AMENDMENT TO THE ZSCALER DATA PROCESSING AGREEMENT

HOW THIS AMENDMENT APPLIES

This Amendment to the Zscaler Data Processing Agreement is only valid and legally binding if the Customer entity signing it entered into a Data Processing Agreement with Zscaler.

INSTRUCTIONS FOR SIGNING THIS AMENDMENT

This Amendment to the Zscaler Data Processing Agreement consists of this cover page, the Amendment, Exhibit A, Exhibit B, Exhibit C (with its Annex I and Annex II), and Exhibit D. To complete this Amendment, Customer must:

1. Complete the “data exporter” details on the first page of Annex I (page 19)
2. Complete and sign each of the Customer/data exporter signature blocks (pages 3 and 19)
3. Submit the completed and signed Amendment to Zscaler by email to privacy@zscaler.com.

If you have any questions about this Amendment, please contact privacy@zscaler.com.

AMENDMENT TO THE ZSCALER DATA PROCESSING AGREEMENT

This Amendment is entered into on the date of the last signature below (the "**Amendment Effective Date**") by and between **Zscaler, Inc**. ("**Zscaler**") and ____ ("**Customer**").

WHEREAS, the parties executed a Data Processing Agreement ("**DPA**"), and now wish to amend the DPA as follows:

1. ***If present, the definitions of "Standard Contractual Clauses" or "Clauses" and "Privacy Shield" shall be entirely deleted. Additionally, if present, Section 9 (Privacy Shield) shall be deleted in its entirety.***

2. ***Capitalized terms and references relating to data transfers from the European Union, the European Economic Area, Switzerland, or the United Kingdom to countries that do not ensure an adequate level of data protection shall be deleted from the DPA and replaced by capitalized terms and references as set out in this Amendment. Any references to specific clauses of the Standard Contractual Clauses shall be replaced with references to the equivalent provisions contained in the EU SCCs (as defined below) or any other Transfer Mechanism (as defined below). All capitalized terms that are not defined in this Amendment will have the meanings assigned to them in the Agreement or DPA. In the event of any conflict between the Amendment, Agreement, or DPA then the Amendment shall prevail.***

3. ***The "International Transfers" section as set out below will entirely replace any section or terms relating to data transfers from the European Union, the European Economic Area, Switzerland, or the United Kingdom to countries that do not ensure an adequate level of data protection as a new section to the DPA.***

"INTERNATIONAL TRANSFERS.

International Transfers. Customer consents to Zscaler Processing or transferring any Personal Data in or to a territory other than the territory in which the Personal Data was first collected. For clarity, Zscaler shall take such measures as are necessary to ensure such Processing or transfer is in compliance with applicable Data Protection Legislation and in accordance with any applicable transfer mechanism provisions set forth in the Transfer Mechanism subsection below.

Transfer Mechanism. If applicable Data Protection Legislation places restrictions on the transfer of Personal Data across international borders, then Zscaler will work with Customer to ensure that any international transfer is performed in accordance with applicable Data Protection Legislation and, if required, the parties will execute such applicable legal mechanism ("**Transfer Mechanism**"). This includes executing the following Transfer Mechanisms as part of this DPA:

EU Standard Contractual Clauses ("EU SCCs"): If Personal Data is transferred outside of the European Economic Area ("EEA") or Switzerland to a country that is not recognized under GDPR to offer an adequate level of protection for Personal Data and is not covered by a suitable framework recognized by relevant authorities or courts that offer an adequate level of protection for Personal Data, then the Parties agree to execute the EU SCCs as set out in Module Two (Controller to Processor) attached herein in **Exhibit C** or any such clauses as amended, replaced or superseded by a decision of the European Commission or by a legally binding decision made by any other authorized body.

UK Standard Contractual Clauses Addendum ("UK Addendum"). If Personal Data is transferred outside of the United Kingdom to a country that is not recognized to offer an adequate level of protection for Personal Data and is not covered by a suitable framework recognized by relevant authorities or courts that offer an adequate level of protection for Personal Data, then the Parties agree to incorporate the UK Addendum as attached herein in **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 other authorized body.

Alternative Transfer Mechanism. Zscaler agrees to notify Customer if it determines that a change in applicable Data Protection Legislation will adversely affect or invalidate the warranties and obligations provided under an executed Transfer Mechanism or if an alternative Transfer Mechanism becomes available to use by the Parties. In such an event, Zscaler will work with the Customer to find a mutually agreeable solution to ensure that Personal Data is transferred in compliance with applicable Data Protection Legislation."

