Whitepaper

Netskope's Privacy-by-Design Approach

Commitment to Data Protection and Privacy

Netskope is dedicated to ensuring the privacy and security of personal data, emphasizing transparency and a commitment to privacy by design. As a data processor, Netskope follows strict protocols to protect the data of its customers, employees, and partners. This includes implementing robust physical, technical, and organizational measures to prevent unauthorized access, loss, or unlawful processing of data. The company also ensures that its security and privacy practices are independently audited annually. Netskope acts in compliance with various data protection regulations and works closely with customers to meet their privacy and data security needs.

Netskope processes personal data across various categories, ensuring that data owners (customers) remain in full control of their information. While Netskope acts as the processor, it applies privacy by design principles, which are ingrained in its architecture and operational processes enabling customers to control where data is processed and stored, and preventing transfers of sensitive data outside chosen regions. For more details, please refer to our Data Processing Agreement. Customers are given the flexibility to select where data is stored and processed, adhering to geographical and regulatory requirements. Furthermore, data processing occurs within designated management planes, ensuring that privacy policies are consistently applied. This prevents the transfer of data outside the EU or other restricted areas.

Key Privacy Controls:

Data Categories: In-memory processing with obfuscation controls for personal data such as names, email addresses, IP addresses.

Data Ownership: As a data processor, Netskope acts on customer instructions, with customers maintaining full control over their data.

Data Residency: Customers choose where their data is stored from a list of global locations, including the U.S., EU, and Australia.

Data Retention: Transaction logs are retained based on customer preferences and regulatory requirements.

International Data Transfers: Netskope complies with GDPR and other regulations, using mechanisms like Standard Contractual Clauses (SCCs).

Data Access & Accuracy: Individuals have the right to (and can) request access, correction, or deletion of their data under applicable laws.

INTERNATIONAL DATA TRANSFERS

Netskope ensures international data transfers comply with GDPR and other privacy laws, particularly through the use of SCCs. In addition, Netskope conducts Data Privacy Impact Assessments (DPIAs) and assists customers in performing their own assessments to ensure regulatory compliance. Netskope also provides tools for filtering transaction logs and guidance on how data can be stored within specific countries. Netskope reviews government data access requests and ensures these requests comply with legal standards. This ensures data transferred internationally remains protected.

CONCLUSION

Netskope takes a proactive approach to data privacy, providing its customers with the tools and measures needed to protect personal data across multiple geographies. By offering robust technical and organizational safeguards, adherence to industry standards, and flexibility in data management, Netskope ensures that privacy and security remain central to its operations. Personal data is processed securely and in compliance with global privacy regulations, empowering customers to manage their data with confidence. This commitment to privacy by design, data transparency, and compliance with global regulations positions Netskope as a trusted partner for secure data processing. We also offer a comprehensive privacy package covering all aspects of our privacy commitment, available upon request for further information.

Additional technical and organizational measures:

Encryption: Data is encrypted both in transit and at rest to safeguard it against unauthorized access.

Backups: Daily encrypted backups are performed with data retention for 30 days, in compliance with data residency policies.

Data Segregation: Management and data planes are separated, ensuring efficient and secure data handling.

Certifications: Netskope holds industry certifications such as ISO 27001, SOC 2 Type 2, and CSA STAR.

Access Controls: Rigorous access control measures are in place to ensure that only authorized personnel can access sensitive data.

Sub-processors: Third-party sub-processors are vetted thoroughly to ensure compliance with data protection standards with customers informed of any changes.

Interested in learning more?

Request a demo

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.