for the protection of children’s data. These changes are expected to be legislated progressively over 2024-2025, modernising the privacy framework for the digital age.

The link to the official law text with amendments is available here.

Scope and Applicability:

The Act and APPs apply to all Federal agencies and private sector organisations, except those with less than AUD 3 million turnover, registered political parties, and State/Territory authorities. However, the notifiable data breaches provisions involving Tax File Numbers (TFNs) apply to all. Following the Uber Decision and December 2022 changes, foreign organisations "carrying on business" in Australia are subject to the Act, regardless of whether they process personal information in Australia. The Act covers all personal information processing by APP entities, excluding de-identified data, purely domestic activities, employee records, and media organisations engaged in journalism.

Personal Information:

Personal information refers to any information or opinion about an individual who is identified or can be reasonably identified, whether it's true or not, and whether it's recorded in any form or not.

Sensitive Information:

Sensitive information refers to personal or health-related details about an individual, including their racial or ethnic background, political opinions, political or professional memberships, religious or philosophical beliefs, sexual orientation or practices, criminal record, genetic information (if not related to health), or biometric data used for automated identification or verification.

Health Information:

Health information refers to personal details or opinions about an individual's health, including any illness, disability, or injury, their wishes regarding future health services, or any health service they have received or will receive. It also includes personal information collected to provide health services, details related to body part or organ donations, and genetic information that can predict the health of the individual or their relatives.

Lawful Basis for Processing Data:

Unlike GDPR, the Privacy Act/APPs do not mandate specific legal bases for processing personal information. Non-sensitive personal information can be collected if it is necessary for an entity's functions or activities, provided a notice (as per APP 5) is given at or before collection. Consent, whether expressed or implied, is required for collecting sensitive information (including health information) under APP 3.3, but only if it is reasonably necessary for the entity's functions. A contract between the entity and individual may satisfy consent requirements, and legal obligations may exempt the need for consent while still requiring notice. Sensitive information can also be collected without consent to assist in locating missing persons, prevent serious threats to life or public safety, or investigate unlawful activity. Entities may also collect sensitive information for legal claims or alternative dispute resolution. However, the main precondition for collecting both personal and sensitive information is that it must be reasonably necessary for the entity's functions or activities. If required by law or court order, this condition is automatically met, but if merely permitted by law, the necessity must still be demonstrated in some cases.

Data Subject Rights:

Individuals have several data protection rights, including the right to be informed when personal information is collected, the right to access and request corrections to their data, and the ability to opt out of direct marketing. While there is no explicit right to erasure, entities must delete or de-identify data once it's no longer needed. Additionally, individuals may interact anonymously with entities, except where impractical or legally required.

International Data Transfers:

Data transfers are generally permitted without specific restrictions, but must comply with the Australian Privacy Principles (APPs) 3 and 6, which ensure that personal information is used as communicated to individuals and protected adequately. For transfers outside of Australia, APP 8 mandates that organisations take "reasonable steps" to ensure overseas recipients comply with APPs 2-13, with the Australian entity remaining liable for any breaches. However, exceptions exist for transfers to countries with laws that are "substantially similar" to the APPs, or when explicit consent is obtained from the individual. Entities are also required to inform individuals if their data will be transferred overseas and disclose the destination when possible. Noncompliance can result in penalties of up to AUD 50 million for organisations and AUD 2.5 million for individuals. Additionally, certain industries like financial services face stricter offshoring regulations, while health and tax data have specific regional transfer restrictions within Australia.

Data Breach Notifications:

In Australia, all "eligible data breaches" must be reported to the OAIC and affected individuals unless a specific exemption applies. Notification is required as soon as practicable after the entity becomes aware of the breach, believes there are reasonable grounds to suspect a breach, or is directed by the Privacy Commissioner. An eligible data breach involves unauthorised access, disclosure, or loss of personal information held by an APP entity, where a reasonable person would believe it could cause serious harm to the affected individuals.