4. ***Exhibit A, B, C, and D attached herein shall be added to the DPA, and shall amend any such previous exhibits on the subject matter, as follows:***

a. Exhibit A shall entirely replace any exhibit relating to description of personal data processing and types of personal data processed;

b. Exhibit B shall entirely replace any exhibit relating to description of information security measures (technical and organizational measures);

c. Exhibit C shall entirely replace any exhibit containing the EU Standard Contractual Clauses based on the EU Commission Decision C (2010) 593;

d. Exhibit D shall be added to the DPA as the new exhibit incorporating the UK Addendum.

Except as set forth in this Amendment, the DPA is unaffected and shall continue in full force and effect in accordance with its terms. If there is conflict between this Amendment (including the exhibits) and the DPA (including the exhibits), then the Amendment will prevail.

IN WITNESS WHEREOF, the parties agree as of the Amendment Effective Date as attested by the signatures of their duly authorized representatives:

CUSTOMER:	**ZSCALER, INC.** DocuSigned by:
Signature:______________________	Signature: Shaun Ghafouri AD9C0A33307E4F6...
Printed Name: ______________________	Printed Name: Shaun Ghafouri
Title: ______________________	Title: VP, Associate General Counsel
Date Signed:______________________	Date Signed: December 8, 2022 | 9:02 AM PST

Exhibit A

Details of Personal Data Processing

Subject Matter of Processing	The subject matter of Processing are the Products pursuant to the Agreement.
Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
Categories of Data Subjects	Employees and other authorized users of Customer.
Nature and Purpose of Processing	Nature: Processing as part of the Products ordered by Customer in the Agreement. Purpose: The purpose of the Processing of Personal Data by Zscaler is to provide the Products pursuant to the Agreement.

I. Types of Personal Data Processed

The following table lists the Personal Data that is processed by all Zscaler Products.

Type of Personal Data	**Description**
Directory Information	Information fetched from Customer's corporate directory such as name, employee number, group, and department.
User Identifier	Name, username, email address, or other identifier that identifies a specific user.
IP Addresses	To map an organization's physical office location to a logical location name in the Product based on the source IP of the traffic being sent to Zscaler. IP address of the user's device.
Location	The location of the device being used by a user.

The tables below list the additional Personal Data that is processed by a particular Product. Each table below should be read to be inclusive of the table above.

Zscaler Internet Access (ZIA)	
Type of Personal Data	**Description**
Cookies and other similar technologies	By enabling the "Cookies Persistence" option for Zscaler Remote Browser Isolation, Customer authorizes Zscaler and its permitted third-party hosting service providers the right to store user-level cookies and other similar technologies.
URL	URLs of internet destinations accessed during the internet-based transactions by users from their devices.

Zscaler Digital Experience (ZDX)	
Type of Personal Data	**Description**
Geolocation Data	Geolocation coordinates (longitude and latitude) of a user’s device.
Home Wifi SSID	Home Wi-Fi SSID would be captured if user is working from home.
Device Serial Number	The unique serial number of the device being used by an authorized user.

Zscaler Deception	
Type of Personal Data	**Description**
Phone Number	Mobile phone number to receive SMS message alerts about interactions with decoys by possible threats.

II. <u>Data Storage and Retention</u>

During the Subscription Term, the Customer Logs shall be generally retained by Zscaler for rolling six (6) month periods, depending on the Product. The data storage and retention for each Product can be found at the “Customer Logs & Fair Use” section under “Documentation” at http://help.zscaler.com/. Additionally, Customer may choose to have its Customer Logs stored exclusively in (a) the EEA and Switzerland for ZIA and (b) the EEA for ZPA.

Exhibit B

Zscaler Data Protection and Information Security

1. Secure Files. Throughout the Subscription Term, Customer's Personal Data in Zscaler's possession or control shall be subject to safeguarding and disaster recovery protection and shall be stored at secure physical or electronic facilities operated under Zscaler's control in a geolocation of the Customer's choice.

2. Data Availability. Zscaler shall adhere to appropriate technical and organizational measures that represent the best industry practices in the storage, safeguarding, and preservation of any Customer's Personal Data in Zscaler's possession or control, including performing real-time backups to regional geographically disperse locations and ensuring the security (*i.e.*, both physical and unauthorized remote access) of all hardware and equipment used to host or store such Personal Data pursuant to the provisioning of the SaaS.

