Netskope Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of, and is subject to the Netskope Subscription Services Agreement available at https://www.netskope.com/subscription-terms (the "**Agreement**") between Netskope, Inc. ("**Netskope**") and the entity executing this DPA below ("**Customer**"). If Netskope and Customer have executed another agreement governing the purchase and use of Netskope's cloud security services by Customer, then "Agreement" refers to the agreement executed by the parties. As used in this DPA, Customer includes Customer's Affiliates using Services pursuant to the Agreement. This DPA shall be effective on the last date of signature below ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

"**Account**" means Customer's account for the Services under which Customer accesses and administers the Services.

"**Affiliate**" means any present or future entity controlling, controlled by, or under common control with, a party to this DPA, or such other Affiliate entity as defined in the Agreement.

"**Authorized Affiliate**" shall mean a Customer Affiliate who is the Data Controller for the Personal Data processed by Netskope pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Compliant Transfer Mechanism**" means a compliant transfer mechanism that is recognized under EU Data Protection Law or other applicable Data Protection Laws for transfers between the parties in the relevant countries.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means the data protection and privacy laws applicable to a party and its Processing of Personal Data under the Agreement, including, where applicable, (i) EU Data Protection Law; (ii) the CCPA; and (iii) the UK Data Protection Laws; in each case, as may be amended, superseded or replaced.

"**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

"**EU Data Protection Law**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**").

"**Personal Data**" means any data relating to an identified or identifiable natural person (including personal information and similarly defined terms in Data Protection Laws) submitted by or on behalf of Customer or its Affiliates to the Services.

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, and dissemination. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) Netskope's provision of the Services in accordance with the Agreement, including Processing initiated or directed by Customer through the Services management interface, and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.

"**Security Incident**" means a breach of security in the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.

"**Services**" means the Netskope subscription services and support services procured by Customer under the Agreement.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Exhibit C**.**

"**Sub-processor**" means any third-party Data Processor or Netskope's Affiliate engaged by Netskope to Process Personal Data in connection with the Services.

"**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the United Kingdom ("**UK**"), including the UK GDPR and the Data Protection Act 2018.

"**UK GDPR**" has the meaning given to it in section 3 of the Data Protection Act 2018.

2. **Scope and Applicability of this DPA.** This DPA applies where and only to the extent that Netskope Processes Personal Data on behalf of Customer as Data Processor in the course of providing the Services.

3. **Roles and Scope of Processing.**

3.1 **Role of the Parties**. As between Netskope and Customer, Customer is the Data Controller of Personal Data, and Netskope shall Process Personal Data only as a Data Processor acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein. The parties agree to comply with applicable Data Protection Laws.

3.2 **Processing Details**. The details of the Processing of Personal Data are included in Exhibit A.

3.3 **Customer Instructions**. Netskope will Process Personal Data only for the Purposes. Customer shall ensure its Processing instructions are lawful and that the Processing of Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. In its administration of the Services, Customer remains responsible for selecting appropriate Services options and configurations for Customer's compliance requirements. Customer understands that Netskope will not assess the contents of communications transmitted by Customer or Personal Data to determine compliance with any specific legal requirements. The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Netskope for the Processing of Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between Customer and Netskope.

3.4 **Customer Affiliates**. Netskope's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:

(a) No entity other than Customer may provide further Processing instructions to Netskope and Customer must accordingly communicate any additional Processing instructions from its Authorized Affiliates directly to Netskope;

(b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer; and

(c) Authorized Affiliates shall not bring a claim directly against Netskope. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Netskope ("**Authorized Affiliate Claim**"): (i) Customer must bring such Authorized Affiliate Claim directly against Netskope on behalf of such Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

3.5 **Customer Processing of Personal Data**. Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Personal Data; and (ii) has obtained all consents, permissions and rights necessary under Data Protection Laws for Netskope to lawfully Process Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Personal Data with third-parties via the Services.

4. Sub-processing.

4.1 **Authorized Sub-processors**. Customer authorizes the engagement of those Sub-processors listed at https://www.netskope.com/netskope-sub-processors as of the Effective Date, and Netskope Affiliates.

4.2 **Sub-processor Obligations**. Netskope shall: (i) enter into a written agreement with each Sub-processor accessing Personal Data that impose obligations for the protection of Personal Data consistent with Netskope's obligations in this DPA to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain responsible and liable for each Sub-processor's compliance with the obligations in this DPA.