Penalties:

The OAIC can impose enforceable undertakings, award compensation, seek fines, and publish determinations detailing infringement and investigation results. Ultimate sanctions include applying to the court for fines of up to AUD 50 million (or 30% of revenue during the breach period) for entities and AUD 2.5 million for individuals for serious or repeated breaches of the APPs, as well as requiring APP entities to remediate their technology and data handling practices to ensure compliance. Additionally, the OAIC may request compliance information from entities regarding the Notifiable Data Breach scheme after a data breach.

The Australian Privacy Act 1988 is a crucial piece of legislation that safeguards individuals' personal information. It ensures that businesses and organisations collect, use, and disclose personal information responsibly and ethically. Compliance with this Act is essential to protect individuals' privacy rights and maintain trust in businesses. Failure to comply with the Act can result in serious consequences, including fines, legal action, and damage to reputation. Moreover, noncompliance can lead to significant financial losses and operational disruptions. By adhering to the Australian Privacy Act, businesses can demonstrate their commitment to responsible data handling and build strong relationships with their customers.

NETSKOPE PRODUCTS OVERVIEW

Netskope's products can be used as a technical control to assist organisations in supporting compliance efforts with the Act through several key features and capabilities:

Data Protection:

Data Loss Prevention (DLP): Netskope provides advanced DLP capabilities that monitor and protect sensitive data in the cloud, helping to prevent unauthorised access, sharing, or transfer of personal information, which is crucial for the Act's compliance.
Encryption and Tokenization: It ensures that personal information is encrypted both in transit and at rest, mitigating the risk of data breaches.

Visibility and Control:

Cloud Activity Monitoring: Netskope offers real-time visibility into cloud usage and data movement across cloud services, enabling organisations to monitor and control the processing of personal information as required by the Act.
User and Entity Behavior Analytics (UEBA): By analysing user behaviour, Netskope can detect and alert on suspicious activities that could indicate potential data breaches or the Act's violations.

Risk Management:

Risk Assessment: Netskope assesses the risk of cloud services and applications, helping organisations identify and mitigate potential risks associated with data processing activities.
Compliance Reporting: The platform provides detailed reports and audit trails that demonstrate compliance with the Act's requirements, making it easier to respond to data subject access requests (DSARs) and regulatory inquiries.

Incident Response:

Threat Protection: Netskope offers protection against malware and other threats that could lead to data breaches, a key concern under the Act.
Automated Incident Response: In the event of a data breach, Netskope helps automate response actions, such as alerting relevant teams and restricting access, which aids in meeting the Act's breach notification requirement.

Data Residency and Sovereignty:

Data Localization: Netskope supports data residency requirements by allowing organisations to enforce policies that ensure personal information remains within specific geographic regions, addressing the Act's restrictions on cross-border data transfers.

By providing these tools and capabilities, Netskope helps enable organisations to protect personal information, maintain control over their data processing activities, and demonstrate compliance with the Act.

HOW TO USE THIS GUIDE

The Netskope platform consists of a suite of tools integrated into a unified Secure Access Service Edge architecture. This SASE architecture's capabilities provide controls to support compliance with several articles of the law. The tools can also be used to secure personal information, monitor compliance, and alert stakeholders where potential breaches or out-of-compliance processing is detected.

Netskope Products

Note the following acronyms and/or aliases for the Netskope products:

Industry Terminology	Netskope Product Line/Abbreviation
Security Access Service Edge	SASE
Security Service Edge	SSE
Next Gen Secure Web Gateway	NG-SWG
Cloud Access Security Broker	CASB
Public Cloud Security	Public Cloud Security
Zero Trust Network Access	ZTNA Next
Cloud Security Posture Management	CSPM
SaaS Security Posture Management	SSPM
Data Loss Prevention	DLP (Standard & Advanced)
Firewall as a Service	Cloud Firewall
Reporting and Analytics	Advanced Analytics
Threat Intelligence	Threat Protection (Standard & Advanced)
Remote Browser Isolation	RBI
Artificial Intelligence Security	SkopeAI
Software-Defined Wide Area Network (SD-WAN)	Borderless SD-WAN Secure SD-WAN Endpoint SD-WAN Wireless SD-WAN IoT Intelligent Accessl
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence

Industry Terminology	Netskope Product Line/Abbreviation
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

AUSTRALIAN PRIVACY ACT 1988

Requirement	Netskope Response	Products
Part I - Preliminary (Includes short title, commencement, objectives, territorial scope, etc.)	Netskope's security tools, including CASB and NG-SWG, are equipped with a data loss prevention (DLP) engine that maps the territorial scope of personal information processing across web, cloud applications, and endpoint devices. The DLP engine, powered by machine learning, aligns personal information identification with organisational and regulatory standards through predefined profiles. These tools enable the mapping of where personal information is processed, helping entities apply real-time, context-aware policies to manage data effectively. Moreover, the Advanced Analytics feature provides a detailed mapping of data flows, assisting entities in understanding and applying policies based on the territorial scope of the data processing.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Part II - Interpretation (Definitions)	This article sets out the key definitions and terms. Netskope's products do not directly map to this requirement.	
Part III - Division 1 (Interferences with privacy)	Part III deals with the definition of interference with someone's privacy and does not map to Netskope products.	
Part III - Division 2 (Australian Privacy Principles)	Refer to the Privacy Principles table for more detail on Netskope's products assistance with compliance with the Australian Privacy Principles.	

Requirement	Netskope Response	Products
Part III - Division 4 (Rules related to Tax File Number information)	Netskope's security solutions, such as CASB and NG-SWG, leverage a data loss prevention (DLP) engine to help organisations comply with privacy regulations. This engine, utilising machine learning, identifies and protects personal information across web, cloud applications, and endpoints in line with regulatory standards, including APPs, through predefined profiles. The DLP engine aids in detecting personal information-processing locations and applying context-aware policies that ensure compliance with the APPs, particularly in securing personal information in real time. Context-aware policies within Netskope's tools are capable of automatically encrypting personal information as required by privacy laws, including the secure handling of TFN information. Furthermore, Netskope's Advanced Analytics provides critical insights into the flow of personal information, enabling entities to apply policies that ensure compliance with territorial scope requirements under Australian law, including securing data during cross-border transfers. Netskope's solutions are designed to assist in managing cross-border data transfers in compliance with proper safeguards in place, and determining when derogations may apply, as required by privacy regulations. The Cloud Confidence Index (CCI) feature scores SaaS applications, offering details on each vendor's compliance with security policies, legal frameworks, and privacy requirements, thus assisting organisations in managing the risks associated with third-party cloud services. The ZTNA Next tool aligns with privacy regulations by securing remote access with zero-trust principles and supporting encrypted data transfer, ensuring personal information, including TFN information, remains protected. Netskope's Borderless SD-WAN extends network perimeters to any user or device, using Netskope's global NewEdge Network for high-availability connectivity and adaptive trust enforcement based on specific criteria assisting in protecting personal information. Netskope's Cloud Security Posture Management (CSPM) tool assists in maintaining compliance with technical and organisational measures (TOMs) as prescribed by the APPs by continuously monitoring IaaS environments to prevent misconfigurations that could lead to data breaches, particularly regarding personal information. CSPM's real-time scanning of cloud storage ensures that personal information, including TFN information, is protected from unauthorised access and exfiltration, integrating with Cloud Ticket Orchestrator for automated remediation. The SaaS Security Posture Management (SSPM) tool ensures ongoing compliance with the APPs by monitoring SaaS applications for misconfigurations that could expose personal information. SSPM's integration with the Cloud Ticket Orchestrator enables automated fixes for compliance violations, while its ability to convert past misconfigurations into new security rules supports continuous protection of personal information, including Tax File Number information. Lastly, Netskope's User Entity and Behavior Analytics (UEBA) tool monitors user behaviours to detect anomalies in data transfers that might violate privacy laws. By setting baselines for normal behaviour and adjusting security policies dynamically based on risk, UEBA assists organisations' compliance with regulations, especially in safeguarding personal information and TFN information.	• CASB • NG-SWG • Public Cloud Security • DLP • ZTNA Next • SD-WAN • CSPM • SSPM • CTO • CCI • UEBA • Advanced Analytics

