netskope

Compliance Series

Using the Netskope Platform to Support

Compliance with the EU GDPR

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that was implemented across the European Union (EU) and the European Economic Area (EEA) on May 25, 2018. It aims to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Scope and Applicability:

GDPR applies to organisations operating within the EU, as well as to organisations outside the EU that offer goods or services to individuals in the EU or monitor the behaviour of individuals within the EU.

Personal Data:

The regulation protects "personal data," which is any information relating to an identified or identifiable natural person (data subject). This includes names, identification numbers, location data, online identifiers, and factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Lawful Basis for Processing Data:

GDPR sets out six lawful bases for processing personal data: consent, contract, legal obligation, vital interests, public task, and legitimate interests.

Data Subject Rights:

Individuals have several rights under GDPR, including the right to access their data, the right to rectify inaccurate data, the right to delete their data (right to be forgotten), the right to data portability, the right to restrict processing, and the right to object to processing.

Consent:

Consent must be freely given, specific, informed, and unambiguous. Data subjects can withdraw their consent at any time.

Data Protection by Design and Default:

GDPR requires organisations to implement data protection measures from the outset of any project (data protection by design) and to ensure that, by default, only the necessary data for each specific purpose is processed (data protection by default).

Data Breach Notifications:

Organisations are required to report certain types of data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, and in some cases, to the data subjects affected.

Penalties:

Organisations that fail to comply with GDPR can face significant fines. The maximum fine for non-compliance can be up to €20 million or 4% of the organisation's annual global turnover, whichever is higher.

Data Protection Officers (DPOs):

Some organisations are required to appoint a Data Protection Officer (DPO) who is responsible for overseeing data protection strategy and compliance with GDPR requirements. This is mandatory for public authorities and organisations that engage in large-scale systematic monitoring or processing of sensitive personal data.

International Data Transfers:

Transfers of personal data outside the EU/EEA are restricted unless the receiving country ensures an adequate level of data protection, as determined by the EU Commission, or the organisation has implemented appropriate safeguards such as binding corporate rules or standard contractual clauses.

GDPR represents a significant step in data privacy regulation, stressing transparency, security, and accountability in the handling of personal data. It provides stronger protections for data subjects and stricter requirements for data controllers and processors.

NETSKOPE PRODUCTS OVERVIEW

Netskope's products can be used as a technical control to assist organisations in supporting compliance efforts with GDPR 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 GDPR 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 GDPR.

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 GDPR 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 GDPR 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 GDPR.

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 GDPR'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 GDPR’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 GDPR.

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 GDPR. 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.

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 AccessI
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)

CHAPTER 1 - GENERAL PROVISIONS

Requirements(s)	Netskope Response	Products
Article 1 - Subject-matter and objectives	This article sets out core objectives of GDPR. Netskope's products do not directly map to this requirement	
Article 2 - Material 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 personal data according to organisational and regulatory standards with predefined GDPR profiles assisting data controllers with scoping	• CASB • NG-SWG • Public Cloud Security • DLP
Article 3 - 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 personal data according to organisational and regulatory standards with predefined GDPR profiles assisting data controllers with scoping.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 4 - Definitions	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 sensitive data according to organisational and regulatory standards with predefined GDPR definitions assisting data controllers with scoping and applying context-aware policies to manage personal data in real time.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 5 - Principles relating to processing of personal data	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 GDPR definitions applying context-aware policies to manage processing of personal data in real time. Specifically Art 5.1 (f) i.e. processed in a manner that ensures appropriate security of the personal data. DLP can additionally through policies automatically discover and encrypt personal data. Netskope scores SaaS applications 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..	• CASB • NG-SWG • Public Cloud Security • DLP • ZTNA Next • SD-WAN • CSPM • SSPM • CTO • CCI • UEBA

Requirements(s)	Netskope Response	Products
Article 5 - Principles relating to processing of personal data	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 GDPR definitions applying context-aware policies to manage processing of personal data in real time. Specifically Art 5.1 (f) i.e. processed in a manner that ensures appropriate security of the personal data. DLP can additionally through policies automatically discover and encrypt personal data. Netskope scores SaaS applications 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. 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 NewEdge Network for high-availability connectivity and adaptive trust enforcement based on specific criteria assisting in protecting personal data. Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organisation's critical IaaS platforms to prevent misconfigurations and ensure compliance with access management policies, regulatory, and industry standards such as protection of personal data. It routinely scans cloud storage buckets to prevent personal data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Netskope's SaaS Security Posture Management (SSPM) similarly monitors SaaS functions to prevent misconfigurations and ensure proper use of assets and personal data. SSPM provides detailed remediation instructions and can also integrate with the Cloud Ticket Orchestrator to create service tickets from alerts and automate fixes. Additionally, SSPM allows previously detected misconfigurations to be converted into new security rules to provide adaptive protection for personal data. Netskope's User Entity and Behavior Analytics (UEBA) monitors user activity across web and cloud services, setting baselines for normal behaviour to detect anomalies such as personal data transfers, and enacting adaptive policy controls based on the riskiness of each user's actions.	