3. Safeguards and Controls. Zscaler agrees that during the Subscription Term, and continuing as long as Zscaler controls, possesses, stores, transmits or processes Personal Data, Zscaler and its subcontractors/sub-processors shall employ and maintain reasonable security measures to ensure that all Personal Data in Zscaler's possession or control is protected from unauthorized use, alteration, access or disclosure, and to protect and ensure the confidentiality, integrity and availability of such Personal Data, consistent with all applicable laws and regulations relating to the security and/or privacy of Personal Data ("Data Protection Legislation"). Such security measures shall include, but not be limited to, the following:

a) implementing reasonable restrictions regarding physical and electronic access to such Personal Data, including, but not limited to, physical access controls, secure user authentication protocols, secure access control methods, firewall protection, malware protection, anonymization, tokenization and use of encryption where appropriate or required by Data Protection Legislation;

b) maintaining a reasonable and appropriate written data security policy that includes technological, physical, administrative and procedural controls to protect the confidentiality, integrity and availability of such Personal Data, that encompasses access, retention, transport, and destruction of such Personal Data, and that provides for disciplinary action in the event of its violation;

c) preventing terminated employees from accessing such Personal Data by terminating without undue delay their physical and electronic access to Zscaler's Products;

d) employing assessment, monitoring and auditing procedures to ensure internal compliance with these safeguards;

e) conducting an independent security assessment of these safeguards at least annually, and, upon Customer's reasonable written request not more than once annually, providing certification to demonstrate compliance with all such applicable security requirements; and

f) only using Customer's Personal Data for the purpose of providing the Products contracted under the Agreement, and Zscaler shall not provide any other third party with access to such Personal Data unless it has received prior written consent from Customer, or such access is specifically allowed under the Agreement. For the avoidance of doubt, Customer consents to the use of service providers currently identified at https://www.zscaler.com/legal/subprocessors as of the date of the Agreement ("Sub-processor List"). Zscaler must notify Customer and Customer may object to any new service providers in accordance with the directions set forth in the notification.

4. Reporting. Zscaler shall maintain records, logs and reports concerning its compliance with Data Protection Legislation and/or relevant industry standards, security breaches, storage, processing, and transmission of Personal Data in its possession or control.

As a condition of providing the Products to Customer under the Agreement, no less than once each calendar year, Zscaler will undergo, at its sole cost and expense, a Statement on Standards for Attestation Engagements (SSAE) No. 18 for Reporting on Controls at a Service Organization, Service Organization Controls (SOC) 2 Type 2 audit (or industry equivalent as the standard may progress). Upon Customer's written request, Zscaler will provide Customer with a copy of its most recent SSAE No. 18 SOC 2 Type 2 report on an annual basis, resulting from such audit and such other evidence, information and documentation as is reasonably necessary to demonstrate compliance with this Exhibit.

5. Security Incident Response. Zscaler shall maintain policies and procedures for responding to Security Incidents. In the event of a Security Incident involving unauthorized disclosure, loss, or destruction of Personal Data in Zscaler's possession or control, Zscaler shall:

a) promptly and without undue delay investigate the reasons for and circumstances surrounding such Security Incident;

b) use best efforts and take all necessary actions to contain and mitigate the impact of such Security Incident;

c) provide written notice to Customer after Zscaler confirms a Security Incident;

d) provide a written report to Customer concerning such security incident detailing Zscaler's findings, and update such report periodically thereafter;

e) collect and preserve all evidence concerning the cause, remedial actions and impact related to such Security Incident, which shall meet reasonable expectations of forensic admissibility;

f) document the incident response and remedial actions taken in detail; and

g) so long as Zscaler is not required to violate the confidentiality obligations with any of its other customers, partners or vendors, provide Customer with any relevant documents related to such security breach, including without limitation, any security assessment and security control audit reports, relevant logs and/or any forensic analysis of such security breach.

6. Destruction. Zscaler shall take all reasonable steps to ensure proper destruction (such that Personal Data is rendered unusable and unreadable) after the expiration or earlier termination of the Agreement.

7. Management Direction for Information Security. Zscaler will assign a qualified member of its workforce with expertise in information security to be responsible for the development, implementation, and maintenance of Zscaler's enterprise information security program.

8. Organization of Information Security

a) Zscaler will ensure that the responsibilities of their workforce are appropriately segregated to reduce opportunities for unauthorized or unintentional access, modification, or misuse of the organization's assets.

b) Zscaler will maintain contact with the governing regulatory authorities to ensure ongoing compliance with the mandated regulatory requirements.

c) Zscaler will maintain appropriate contact with special interest groups, specialist security forums, and/or professional associations to remain abreast of evolving information security threats and trends.

d) As applicable, Zscaler will ensure that Information security is addressed within its internal project management processes.