Requirement	Netskope Response	Products
Part IIIA (Privacy of information relating to credit reporting)	Netskope's security solutions, such as CASB and NG-SWG, are designed with a data loss prevention (DLP) engine that helps identify and secure personal information across environments, including web, cloud applications, and endpoint devices. The DLP engine employs machine learning to classify and protect personal information, conforming to both organisational and legal standards through predefined profiles. In the context of credit reporting, this tool enables the mapping of personal information processing activities and the enforcement of context-aware policies, such as automatic encryption, to safeguard sensitive credit-related information in real time. Advanced Analytics within Netskope can further map the flow of credit-related personal information, helping entities manage the territorial scope of data processing. By showing where data is transferred, especially in cross-border scenarios, these tools ensure that the processing complies with legal requirements, such as adequacy decisions or approved safeguards. Netskope's DLP policies can automatically detect and encrypt personal information to meet credit reporting regulations, while Advanced Analytics helps visualise these flows for compliance assessment. Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications, providing critical insights into each vendor's risk, including security and privacy concerns related to credit reporting. This mapping allows organisations to assess whether these tools are appropriate for handling personal credit information. ZTNA Next secures remote access using zero-trust principles, ensuring that encrypted data transfer and login policies protect access to personal information related to credit reporting. Netskope's Borderless SD-WAN extends these protections across devices and users, applying adaptive trust criteria to safeguard such personal information. In cloud environments, Netskope's Cloud Security Posture Management (CSPM) ensures that misconfigurations in IaaS platforms are corrected, monitoring for compliance with technical and organisational measures required under credit reporting laws. CSPM's continuous scanning of cloud storage for potential personal information exfiltration ensures adherence to data protection laws. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of personal information. SSPM provides detailed remediation instructions, integrates with Cloud Ticket Orchestrator for service tickets from alerts, and automates fixes. Additionally, SSPM allows previously detected misconfigurations to be converted into new security rules to provide adaptive protection for personal information.	• CASB • NG-SWG • Public Cloud Security • DLP • ZTNA Next • SD-WAN • CSPM • SSPM • CTO • CCI • UEBA • Advanced Analytics

Requirement	Netskope Response	Products
Part IIIB (Privacy codes)	Netskope's security solutions, including CASB and NG-SWG, are designed with a data loss prevention (DLP) engine that serves as a tool for discovering and securing personal information across environments such as web, cloud applications, and endpoint devices. The DLP engine, powered by machine learning, aligns with the law's standards by identifying and protecting personal information based on predefined profiles reflecting regulatory requirements. This tool allows entities to map where personal information is processed and apply context-aware policies that comply with privacy provisions in real time. Furthermore, the discovery mechanism within the tool helps entities establish and map codes of conduct for personal information processing. By configuring DLP policies, the tool can enforce actions like encryption or quarantining of personal information when found outside sanctioned applications or providers, in alignment with the law's requirements. Additionally, the tool's Advanced Analytics feature aids in mapping the law's provisions to data flows, including understanding cross-border transfers and updating privacy codes of conduct as necessary.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Part IIIC (Notification of eligible data breaches)	Netskope's security solutions, including CASB and NG- SWG, utilise a data loss prevention (DLP) engine to discover personal information across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal information according to organisational and regulatory standards with pre- defined profiles. These products can assist entities in determining where personal information is being processed and applying context-aware policies to manage personal information in real time, ensuring compliance with breach notification provisions. Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with defined technical and organisational measures (TOMs), access management policies, regulatory, and industry standards such as protection of personal information. CSPM routinely scans cloud storage to prevent personal information exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation to meet the standards for breach notification. Similarly, the SaaS Security Posture Management (SSPM) tool continuously monitors SaaS functions to prevent misconfigurations that could compromise personal information. By providing detailed remediation instructions and automating fixes, SSPM ensures adherence to the regulatory requirements. It also allows previously detected misconfigurations to be turned into new security rules, adapting to the evolving legal framework for breach notification. The DLP engine helps the entities to determine the scope of the breach, identify affected data subjects, and ensure that the necessary notifications to authorities and impacted individuals are issued. Additionally, DLP detects records tied to data incidents and provides forensic reporting, aiding in the mitigation of data breaches in accordance with requirements. All of Netskope's products contribute to entities' ability to understand the scope of a breach and assess the need for notification to supervisory authorities or data subjects.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO

Requirement	Netskope Response	Products
Part IV (Functions of the Information Commissioner)	Part IV deals with the functions of the Information Commissioner and does not map to Netskope products.	
Part V (Investigations)	Netskope's security tools, including CASB and NG-SWG, use data loss prevention (DLP) engine to discover personal information across environments such as web, cloud applications, and endpoint devices. The DLP engine applies machine learning to identify personal information based on both organisational and regulatory standards, using predefined personal information definitions. These tools align with the law by enabling entities to identify where personal information is processed, facilitating compliance in legal investigations or audits.	• CASB • NG-SWG • Public Cloud Security • DLP
Part VI (Public interest determinations)	Part VI deals with public interest determinations by the Commissioner and does not map to Netskope products.	
Part VIA (Dealing with personal information in emergencies and disasters)	Part VIA deals with special provision for the collection, use and disclosure of personal information in emergencies and disasters, and does not map to Netskope products.	
Part VIB—Enforcement	Part VIB deals with enforcement provisions and does not map to Netskope products.	
Part VII—Privacy Advisory Committee	Part VII deals with a Privacy Advisory Committee consisting of commissioners and does not map to Netskope products.	
Part VIII—Obligations of confidence	Part VIII deals with obligations of a confidant and does not map to Netskope products.	
Part IX—Miscellaneous	Part IX deals with miscellaneous provisions such as guidelines, conduct of employees, review by authorities, etc, and does not map to Netskope products.	

AUSTRALIAN PRIVACY PRINCIPLES

Requirement	Netskope Response	Products
Principle 1 - Open and transparent management of personal information	Netskope provides open and transparent management of personal information by enforcing customizable cybersecurity and data privacy policies aligned with risk and regulatory requirements. Its Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms, preventing misconfigurations and ensuring compliance with access management and regulatory standards to protect data integrity. CSPM also scans cloud storage to prevent data exfiltration and integrates with the Cloud Ticket Orchestrator for automated alerts and remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) oversees SaaS applications, offering real-time monitoring and alerts for addressing configuration issues while automating remediation processes. Detected misconfigurations can be converted into actionable rules, enhancing security over time. Furthermore, Netskope's Advanced Analytics tracks data flows across web and cloud services, categorizing data by type and sensitivity to assess cloud risk and usage. This tool helps maintain transparency by supporting administrators in monitoring security trends, such as app access and threat detection, through its comprehensive dashboard. Together, these capabilities ensure that personal information is managed transparently and securely, consistent with the organization's policies and regulatory obligations.	• All products
Principle 2 - Anonymity and pseudonymity	Netskope's security solutions provide continuous monitoring for both IaaS and SaaS platforms, aiming to prevent misconfigurations that could lead to privacy risks. The Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) tools ensure compliance with organizational policies and regulatory standards, crucial for maintaining anonymity and pseudonymity by securing access to data according to intended purposes. By integrating with Netskope's Cloud Ticket Orchestrator, these tools automate remediation, minimizing human intervention and potential privacy breaches. CSPM also routinely scans cloud storage to prevent unauthorized data access or exfiltration, further protecting user identities. SSPM offers detailed remediation instructions and can adapt by creating new security rules from past incidents, continuously strengthening data protection protocols. Netskope's Advanced Analytics adds an extra layer of security by mapping data flows and assessing cloud app risks, helping administrators track data access, usage patterns, and potential threats. This detailed monitoring and risk assessment help maintain anonymity by ensuring that only authorized parties have access to sensitive data and that all data usage is meticulously tracked and controlled.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO

Requirement	Netskope Response	Products
Principle 3 - Collection of solicited personal information	Netskope provides detailed tools and analytics to help organizations assess and manage risks associated with SaaS applications and cloud services, focusing on security, legal, and privacy concerns. Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on various criteria, including security policies and certifications, and privacy issues. Advanced Analytics maps and assesses data flows across web and cloud services, offering insights into data categorization and sensitivity. Cloud Risk Exchange integrates risk scores from third-party plug-ins, such as Crowdstrike and ServiceNow, to enforce adaptive controls against high-risk users, apps, and devices. Netskope's Cloud Threat Exchange facilitates real-time sharing of threat indicators, enhancing companies' ability to manage security threats. Both Cloud Risk Exchange and Cloud Threat Exchange are included with Netskope deployments, helping organizations secure their data and manage cloud-related risks effectively. These features collectively support organizations in protecting personal information and satisfying legal and privacy requirements by delivering comprehensive insights and controls over cloud applications and potential threats.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • Advanced Analytics • CRE • CTE
Principle 4 - Dealing with unsolicited personal information	Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on various risk factors, helping organizations assess potential risks when dealing with unsolicited personal information. The CCI scoring criteria include an analysis of the vendor's security policies and certifications, their ability to conduct audits, and address legal and privacy concerns. This comprehensive approach enables businesses to make informed decisions about the safety and compliance of using specific cloud services, especially concerning the handling of unsolicited personal data. By considering these factors, organizations can better manage and mitigate risks associated with unauthorized or unexpected data exposure.	• CASB • NG-SWG • Cloud Confidence Index (CCI)
Principle 5 - Notification of the collection of personal information	Netskope enforces organisational policies and aids in communication and acknowledgment of these policies through pop-up banners to data subjects and provides guidance, notices, and coaching pages.	• All products
Principle 6 - Use or disclosure ofUpersonal information	Netskope's platform offers comprehensive security measures to manage the use and disclosure of personal information across various cloud services. Through its Cloud Confidence Index (CCI), Netskope evaluates SaaS applications, considering factors such as security policies, legal, and privacy concerns. This helps organizations assess risks associated with third-party applications. Netskope's Data Loss Prevention (DLP) engine enhances security by using machine learning to identify and classify sensitive data, applying context-aware policies for real-time protection. This can include obfuscating personal data, encrypting sensitive files, or blocking certain actions, ensuring personal information is managed according to regulatory and organizational standards. Additionally, DLP enforces role-based access to protect data during incident response and supports continuous monitoring and forensic investigations. Netskope's Cloud and SaaS Security Posture Management tools prevent misconfigurations in mission-critical platforms and applications, alerting users to any deviations from access management policies or regulatory standards. These alerts provide detailed remediation instructions to ensure the proper use and protection of personal data, with automated remediation efforts facilitated through integration with Netskope's Cloud Ticket Orchestrator. This continuous monitoring and automated response capability enhance the security and compliance of personal information handled by organizations.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • DLP • SSPM • CTO