4.3 **Changes to Sub-processors.** Netskope will maintain an up-to-date list of Sub-processors, which will be available at https://www.netskope.com/netskope-sub-processors and upon request via email to privacy@netskope.com. Netskope will update the list at least thirty (30) days prior to adding or changing Sub-processors and provide notice to Customer's designated support contacts. During the notice period, Customer may object in writing to Netskope's appointment of the new Sub-processor(s), provided that such objection is based on reasonable grounds relating to data protection or regulatory compliance. In such event, the parties will discuss Customer's concerns in good faith. If the new Sub-processor is unable to Process Personal Data in compliance with the terms of this DPA and Netskope cannot provide an alternative, or the parties are not otherwise able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the affected Services, and Netskope will provide a pro rata refund of prepaid fees received by Netskope for the remaining portion of the subscription period following the effective date of termination.

5. Security.

5.1 **Security Measures**. Netskope shall maintain appropriate administrative, physical and technical safeguards for the security, confidentiality and integrity of Personal Data as set forth Exhibit B ("**Security Measures**") to protect Personal Data from Security Incidents. Netskope may review and update its Security Measures from time to time, provided that any such updates will not materially diminish the overall security of the Services during the Customer's then current subscription period.

5.2 **Third-Party Certifications and Audits.** Netskope has obtained third-party certifications and audits, which evidence Netskope's compliance with its obligations under this DPA, including (i) Netskope's ISO 27001 and ISO 27018 third-party certifications, (ii) Netskope's SOC 2 Type II audit reports, and (iii) Netskope's most recently completed relevant industry standards certifications or reports (collectively, "**Reports**"). Reports are generally made available to Netskope customers throughout the subscription period, upon a signed confidentiality agreement. Customer is responsible for reviewing the information made available by Netskope relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

5.3 **Confidentiality of Processing**. Netskope shall ensure that any person who is authorized by Netskope to Process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

6. Customer Audit Rights.

6.1 Audits shall be available to Customer (i) upon Netskope's notice to Customer of a Security Incident, (ii) as required by a supervisory authority under applicable Data Protection Laws, or (iii) if neither (i) or (ii) above apply, then no more than once annually. Upon receipt of a written audit request, Netskope shall provide Customer, the requesting supervisory authority, or Customer's appropriately qualified third-party representative (collectively, "**Auditor**"), access to its Reports, books, and/or records. If the requested audit is in response to Netskope's notice of a Security Incident or a request made by a supervisory authority, then Netskope shall permit the scope of the audit to include onsite access at Netskope's offices if necessary to demonstrate Netskope's compliance with its obligations under this DPA.

6.2 Audits shall be performed upon a minimum of 30 days advance written notice and in a manner that is least disruptive to Netskope employees, operations, and the delivery of Services to customers. Netskope and Customer shall mutually determine in advance the details of the audit, including reasonable start date, scope, duration, security and confidentiality controls applicable to the audit. Auditor costs and expenses in connection with any audit shall be borne exclusively by Customer. Netskope may charge a fee (rates shall be reasonable, taking into account the resources expended by Netskope) for any such

audit that exceeds one day onsite.

6.3 The Reports, audit, and any information arising from any audit are deemed to be Netskope's confidential information. An Auditor may be required to execute a separate confidentiality agreement with Netskope prior to any review of Reports or an audit of Netskope. Netskope may object in writing to a third-party Auditor, if in Netskope's reasonable opinion, the Auditor is not suitably qualified or is a competitor of Netskope. Any such objection by Netskope will require Customer to either appoint another Auditor or conduct the audit itself.

7. Data Transfers

7.1 **Hosting and Processing Locations.** Netskope will only Process Personal Data in the region(s) offered by Netskope that are selected by Customer in Customer's implementation and configuration of the Services. Customer is solely responsible for selecting the regions in which it accesses or transmits the Personal Data, for any transfer or sharing of Personal Data by Customer, and for any subsequent changes in Service configurations implemented by or at the direction of Customer (either for the same Account, a different Account, or a separate Service). Once Customer has selected and implemented a Service configuration, Netskope will not Process Personal Data from outside the data centers included in Customer's configuration except as reasonably necessary to provide the Services procured by Customer, or as necessary to comply with the law or binding order of a governmental body.