Requirements(s)	Netskope Response	Products
Article 6 - Lawfulness of processing	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 in line with lawfulness of processing with predefined GDPR definitions applying context-aware policies to manage processing of personal data in real time. In particular, DLP can automatically encrypt personal data based on predefined policies. Netskope scores SaaS applications 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. 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 NewEdge Network for high-availability connectivity and adaptive trust enforcement based on specific criteria assisting in protecting personal data. Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organisation's critical IaaS platforms to prevent misconfigurations and ensure compliance with access management policies, regulatory, and industry standards such as protection of personal data. It routinely scans cloud storage buckets to prevent personal data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Netskope's SaaS Security Posture Management (SSPM) similarly monitors SaaS functions to prevent misconfigurations and ensure proper use of assets and personal data. SSPM provides detailed remediation instructions and can also integrate with the Cloud Ticket Orchestrator to create service tickets from alerts and automate fixes. Additionally, SSPM allows previously detected misconfigurations to be converted into new security rules to provide adaptive protection for personal data. Netskope's User Entity and Behavior Analytics (UEBA) monitors user activity across web and cloud services, setting baselines for normal behaviour to detect anomalies such as personal data transfers, and enacting adaptive policy controls based on the riskiness of each user's actions.	• CASB • NG-SWG • Public Cloud Security • DLP • ZTNA Next • SD-WAN • CSPM • SSPM • CTO • CCI • UEBA
Article 7 - Conditions for consent	This article sets conditions for consent under GDPR. Netskope's products do not directly map to this requirement	
Article 8 - Conditions applicable to child's consent in relation to information society services	This article sets out GDPR processing restrictions related to obtaining a child's consent. Netskope's products do not directly map to this requirement.	
Article 9 - Processing of special categories of personal data	Netskope's security solutions, including CASB and NG-SWG, utilise a Data loss prevention (DLP) engine to discover and secure special categories of personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting sensitive data according to organisational and regulatory standards with predefined GDPR definitions applying context-aware policies to manage processing of personal data in real time.	• CASB • NG-SWG • Public Cloud Security • DLP

Requirements(s)	Netskope Response	Products
Article 10 - Processing of personal data relating to criminal convictions and offences	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover and secure special categories of personal data such as criminal convictions and offences across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting sensitive data according to organisational and regulatory standards with predefined GDPR definitions applying context-aware policies to manage processing of personal data in real time.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 11 - Processing which does not require identification	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover and secure categories of personal data where identification is not required across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting sensitive data according to organisational and regulatory standards with predefined GDPR definitions applying context-aware policies to manage processing of personal data in real time.	• CASB • NG-SWG • Public Cloud Security • DLP

CHAPTER 3 - RIGHTS OF THE DATA SUBJECT

Requirements(s)	Netskope Response	Products
Article 12 - Transparent information, communication, and modalities for the exercise of the rights of the data subject	Netskope enforces organisational policies and aids in communication and acknowledgment of these policies through pop-up banners to data subjects and provides guidance and coaching pages. These notifications alert employees of potential policy infringements in accordance with organisational requirements.	• All products
Article 13 - Information to be provided where personal data are collected from the data subject	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 sensitive data according to organisational and regulatory standards with predefined GDPR definitions applying context-aware policies to manage processing of personal data in real time.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 14 - Information to be provided where personal data have not been obtained from the data subject	Netskope enforces organisational policies and aids in communication and acknowledgment of these policies through pop-up banners to data subjects and provides guidance and coaching pages. These notifications alert employees of potential policy infringements in accordance with organisational requirements.	• All products
Article 15 - Right of access by the data subject Article 16 - Right to rectification Article 17 - Right to erasure ('right to be forgotten') Article 18 - Right to restriction of processing Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 20 - Right to data portability Article 21 - Right to object	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 Art 15-21. DLP can also assist in verifying Art 17 right to erasure has been performed by using discovery across web, cloud applications, and endpoint devices.	• CCASB • NG-SWG • Public Cloud Security • DLP