9. Human Resources Security

a) Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

b) Zscaler will train new and existing employees and subcontractors to comply with relevant data security and data privacy obligations. Ongoing training is to be provided at least annually and more frequently as appropriate.

c) To the extent applicable, Zscaler will ensure that employees, contractors, sub-contractors or vendors are required to sign an agreement that contains confidentiality requirements at least as protective as those in the Agreement.

10. Asset Management

a) Zscaler will maintain an inventory of assets associated with information and information processing facilities.

b) Assets maintained in the inventory are assigned to an individual or group that is accountable and responsible for the assigned asset(s).

c) Acceptable use of assets is defined within a formal policy or standard.

d) The return of assets is clearly communicated, via policies and/or training, to all employees and external party users upon termination of their employment, contract or agreement. Return of assets is documented and tracked.

e) Zscaler classifies data in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. Procedures for handling assets are developed and implemented in accordance with this information.

11. Media Handling. Procedures are implemented for the management of removable media in accordance with the information classification.

12. Access Control

a) Zscaler will ensure that Customer's Confidential Information and Personal Data will be accessible only by authorized personnel with appropriate user identification, two-factor authentication and access controls commensurate with information classification.

b) Two-factor authentication is required for remote connectivity.

c) Each authorized personnel shall have unique access credentials and shall receive training which includes a prohibition on sharing access credentials with any other person.

d) Zscaler will have a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.

e) The allocation and use of privileged access rights will be restricted and controlled.

f) The allocation of secret authentication information is controlled through a formal management process.

g) User access rights are reviewed at regular intervals but at a minimum on an annual basis.

h) The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted as appropriate upon change in role or responsibilities.

i) Password management systems are interactive and ensure strong passwords.

13. Cryptography

a) Zscaler has a formal policy on the use of cryptographic controls for protection, including the use, protection and lifecycle of cryptographic keys.

b) Zscaler agrees that all Personal Data will be protected and, where encrypted, will use a Federal Information Processing Standard (FIPS) compliant encryption product, also referred to as 140-2 compliant. Symmetric keys will be encrypted with a minimum of 128-bit key and asymmetric encryption requires a minimum of 1024 bit key length. Encryption will be utilized in the following instances:

i. Personal Data that is stored on any portable computing device or any portable storage medium.

ii. Personal Data that is transmitted or exchanged over a public network.

14. Physical and Environmental Security

a) A clear desk policy for papers and a clear screen policy for facilities processing Personal Data is adopted and adhered to.

b) Systems are located in co-location facilities and are maintained by Zscaler personnel.

c) Only individuals on the approved access list can access Zscaler equipment and systems.

d) All facilities require badge and/or biometric access and have 24x7 security guards and CCTV.

e) Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

f) Access is created and maintained by Zscaler and only authorized to Zscaler personnel with a business need.

g) Visitors to the facility are required to be escorted at all times and are not allowed in caged areas.

15. Operations Security

a) Changes to the organization, business processes, information processing facilities and systems that affect information security shall be formally controlled.

b) Zscaler agrees that development and testing environments shall be separated from operational or production environments to reduce the risks of unauthorized access or changes to the operational or production environment.

c) Zscaler's software development processes and environment must protect against malicious code being introduced into its Product(s), future releases thereof, and/or updates thereto.

d) Zscaler shall have a dedicated team responsible for performing security audits, vulnerability scans, evaluating results and monitoring the remediation of technical vulnerabilities to ensure measures are taken to address the associated risk.

e) Zscaler software that controls access to Confidential Information or Personal Data must log and track all access to the information.

i. Logging facilities and log information shall be protected against tampering and unauthorized access.

ii. Zscaler shall maintain access logs relevant to Personal Data for the time period stated in the Agreement depending on the Product being used.

f) Rules governing the installation of software by Zscaler personnel are established and implemented on operational systems.

16. **Network Security**. Zscaler agrees to implement and maintain network security controls that conform to industry standards, including but not limited to the following:

a) Zscaler will appropriately segment its network to only allow authorized hosts and users to traverse areas of the network and access resources that are required for their job responsibilities.

b) Zscaler will ensure that publicly accessible servers are placed on a separate, isolated network segment typically referred to as the Demilitarized Zone (DMZ).

c) Zscaler will ensure that its wireless network(s) only utilize strong encryption, such as WPA2.

d) Zscaler will have an IDS and/or IPS in place to detect inappropriate, incorrect or anomalous activity and determine whether Zscaler's computer network and/or server(s) have experienced an unauthorized intrusion.

e) As appropriate, groups of information services, users and information systems shall be segregated on networks.