7.2 **Transfer Mechanisms.** If Data Protection Laws place restrictions on the transfer of Personal Data across international borders, then Netskope will work with the Customer to ensure that international transfers of Personal Data stored by Netskope are performed in accordance with Data Protection Laws, and if required by Data Protection Laws, the parties will execute such applicable Compliant Transfer Mechanism. Customer remains responsible for ensuring that Customer's communication transmissions using the Services are compliant with Data Protection Laws.

(a) **EEA and Switzerland.** To the extent that Netskope maintains Personal Data and transfers such Personal Data outside of the European Economic Area ("**EEA**") or Switzerland, to a jurisdiction other than a jurisdiction in the EEA, or the European Commission-approved countries providing adequate data protection, Netskope agrees it will transfer such data under the EU Standard Contractual Clauses, attached as Exhibit C, or any such clauses as amended, replaced, or superseded by a decision of the European Commission or by legally binding decision made by any other authorized body. The parties are entering into Module 2 of the Standard Contractual Clauses.

(b) **UK.** To the extent that Netskope maintains UK Personal Data and transfers such UK Personal Data to a jurisdiction other than a jurisdiction in the UK, European Union ("**EU**"), the EEA, or the UK or EU-approved countries providing adequate data protection, Netskope agrees it will transfer such data using the UK Standard Contractual Clauses Addendum, attached as Exhibit D, or any other Transfer Mechanism as adopted by a decision of the applicable supervisory authority or by a legally binding decision made by any authorized body.

(c) Netskope shall be the "data importer" and Customer is the "data exporter" under the Standard Contractual Clauses (notwithstanding that Customer may be an entity located outside of a restricted country). Notwithstanding the foregoing, Netskope may adopt any alternative Compliant Transfer Mechanism in accordance with Data Protection Laws, in which case Netskope will notify Customer of the relevant Compliant Transfer Mechanism and ensure that such transfers are made in accordance with it.

8. **Return or Deletion of Data.** Customer may retrieve or delete all Personal Data stored by Netskope upon expiration or termination of the Agreement as set forth in the Agreement. Any Personal Data not deleted by Customer shall be deleted by Netskope promptly upon the later of (i) 90 days after expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement. Notwithstanding the foregoing, Netskope shall not be required to delete Personal Data to the extent Netskope is required by applicable law or order of a governmental or regulatory body to retain the Personal Data. Where Netskope is required to retain Personal Data as set forth in the preceding sentence, then Netskope will notify Customer of such requirement, to the extent legally permitted.

9. Security Incident Response.

9.1 **Security Incident Reporting.** If Netskope becomes aware of a Security Incident, Netskope shall notify Customer without undue

delay. Netskope shall promptly take reasonable steps to contain, investigate, and mitigate the Security Incident.

9.2 **Security Incident Communications.** Netskope shall provide Customer timely information about the Security Incident, including, to the extent available, the nature and consequences of the Security Incident, the measures taken and/or proposed by Netskope to mitigate or contain the Security Incident, the status of Netskope's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Netskope personnel may not have visibility to the content of Personal Data, Netskope may not be able to provide information as to the particular nature of the Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of Netskope with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Netskope of any fault or liability with respect to the Security Incident.

10. Cooperation.

10.1 **Data Subject Requests.** To the extent legally permitted, Netskope shall promptly notify Customer if Netskope receives a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Personal Data, or to restrict the Processing of Personal Data ("**Data Subject Request**"). To the extent that the Customer is able to directly access or control Personal Data hosted in the Service, Customer will be responsible for responding to and complying with any such Data Subject Request. To the extent that Customer is unable to access or control the relevant Personal Data within the Services, taking into account the nature of the Processing, Netskope shall (upon Customer's written request) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

10.2 **Data Protection Impact Assessments.** Netskope shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, to the extent such information is available to Netskope and where Customer does not otherwise have access to the relevant information.

10.3 **Government Inquiries.** If compelled to disclose Personal Data to a law enforcement or governmental entity, then Netskope will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Netskope is legally permitted to do so.