Requirements(s)	Netskope Response	Products
Article 22 - Automated individual decision-making, including profiling	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 GDPR definitions applying context-aware policies to manage processing of personal data in real time. Netskope's NG-SWG can also detect usage of applications that may include automated decision-making, in particular, use of artificial intelligence. 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.	• CASB • NG-SWG • Public Cloud Security • DLP • CCI
Article 23 - 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 and protecting personal data according to organisational and regulatory standards with predefined GDPR definitions applying context-aware policies to manage processing of personal data in real time. This discovery can assist data controllers in defining where specific restrictions may apply to personal data processing as defined in Art 23.	• CASB • NG-SWG • Public Cloud Security • DLP

CHAPTER 4 - CONTROLLER AND PROCESSOR

Requirements(s)	Netskope Response	Products
Article 24 - Responsibility of the controller	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 GDPR 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 compliance with defined technical and organisational measures (TOMs). CSPM scans cloud storage to prevent personal 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.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO

Requirements(s)	Netskope Response	Products
Article 25 - Data protection by design and by default	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 GDPR 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 NewEdge 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 26 - Joint controllers	This article sets out joint controllers' obligations under GDPR. Netskope's products do not directly map to this requirement	
Article 27 - Representatives of controllers or processors not established in the Union	This article sets out representatives of controllers or controllers not established under GDPR. Netskope's products do not directly map to this requirement	
Article 28 - Processor	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. In particular 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 GDPR 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.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO • CCI • Advanced Analytics

Requirements(s)	Netskope Response	Products
	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 organization Advanced Analytics can assist controllers in visualising potential personal data flows to/from processors and apply policies based on CCI scoring and vendors' secure posture.	
Article 29 - Processing under the authority of the controller or processor	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. In particular, 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 GDPR 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.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO • CCI • Advanced Analytics
Article 30 - Records of processing activities	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 GDPR definitions. Netskope provides an export capability through the use of 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 31 - Cooperation with the supervisory authority	This article sets out controllers' obligation to cooperate with the supervisory authority under GDPR. Netskope’s products do not directly map to this requirement	

Requirements(s)	Netskope Response	Products
Article 32 - Security of processing	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 GDPR 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 NewEdge 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 33 - Notification of a personal data breach to the supervisory authority	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 GDPR 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

Requirements(s)	Netskope Response	Products
Article 34 - Communication of a personal data breach to the data subject	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 predefined GDPR definitions. DLP can assist the controller in determining the scope of the breach, which data subjects are impacted and who should be communicated to in accordance with Art 34.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 35 - Data protection 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 GDPR 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
Article 36 - Prior consultation	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 GDPR 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 determining if prior consultation with the supervisory authority is required when processing would result in high risks due to absence of measures.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Article 37 - Designation of the data protection officer	This article sets out controllers' obligation to appoint a data protection officer under GDPR. Netskope's products do not directly map to this requirement.	

Requirements(s)	Netskope Response	Products
Article 38 - Position of the data protection officer	This article sets out the data protection officer’s obligations under GDPR. Netskope’s products do not directly map to this requirement.	
Article 39 - Tasks of the data protection officer	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 GDPR 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. Similarly, 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 protection officer in their defined tasks under GDPR in protecting personal data.	• CCASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Article 40 - Codes of conduct	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 predefined GDPR definitions. This discovery mechanism can assist the data controller in determining a code of conduct with respect to personal data processing. Additionally, DLP policies can be established to force encryption or quarantining personal data when discovered outside sanctioned applications or hosting providers. Advanced Analytics can assist data controllers in understanding data flows including cross-border transfers and potential updates to codes of conduct.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 41 - Monitoring of approved codes of conduct	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 securing personal data according to organisational and regulatory standards with predefined GDPR definitions. This discovery mechanism can assist the data controller in monitoring codes of conduct with respect to personal data processing. Additionally, DLP policies can be established to force encryption or quarantining personal data when discovered outside sanctioned applications or hosting providers. Advanced Analytics can assist data controllers in understanding data flows including cross-border transfers and potential updates to codes of conduct.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics

Requirements(s)	Netskope Response	Products
Article 42 - Certification	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 GDPR 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 providing evidence of compliance with GDPR in order to seek a certification.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Article 43 - Certification bodies	This article sets out supervisory authorities' obligations to establish certification bodies under GDPR. Netskope's products do not directly map to this requirement.	

