netskope

Compliance Series

Using the Netskope Platform to Support Compliance with the SDAIA PDPL - Saudi Arabia

TABLE OF CONTENTS

INTRODUCTION 3

NETSKOPE PRODUCTS OVERVIEW 5

HOW TO USE THIS GUIDE 6

NETSKOPE PRODUCTS 6

PERSONAL DATA PROTECTION LAW 8

INTRODUCTION

On September 7, 2023, the Saudi Authority for Data and Artificial Intelligence (SDAIA) issued the Implementing Regulations of the Personal Data Protection Law (the Implementing Regulations) and the Regulations on Personal Data Transfer outside the Geographical Boundaries of the Kingdom (the Data Transfer Regulations, together, the Regulations). These Regulations mark an important development in the Kingdom of Saudi Arabia's (KSA) data protection landscape as they set out to clarify and detail supplementing the KSA Personal Data Protection Law (PDPL), the KSA's first comprehensive national data protection legislation which is broadly modelled on the GDPR.

The PDPL and the Regulations entered into force on September 14, 2023, although data controllers have a one-year grace period to comply with the PDPL (i.e., September 14, 2024). The legal framework applies across all industry sectors and prescribes strict obligations on almost anyone dealing with personal data, such as reporting data breaches within 72 hours, appointing a Data Protection Officer in certain circumstances, carrying out legitimate interest assessments and data protection impact assessments, and maintaining a record of processing activities. The international data transfer restrictions are to a degree stricter than the General Data Protection Regulations (GDPR), as the grounds on which transfers may be carried out are more limited, absent adequacy decisions or appropriate safeguards. As the PDPL and the Regulations have now entered into force, businesses should promptly implement compliance measures.

Scope and Applicability:

PDPL applies to any processing of personal data carried out within the Kingdom, regardless of the means used, and applies to entities located outside Saudi Arabia if they process the personal data of individuals residing in the Kingdom. Uniquely, the PDPL extends to the personal data of deceased persons if such data can identify the deceased or their family members. The law covers both general and sensitive data, including health and genetic information, with specific protections in place. However, it does not apply to corporate, government, or technical data that does not identify individuals. Additionally, personal data processed for personal, or family use is excluded from the law's scope, provided the data has not been published or disclosed to others, with further details on this defined in accompanying regulations.

Personal Data

Any information that can identify an individual, directly or indirectly. This includes names, IDs, contact details, addresses, licence numbers, bank/credit card info, photos, videos, and personal records.

Sensitive Information

Personal data that reveals a person's racial/ethnic origin, beliefs (religious, political, etc.), criminal history, biometric/genetic info, health data, or if their parents are unknown.

Health Information

Personal information about a person's physical, mental, or psychological health, or any health services they have received.

Genetic Data

Any Personal Data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the physiological or health characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating Genetic Data.

Credit Data

Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.

Lawful Basis for Processing Data:

Under Article 6 of the PDPL, personal data can be processed without consent in specific circumstances, such as when it's necessary to protect the interests of the data subject, to comply with a legal obligation, under a prior agreement, for legitimate interests of the controller (if not prejudicing the data subject's rights), or if the controller is a public entity processing data for security or judicial purposes.
Article 10 allows data collection from other sources or for new purposes with consent, when the data is public, or in cases involving public interest, health, or safety. Consent is generally required for processing unless an exception applies. Data disclosure follows strict rules and cannot occur without consent unless it's for public interest, health, or safety, or to comply with legal or judicial requirements, while anonymized data or public data can be used more freely.

Data Subject Rights:

Individuals are entitled to several rights: the right to be informed of the legal basis and purpose of collecting their personal data; the right to access their data held by the Controller; the right to request their data in a readable format; the right to request correction, completion, or updating of their data; and the right to request the destruction of their data when it is no longer needed, in accordance with the Law's provisions.

International Data Transfers:

PDPL allows controllers to transfer or disclose personal data outside Saudi Arabia, provided it aligns with the PDPL, its amendments, and relevant regulations. Transfers are permitted for purposes like fulfilling obligations under agreements, serving the interests of Saudi Arabia, or providing benefits to the data subject. Such transfers must not compromise national security, and the level of protection must meet Saudi standards.