11. Additional Terms to the Standard Contractual Clauses

11.1 The parties agree that the following terms shall apply where the Standard Contractual Clauses are in effect between the parties:

(a) for the purposes of clause 8.9 of the Standard Contractual Clauses, the parties agree that the audits shall be carried out in accordance with Section 6 of this DPA;

(b) for the purposes of clause 9(a) of the Standard Contractual Clauses, the parties agree that Netskope has Customer's general authorisation to engage Sub-processors in accordance with Section 4 of this DPA and that any changes to the Sub-processors engaged by Netskope shall be governed in accordance with Section 4 of this DPA; and

(c) for the purposes of clause 12 of the Standard Contractual Clauses, any claims brought under the Standard Contractual Clauses shall, to the maximum extent permitted by law, be subject to any aggregate limitations on liability set out in the Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under the Standard Contractual Clauses.

12. Relationship with the Agreement.

12.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment or exhibit (including the Standard Contractual Clauses, as applicable) that Netskope and Customer may have previously entered into in connection with the Services.

12.2 Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict regarding the Processing of Personal Data.

Notwithstanding the foregoing, and solely to the extent applicable to any Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state health care laws, rules or regulations ("**HIPAA Data**"), if there is any conflict between this DPA and a Business Associates Agreement between Customer and Netskope ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

12.3 Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA or other data protection agreements in connection with the Agreement (if any), shall be subject to the limitations on liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by a party in relation to the Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the incurring party's liability under the Agreement as if it were liability under the Agreement. In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

12.4 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

This DPA shall only become legally binding between Customer and Netskope when executed by each party's authorized representative below.

Netskope, Inc.	Customer:
Signed: James Bushnell	Signed:
Printed Name: James Bushnell	Printed Name:
Title: General Counsel	Title:
Date: November 29, 2022	Date:
Address:	Address:
Netskope, Inc.	
2445 Augustine Drive, Suite 301	
Santa Clara, CA 95054 USA	

Exhibit A

Processing Details

A. LIST OF PARTIES

Data Exporter(s):

Name: Customer
Address: As specified in the DPA.
Contact person's name, position and contact details: As specified in the DPA.
Activities relevant to the data transferred under these Clauses: data processing for the performance of the Agreement.
Role (controller/processor): Controller

Data Importer(s):

Name: Netskope, Inc.

Address: 2445 Augustine Drive, Suite 301, Santa Clara, CA 95054.

Contact person's name, position and contact details: James Bushnell, General Counsel, legal@netskope.com.

Activities relevant to the data transferred under these Clauses: data processing for the performance of the Agreement.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The categories of Data Subjects to which Personal Data may include, but are not limited to: employees and independent contract persons of Customer and Authorized Affiliates.

Categories of personal data transferred

The categories of Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to: name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number; Source IP address of the user, Active Directory (AD) name of the user, Organizational Unit (OU) mapping of the user in Active Directory (conditional, if exposed by the logs), cloud application accessed by the user (no Personal Data), Activity performed by the user in the cloud application (activity limited to data exchange interfaces), and Active Directory name and/or email alias of parties that data is shared with through the cloud application.

Sensitive data transferred (if applicable) and applied restrictions or safeguards.

Use of the Services does not require the Processing of any sensitive data. Information transmitted is solely at the discretion of Data Exporter and without any knowledge of or direction from Data Importer; no specific measures other than those set forth in Exhibit B shall be applied to sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Processing and the transfer of data will be on a continuous basis for the subscription period.

Nature of the processing

Netskope provides the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Netskope shall Process Personal Data only for the Purposes.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Netskope shall retain Personal Data for the period specified in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors are listed at https://www.netskope.com/netskope-sub-processors and also includes Netskope Affiliates. Processing shall be in accordance with section 4 of the DPA.

netskope

Exhibit B

Security Measures

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) designed to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Pseudonymization and data minimization

ID	Measure
1.1	Personal data is pseudonymized / key-coded whenever directly identifying data are not necessary for data processing
1.2	Lists with pseudonyms / key-codes are stored separately from pseudonymized / key-coded data, and access to such lists is restricted
1.3	Where subsets of personal data are sufficient for data processing steps performed by a function / department, only such subsets are used and accessible by such functions / departments

Confidentiality, integrity, availability and resilience of processing systems and services