CHAPTER 5 - TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Requirements(s)	Netskope Response	Products
Article 44 - General principle for 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 predefined GDPR definitions.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analyticss
Article 45 - Transfers on the basis of an adequacy decision	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 predefined GDPR definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if those transfers are permitted under the basis of adequacy decisions by the EDPB (European Data Protection Board).	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics

Requirements(s)	Netskope Response	Products
Article 46 - Transfers subject to appropriate safeguards	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 predefined GDPR definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if those transfers are approved and have appropriate safeguards.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 47 - Binding corporate rules	This article sets out supervisory authorities' approval of binding corporate rules under GDPR. Netskope's products do not directly map to this requirement.	
Article 48 - Transfers or disclosures not authorised by Union law	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 predefined GDPR 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 GDPR. 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 49 - Derogations for specific situations	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 predefined GDPR definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if those transfers may use derogations.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 50 - International cooperation for the protection of personal data	This article sets out the commissions and supervisory authorities' cooperation for protection of personal data under GDPR. Netskope's products do not directly map to this requirement.	• All products

CHAPTER 6 - INDEPENDENT SUPERVISORY AUTHORITIES

Chapter 6 deals with supervisory authorities and has no mapping to Netskope products.

CHAPTER 7 - COOPERATION AND TRANSPARENCY

Chapter 7 deals with cooperation and transparency related to supervisory authorities and has no mapping to Netskope products.

CHAPTER 8 - REMEDIES, LIABILITY, AND PENALTIES

Chapter 8 deals with remedies, liability, and penalties and has no mapping to Netskope products.

CHAPTER 9 - PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Requirements(s)	Netskope Response	Products
Article 85 - Processing and freedom of expression and information	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover specific personal data such as those defined in Art 85 (personal data types that cover journalistic purposes and the purposes of academic, artistic, or literary expression) across various environments such as web, cloud applications, and endpoint devices. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers to determine if these are exempt of restrictions for example cross-border transfers.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics
Article 86 - Processing and public access to official documents	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover specific personal data such as those defined in Art 86 across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying specific personal data according to organisational and regulatory standards with predefined GDPR definitions. Additionally, DLP can assist in tracking any such release of this category of personal data to ensure compliance with Art 86.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 87 - Processing of the national identification number	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover specific personal data such as those defined in Art 87 across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying specific personal data according to organisational and regulatory standards with predefined GDPR definitions.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 88 - Processing in the context of employment	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover and secure specific personal data such as those defined in Art 88 specifically processing personal data in context of employment across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and securing specific personal data according to organisational and regulatory standards with predefined GDPR definitions.	• CASB • NG-SWG • Public Cloud Security • DLP

Requirements(s)	Netskope Response	Products
Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover and secure specific personal data such as those defined in Art 89 across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and securing specific personal data according to organisational and regulatory standards with predefined GDPR definitions.	• CASB • NG-SWG • Public Cloud Security • DLP
Article 90 - Obligations of secrecy	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 GDPR definitions applying context-aware policies to manage processing of personal data in real time. DLP policies can also automatically discover and encrypt personal data. Netskope scores SaaS applications 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. 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 NewEdge Network for high-availability connectivity and adaptive trust enforcement based on specific criteria assisting in protecting personal data. Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organisation's critical IaaS platforms to prevent misconfigurations and ensure compliance with access management policies, regulatory, and industry standards such as protection of personal data. It routinely scans cloud storage buckets to prevent personal data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Netskope's SaaS Security Posture Management (SSPM) similarly monitors SaaS functions to prevent misconfigurations and ensure proper use of assets and personal data. SSPM provides detailed remediation instructions and can also integrate with the Cloud Ticket Orchestrator to create service tickets from alerts and automate fixes. Additionally, SSPM allows previously detected misconfigurations to be converted into new security rules to provide adaptive protection for personal data. Netskope's User Entity and Behavior Analytics (UEBA) monitors user activity across web and cloud services, setting baselines for normal behaviour to detect anomalies such as personal data transfers, and enacting adaptive policy controls based on the riskiness of each user's actions.	• CASB • NG-SWG • Public Cloud Security • DLP • ZTNA Next • SD-WAN • CSPM • SSPM • CTO • CCI • UEBA
Article 91 - Existing data protection rules of churches and religious associations	This article sets out existing data protection rules of churches and religious associations under GDPR. Netskope's products do not directly map to this requirement.	

CHAPTER 10 - DELEGATING ACTS AND IMPLEMENTING ACTS

Chapter 10 deals with delegation and implementation acts and does not map to Netskope products.

CHAPTER 11 - FINAL PROVISIONS

Chapter 11 deals with final provisions of GDPR and does not map to Netskope products.

Disclaimer

The content provided has been created to the best of Netskope's ability and knowledge. However, Netskope cannot guarantee the accuracy, completeness, or timeliness of the information. Netskope are not liable for any errors or omissions in the content, and readers are encouraged to verify the information independently. The use of this content is at the reader's own risk, and Netskope shall not be held responsible for any consequences resulting from reliance on the provided information.

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.