Data Breach Notifications:

Under the Law, controllers must notify the Saudi Authority for Data and Artificial Intelligence (SDAIA) within 72 hours of becoming aware of any personal data breach, including leaks, damage, unauthorised access or if it poses a risk to personal data or conflicts with the data subject's rights. The notification must include details of the breach, its impact, measures taken, and contact information. If the controller cannot provide all information immediately, they must submit it as soon as possible with an explanation for the delay. Additionally, controllers must promptly inform affected data subjects in clear language, detailing the breach, potential risks, mitigation steps if the breach may cause damage to their data or conflict with their rights or interests.

Penalties:

PDPL stipulates that disclosing or publishing sensitive data in violation of its provisions, whether to harm the data subject or for personal gain, can result in imprisonment for up to 2 years and/or a fine of up to 3 million Riyals (approx. $800,000). The public prosecution investigates such violations, and the competent court can double fines for repeat offences. Article 36 outlines penalties for non-sensitive data breaches, including fines up to 5 million Riyals (approx. $1.33 million) or warnings, determined by a committee that evaluates the nature and impact of violations. Article 38 allows the court to confiscate funds from violations and order publication of judgments at the violator's expense. Article 39 mandates public authorities to discipline staff violating the PDPL, following legal accountability procedures.

Netskope Products Overview

Netskope's products can be used as a technical control to assist organisations in supporting compliance efforts with the PDPL 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 data, which is crucial for PDPL compliance. Encryption and Tokenization: It ensures that personal data 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 data as required by PDPL. 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 PDPL 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 PDPL 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 PDPL. 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 PDPL's 72-hour breach notification requirement.

Data Residency and Sovereignty:

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

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

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 PDPL. The tools can also be used to secure personal data, monitor compliance and alert stakeholders where potential breaches or out of compliance processing is detected.

The tables below break down each chapter and provide the reader with guidance on where Netskope's products can assist data controllers and processors in complying with the directive.

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

Industry terminology	Netskope Product Line/Abbreviation
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

PERSONAL DATA PROTECTION LAW

Requirements(s)	Netskope Response	Products
Article 1 Definitions	This article sets out the key definitions and terms, Netskope's products do not directly map to this requirement	
Article 2 Territorial Scope	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with pre-defined personal data profiles. These products can assist data controllers in determining where personal data is being processed and applying context-aware policies to manage personal data in real time. In addition, Advanced Analytics can show mapping of where the personal data is flowing and assist controllers in applying policies to understand the territorial scope of processing.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 3 Data Subject Protections	This article sets out the new data subject protections, Netskope's products do not directly map to this requirement	
Article 4 Data Subject Rights	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers with executing data subject access requests (DSAR) defined in Article (4) DLP can also assist in verifying the right to erasure has been performed by using discovery across web, cloud applications, and endpoint devices as defined in Paragraph (5) of Article (4)	• CASB • NG-SWG • Public Cloud Security • DLP
Article 5 Consent	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time. Netskope scores SaaS applications that may include automated decision making in its Cloud Confidence Index (CCI) and provides many important details that help organisations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. The above discovery can assist data controllers in ensuring the relevant consent is obtained for personal data processing in compliance with Article (5).	• CASB • NG-SWG • DLP • CCI

Requirements(s)	Netskope Response	Products
Article 6 Consent Exceptions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time. Netskope scores SaaS applications that may include automated decision making in its Cloud Confidence Index (CCI) and provides many important details that help organisations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. The above discovery can assist data controllers in ensuring where exceptions to consent are applicable for personal data processing records are maintained of where the processing occurs.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 7 Conditions for Consent	This article sets conditions for consent under PDPL. Netskope's products do not directly map to this requirement.	
Article 8 Processors	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices where personal data may be processed by third parties (processors). The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time within processors. Cloud Confidence Index (CCI) scores cloud apps and services (potential processors) based on security, certifications, audit capabilities, legal and privacy concerns. Utilising CCI scoring a data controller can apply policies to limit and restrict transfers to potential risky processors. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations of processors, CSPM scans cloud storage processors to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring proper use of assets and data. SSPM provides remediation instructions, integrates with Cloud Ticket Orchestrator for service tickets and automated remediation, and converts detected misconfigurations into new security rules. Both CSPM and SSPM aim to ensure data protection by default is applied across the organisation. Advanced Analytics can assist controllers in visualising potential personal data flows to/from processors and apply policies based on CCI scoring and vendor's secure posture.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO • CCI • Advanced Analytics