ID	Measure
2.1	Internal policies require that personal data is not used for any purpose other than agreed in the contract
2.2	Only authorized personnel are permitted to modify personal data within the scope of their function
2.3	Modification of personal data is logged in an audit trail
2.4	Personal data received from different customers are processed and stored physically or logically separated to ensure that the data of a specific customer can always be identified
2.5	Each computer system runs an up-to-date antivirus / malware protection solution
2.6	Server rooms are protected against overvoltage, power interruption, overheating, fire, and water and those measures are regularly checked and maintained
2.7	Regular backups are performed (daily incremental backup, weekly full backup)
2.8	Data carriers are stored in secure areas and inventory documentation is maintained
2.9	Physical documents containing personal data are placed in a safe or secure environment
2.10	Electronic communication is protected (e.g., through state-of-the-art encryption)

Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

ID	Measure
3.1	Data restore tests of backups are performed regularly
3.2	A business continuity strategy is in place and tested at least once per year
3.3	Regular disaster recovery tests are performed

Testing, assessing and evaluating the effectiveness of technical and organizational measures

ID	Measure
4.1	Security measures are regularly assessed to ensure appropriateness and correct implementation
4.2	Fulfillment of contractual obligations of subcontractors are regularly verified (SLA monitoring)
4.3	Regular penetration tests are performed and mitigating activities based on the associated risk
4.4.	Tests, audits and assessments are documented

Measures for user identification and authorization

ID	Measure
5.1	Authorization concept for data access is documented and implemented

5.2	Individuals who process personal data are identifiable and formally authorized to do so
5.3	Users have a dedicated user ID for authentication against systems user management
5.4	Each user has an individual, complex password and no group accounts are used for systems processing personal data
5.5	A process is implemented to modify / deactivate user accounts when a user changes job function or leaves the company
5.6	Access to applications, files and records are restricted according to a "need-to-know" principle
5.7	Computers that are used to process personal data (including remotely) are password-protected after the boot sequence
5.8	Computers that are used to process personal data (including remotely) are password-protected when left unattended and password-protected screensaver are enabled
5.9	Users with high-privilege access are required to use multi-factor authentication

Protection of data during transmission

ID	Measure
6.1	Personal data in transit is encrypted with a state-of-the-art methodology during transmission by Netskope from / to third parties and service providers. This excludes Customer communications transmitted using the Netskope communication network; Customer communications that are not encrypted by the Customer remain unencrypted in transmission.
6.2	Data carriers are sealed during physical transportation of personal data

Protection of data during storage

ID	Measure
7.1	Backups are created and stored in protected environments / backup procedure is automatically monitored and restoration performed regularly
7.2	Sensitive personal data at rest is encrypted with a state-of-the-art methodology
7.3	Measures are implemented to prevent unauthorized data exports (e.g. interfaces are technically restricted, data loss prevention system are implemented, etc.)

Physical security of locations at which personal data are processed

ID	Measure
8.1	Written regulations and/or policies are in place regarding admission and access control and obtaining/changing/withdrawing access/admission rights
8.2	Access controls are in place to avoid unauthorized access to premises (e.g., electronic access control, registration desk, night guards etc.)
8.3	Access controls are in place to restrict access to data centers and server rooms to specifically defined access groups, whose access rights and roles are regularly evaluated and documented
8.4	Access to data centers and server rooms is traceable
8.5	Unauthorized admission/access attempts are detected, documented and followed up
8.6	Video surveillance and / or alarm devices are in place
8.7	Personnel with access authorization always need to carry visible IDs including their photo
8.8	Visitors and personnel without access authorization are always accompanied
8.9	Visitors are registered and need to carry a visitor's ID
8.10	Security relevance is defined for premises, locations, buildings, rooms and other areas
8.11	Protection measures are implemented such as automatic closing and locking of doors, locking of all building entrances, windows and doors
8.12	Windows and doors at data centers and offices are burglar resistant (e.g., SG1 VdS 2333)

Event logging

ID	Measure
9.1	Users' and administrators' activities (logon, logoff, denial of access, etc.) are logged on systems processing personal data
9.2	Administrative changes are logged
9.3	External support is logged
9.4	Regarding the network, operating system and applications, there is a procedure in place for dealing with and documenting incorrect log-in attempts
9.5	Logging protocols are securely stored and protected against unauthorized tampering
9.6	Internal network traffic monitored and evaluated (e.g. IDS/IPS systems used, proxy servers with content filters etc.)