Requirement	Netskope Response	Products
Principle 7 - Direct marketing	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover and manage personal information used for marketing across various environments such as web, cloud applications, and endpoint devices. It can assist in ensuring personal information is not misused or disclosed for direct marketing purposes without proper consent or adherence to legal exceptions.	• CASB • NG-SWG • Public Cloud Security • DLP
Principle 8 - Cross-border disclosure of personal information	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal information across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning to identify personal information in accordance with organisational and regulatory standards, including predefined definitions, ensuring that individuals' data is handled in compliance with relevant privacy regulations. Advanced Analytics assists entities in understanding and visualising data flows, including cross-border transfers, allowing them to determine if those transfers are approved and have appropriate safeguards in place. This ensures that personal information is protected and handled in a manner consistent with privacy principles, particularly in the context of international data transfers. Additionally, DLP rules can be applied based on application and transfers to block or restrict transfers and assist in performing transfer impact assessments by using CCI scoring.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics • CCI
Principle 9 - Adoption, use, or disclosure of government-related identifiers	Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) leverage a data loss prevention (DLP) engine to secure organizational data across various environments. This advanced DLP employs machine learning to identify and protect sensitive data, meeting both organizational and regulatory needs. Context-aware policies incorporate user and device information to safeguard data in real time by obfuscating personal data, encrypting sensitive files, and blocking unauthorized actions. For handling government-related identifiers, Netskope's DLP enforces strict role-based access, ensuring that sensitive data is only accessible to authorized personnel. It can facilitate secure incident response and recovery, maintain integrity of backups, and store log files for continuous monitoring and forensic investigations, thereby preventing unauthorized disclosure of government identifiers.	• CASB • NG-SWG • DLP
Principle 10 - Quality of personal information	Netskope's security solutions offer robust monitoring and protection for personal information across various platforms. Its Cloud Access Security Broker (CASB) monitors and logs detailed activities in SaaS and IaaS environments, such as user actions, device details, and data interactions, while applying real-time controls to prevent data loss. This not only blocks unauthorized actions but can also enforce business justification and provide policy training to users, enhancing the quality and protection of personal information. Netskope's Cloud Security Posture Management safeguards critical IaaS platforms by preventing misconfigurations and ensuring compliance with access management policies, which helps maintain the security and integrity of stored personal data. It routinely scans cloud storage to prevent data exfiltration and automates alerts and remediation efforts through integration with their Cloud Ticket Orchestrator. Their Next Gen Secure Web Gateway (NG-SWG) offers advanced protection by working with web and cloud apps to enforce SSO and MFA, utilizing context-aware controls that can detect and respond to risky behaviors. It provides detailed logging and alerts that can enhance incident response and assist in demonstrating non-repudiation of user actions. Netskope's tools collectively ensure that personal data is securely managed and access is carefully controlled, aligning with organizational and regulatory standards for data protection.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • CTO

Requirement	Netskope Response	Products
Principle 11 - Security of personal information	Netskope enhances the security of personal information through comprehensive cloud security solutions. Its Cloud Confidence Index (CCI) evaluates SaaS applications by assessing security policies, certifications, audit capabilities, and privacy concerns, helping organizations manage the risk associated with using specific cloud services. Netskope's Cloud Security Posture Management ensures mission-critical IaaS platforms are free from misconfigurations that could jeopardize data security, consistently monitoring and aligning with organizational policies and regulatory standards. It also scans cloud storage to prevent unauthorized data exfiltration. Integration with Netskope's Cloud Ticket Orchestrator automates alerts and remediation processes, minimizing the risk of personal data breaches. Similarly, Netskope's SaaS Security Posture Management safeguards SaaS functions by automatically identifying and correcting misconfigurations. It provides clear remediation instructions and can convert past issues into preventative rules, continuously improving security. Netskope's Advanced Analytics maps and evaluates data flows across web and cloud services, categorizing data by sensitivity and usage patterns. This feature allows organizations to track security trends—such as app access, threat detection, and policy enforcement—via a user-friendly dashboard. Through these measures, Netskope effectively protects personal information within cloud environments.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • Advanced Analytics • CTO
Principle 12 - Access to personal information	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal information across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal information to assist entities with executing individuals' requests.	• CASB • NG-SWG • Public Cloud Security • DLP
Principle 13 - Correction of personal information	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal information across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal information to assist entities with executing individuals' requests for correction of personal information.	• CASB • NG-SWG • Public Cloud Security • DLP

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.