Requirements(s)	Netskope Response	Products
Article 9 Rights to Access Timeframes	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers with executing data subject access requests (DSAR) defined in Paragraph (2) of Article (4) in line with the timeframe with Article (9).	• CASB • NG-SWG • Public Cloud Security • DLP
Article 10 Processing Restrictions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers ensuring processing restrictions are applied in accordance with Article (10).	• CASB • NG-SWG • Public Cloud Security • DLP
Article 11 Collection and Processing Restrictions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers ensuring processing restrictions are applied in accordance with Article (11) and verification of deletion of personal data in accordance with Paragraph (5) of Article (11).	• CASB • NG-SWG • Public Cloud Security • DLP
Article 12 Notices and Privacy Policy	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. These notifications alert employees of potential policy infringements in accordance with organisational requirements.	• All Products
Article 13 Collection Notification	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. These notifications alert employees of potential policy infringements in accordance with organisational requirements.	• All Products
Article 14 Accuracy, Completeness, Timeliness and Relevance	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers in ensuring personal data is being processed in the expected locations (sanctioned).	• CASB • NG-SWG • DLP
Article 15 Disclosures	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre-defined personal data definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if those transfers are not approved under PDPL. 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

Requirements(s)	Netskope Response	Products
Article 16 Limitation of Disclosures	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre-defined personal data definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if those transfers are not approved under PDPL. 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
Article 17 Correction of Personal Data	This article sets conditions for correction of personal data under PDPL. Netskope's products do not directly map to this requirement.	
Article 18 Retention	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers ensuring retention processes are robust i.e. personal data has been purged in accordance with Article (18).	• CASB • NG-SWG • Public Cloud Security • DLP
Article 19 Technical and Organisational Measures	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time. These context aware policies include applying automatic encryption of personal data. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure personal data security measures are implemented and maintained. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of personal data. SSPM provides remediation instructions, integrates with Cloud Ticket Orchestrator for service tickets and automated remediation, and converts detected misconfigurations into new security rules. ZTNA Next provides secure remote access based on zero trust principles, supports encrypted data transfer, and enforces login policies to protect access to personal data. Netskope's Borderless SD-WAN extends network perimeters to any user or device, using Netskope's global New Edge network for high-availability connectivity and adaptive trust enforcement based on specific criteria assisting in protecting personal data.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO • ZTNA-Next • SD-WAN

Requirements(s)	Netskope Response	Products
Article 20 Breach Notification	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time. These context aware policies include applying automatic encryption of personal data. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure personal data security measures are implemented and maintained. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of personal data. SSPM provides remediation instructions, integrates with Cloud Ticket Orchestrator for service tickets and automated remediation, and converts detected misconfigurations into new security rules. DLP can additionally detect records associated with a data incident and provide forensic reporting to assist the data controller in mitigating the impact of data breaches. All these products assist the data controller in understanding the scope of the breach and the potential need to notify the supervisory authority.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Article 21 Timelines for Data Subject Access Requests	This article sets out timelines for data subject access requests. Netskope's products do not directly map to this requirement.	
Article 22 Personal Data Impact Assessment	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time. These context aware policies include applying automatic encryption of personal data. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure personal data security measures are implemented and maintained. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of personal data. All these products assist the data controller in completing a Data Protection Impact Assessment in understanding where personal data is processed and what security measures are in place.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO

Requirements(s)	Netskope Response	Products
Article 23 Health Data Processing	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure health data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting health data according to organisational and regulatory standards with predefined health data definitions applying context-aware policies to manage processing of health data in real time. These context aware policies include applying automatic encryption of health data, Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure health data security measures are implemented and maintained. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of health data.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Article 24 Credit Data Processing	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover credit data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting credit data according to organisational and regulatory standards with predefined credit/financial data definitions applying context-aware policies to manage processing of credit data in real time. These context aware policies include applying automatic encryption of credit data, Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure credit data security measures are implemented and maintained. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of credit data.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Article 25 Advertising Restrictions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and block personal data used for advertising across various environments such as web, cloud applications, and endpoint devices.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 26 Marketing Restrictions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and block personal data used for marketing across various environments such as web, cloud applications, and endpoint devices.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 27 Scientific, Research or Statistical Restrictions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover if personal data related to scientific, research or statistical purposes has been appropriately anonymized across various environments such as web, cloud applications, and endpoint devices.	• CASB • NG-SWG • Public Cloud Security • DLP

Requirements(s)	Netskope Response	Products
Article 28 Copying Restrictions	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data and potential copies across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre-defined personal data definitions.	• CASB • NG-SWG • DLP
Article 29 International Transfers	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre-defined personal data definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if those transfers are not approved under PDPL. 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
Article 30 Oversight & Data Protection Officers	This article sets out oversight and relevant appointments of Data Protection Officers under PDPL. Netskope's products do not directly map to this requirement.	
Article 31 Record of Processing	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data with predefined personal data definitions. Netskope provides an export capability using Cloud Exchange to assist the data controller in maintaining an accurate and up to date record of processing.	• CASB • NG-SWG • Public Cloud Security • DLP • Cloud Exchange
Article 32 repealed	This article has been repealed.	
Article 33 Accreditations, Certifications and Licensing	This article sets out accreditations, certifications and licences under PDPL. Netskope's products do not directly map to this requirement.	
Article 34 Complaints	This article sets out data subject complaints under PDPL. Netskope's products do not directly map to this requirement.	
Article 35 Penalties	This article sets out penalties under PDPL. Netskope's products do not directly map to this requirement.	
Article 36 Penalties Governance	This article sets out penalties' governance under PDPL. Netskope's products do not directly map to this requirement.	
Article 37 Right to Audit	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre-defined personal data definitions. These tools can assist a data controller in determining where personal data is processed in any legal discovery or audit.	• CASB • NG-SWG • Public Cloud Security • DLP

Requirements(s)	Netskope Response	Products
Article 38 Confiscation of Funds	This article sets out legal confiscation of funds under PDPL. Netskope's products do not directly map to this requirement.	
Article 39 Public Entity Disciplinary Provisions	This article sets out public entity disciplinary provisions under PDPL. Netskope's products do not directly map to this requirement.	
Article 40 Compensation	This article sets out compensation provisions under PDPL. Netskope's products do not directly map to this requirement.	
Article 41 Processing Confidentiality	Netskope's security solutions, including CASB and NG-SWG, utilise a Data Loss Prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with predefined personal data definitions applying context-aware policies to manage processing of personal data in real time. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure data protection by design is applied, CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of personal data. SSPM provides remediation instructions, integrates with Cloud Ticket Orchestrator for service tickets and automated remediation, and converts detected misconfigurations into new security rules to protect personal data. ZTNA Next provides secure remote access based on zero trust principles, supports encrypted data transfer, and enforces login policies to protect access to personal data. Netskope's Borderless SD-WAN extends network perimeters to any user or device, using Netskope's global New Edge network for high-availability connectivity and adaptive trust enforcement based on specific criteria assisting in protecting personal data.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO • ZTNA-Next • SD-WAN
Article 42 Timeline for Issuance of Regulations	This article sets out timeliness for issuance of PDPL. Netskope's products do not directly map to this requirement.	
Article 43 Timeline for Enforcement of Law	This article sets out a timeline for enforcement of PDPL. Netskope's products do not directly map to this requirement.	

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.