System configuration, including default configuration

ID	Measure
10.1	Processes are implemented to prevent use and installation of unauthorized hardware and / or software in the company's IT infrastructure
10.2	Firewalls are in place on network level to prevent unauthorized access to network, operating systems, devices and applications
10.3	Demilitarized zones are implemented
10.4	For remote access, VPN restrictions are implemented (e.g., site2site connection)
10.5	Users are automatically deactivated after several failed logins
10.6	Expiration of user passwords is implemented
10.7	Processes are implemented for rolling out (operating) system, network and application patches and updates and dealing with security gaps
10.8	Network infrastructure and configurations well as changes are documented
10.9	Test and productive environments are separated
10.10	Operating systems and interfaces are hardened in accordance with state-of-the-art standards

Internal IT and IT security governance and management

ID	Measure
11.1	A formal information security management system (ISMS) is implemented
11.2	A password policy is in place that prohibits sharing of passwords, specifies state-of-the-art requirements for password-quality and outlines processes after disclosure of a password and the unblocking/resetting of accounts/passwords
11.3	Technical measures are implemented to enforce the password policy
11.4	Passwords are stored encrypted with state-of-the-art encryption
11.5	Specific measures are implemented to protect central passwords (e.g., administrator, directory (recovery), root passwords) from unauthorized access
11.6	Personnel are obliged to obey data security and confidentiality policies
11.7	A policy for documenting and implementing system roles and rights is documented and implemented
11.8	Data protection and data security responsibilities have been assigned to dedicated individuals
11.9	Employees processing personal data are trained on data privacy and security with refresher training annually
11.10	Internal process instructions cover activities necessary for processing personal data
11.11	Data privacy relevant processing activities are assessed to meet legal requirements and documented
11.12	(Sub-)processors are selected in accordance with data privacy and IT Security considerations and requirements

Certification/assurance of processes and products

ID	Measure
12.1	Audits with respect to internal policies are performed regularly and documented
12.2	Audits with respect to technical and organizational security measures are performed regularly and documented
12.3	Audit reports on effectiveness of internal control frameworks are available, specifically SSAE18, SOC 2 and BSI C5
12.4	Certificates are available and regularly renewed, specifically ISO 27001, ISO 27017, ISO 27018 and CSA STAR

Limited data retention

ID	Measure
13.1	Retention periods are defined for personal data
13.2	Processes are implemented for data deletion according to retention policies
13.3	State-of-the-art data deletion processes are implemented ensuring data recovery is not possible

Data portability and erasure

ID	Measure
14.1	A process is in place to permanently and safely destroy data that is no longer required
14.2	A process is in place for secure disposal of documents or data carriers containing personal data
14.3	Physical media is destroyed according to NIST 800-88

Transfers to Sub-processors

Netskope Sub-processors are required to maintain technical and organizational measures consistent to those set out in this Exhibit B as applicable to the Personal Data processed by those Sub-processors.

netskope

Exhibit C

Standard Contractual Clauses (Module 2)

SECTION I

Clause 1
Purpose and Scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking Clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 - Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 - Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 - Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 - Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 - Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not

in line with the requirements under Clause 14(a).

8.6 - Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 - Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 - Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 - Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate

documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data Subject Rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clause

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is

based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 - Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 - Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Ireland.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

netskope

APPENDIX

ANNEX I TO THE SCCs

A. LIST OF PARTIES

As specified in Exhibit A. The parties agree that execution of the DPA shall constitute execution of these Standard Contractual Clauses by both parties.

B. DESCRIPTION OF TRANSFER

As specified in Exhibit A. The competent supervisory authority shall be in accordance with Clause 13 or otherwise the Data Protection Commission of Ireland.

ANNEX II TO THE SCCs

As specified in Exhibit B.

ANNEX III TO THE SCCs

LIST OF SUB-PROCESSORS

The parties acknowledge that Article 28 of the GDPR allows for the general written authorization of a sub-processor subject to notice of, and the opportunity to object to, the sub-processor. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 9(a) of the Standard Contractual Clauses, to engage onward sub-processors listed at https://www.netskope.com/netskope-sub-processors and Netskope Affiliates.

Exhibit D

UK Addendum to the EU Standard Contractual Clauses

Part 1: Tables

The parties agree to use the information provided in the DPA, including any exhibits, schedules and appendices incorporated into the DPA, to complete the tables. Start date shall be the Effective Date. Either party may end this Addendum when the Approved Addendum changes.

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses, are incorporated by reference.