17. **Data Transfers**. Zscaler may transfer Personal Data to provide our Products. The transfers of data may involve movement between jurisdictions and crossing international borders. Zscaler will ensure Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transport or storage and that the transmission facilities receiving any Personal Data can be established and verified. Practices implemented and maintained by Zscaler include, but are not limited to, the following:

a) All management connections to the servers occur over encrypted Secure Shell (SSH), Transport Layer Security (TLS) or Virtual Private Network (VPN) channels and remote access always requires multi-factor authentication.

b) Unless the connection originates from a list of trusted IP addresses, Zscaler does not allow management access from the Internet.

c) Zscaler maintains a change management system to submit, authorize, and review any changes made in the production environment.

d) Zscaler maintains a dedicated Network Operations Center (NOC), which is staffed 24/7.

18. **Communications Security**

a) Formal data transfer policies, procedures and controls shall be in place to protect the transfer of sensitive Confidential Information or Personal Data within electronic messaging.

b) Zscaler will execute a data protection and information security agreement with electronic communication service providers to ensure that security controls meeting Zscaler's requirements have been implemented.

19. **System Acquisition, Development, and Maintenance**

a) Applicable information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

b) Confidential Information or Personal Data involved in application services passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.

c) Zscaler shall have policies that govern the development of software and systems and how information security and integrity are established and applied during development. Zscaler shall have a policy that outlines a governing framework to validate that security controls are present in the solution to ensure confidentially, integrity and availability. Additionally, the policy will outline the processes, procedures, and standards to ensure no known security flaws have been introduced intentionally or unintentionally at any point in the Product's lifecycle or such time as the Product has formally reached end of life.

d) Upon initial hire or engagement of software developers, Zscaler shall provide them with secure software development training. Thereafter, Zscaler shall provide supplemental training periodically as necessary to address changing industry conditions and vulnerabilities. Any such training shall occur at least every two years.

e) Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.

f) Zscaler does not currently outsource system development responsibilities; however, should this change in the future, Zscaler shall supervise and monitor the activity of any such outsourced system development.

20. Service Provider Due Diligence

a) Zscaler will conduct due diligence reviews on our service providers who may have impact on Zscaler's ability to meet the requirements of the Agreement and this Exhibit.

b) Due diligence of such service providers shall include, but is not limited to, determining the appropriate information security requirements that should be included in agreements between Zscaler and its service providers.

21. Application and Software Security. Zscaler agrees that its Product(s) will, at a minimum, incorporate the following:

a) Zscaler uses third party auditors at least annually, to conduct automated (i.e., SAST, DAST and SCA) and manual security (i.e., penetration testing) assessments to ensure the Product codebase contains no known exploitable conditions classified as 'Critical/Very High' or 'High', or otherwise captured on the OWASP Top 10 or SAN Top 25 lists.

b) Zscaler agrees to provide, maintain and support its software and subsequent updates, upgrades, and bug fixes, such that the software is, and remains secure from Common Software Vulnerabilities in accordance with its product end of life (EOL) and end of sale (EOS) policy.

c) Zscaler agrees to provide updates and patches to remediate security vulnerabilities based on severity by CVSSv3 score and will work to remediate any known zero-day exploits without undue delay. In case of critical vulnerabilities, Zscaler will deploy mitigation with urgency upon discovering the issue and push out a patch without undue delay thereafter depending on risk level post mitigation.

Exhibit C

EU Standard Contractual Clauses (EU SCCs)

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – 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.

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 as specified in the DPA 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 clauses

(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.

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 the EU Member State in which the data exporter is established.

(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.

Annex I

This Annex forms part of the EU SCCs and must be completed and signed by the parties. Capitalized terms used in this Annex which are otherwise undefined in the EU SCCs have the meanings given to them in the DPA to which these clauses are attached to. By signing this Annex the parties agree and accept the EU SCCs.

A. List of Parties

Data Exporter (Controller)

Name(s) of data exporting organization:	
Address(es):	
Tel.:	
Email:	

Activities Relevant to Data Transferred:

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all affiliates of such legal entity established within the European Economic Area (EEA), the United Kingdom and Switzerland that have ordered or subscribed to Products through one or more Agreement(s).

Data Exporter Name:

Printed Name: ____ (affix stamp of organisation below, if any)

Title: ____

Signature:____

Date Signed:____

Data Importer (Processor)

Name of data importing organization:	Zscaler, Inc.
Address:	120 Holger Way, San Jose, CA 95134 USA
Tel.:	(408) 533-0288
Email:	privacy@zscaler.com

***Activities Relevant to Data Transferred*:**

Zscaler, Inc. is a provider of cloud-based Internet security solutions which process Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement. This includes providing the Product(s) and customer support services.

Data Importer Name: Zscaler, Inc.

Printed Name: Shaun Ghafouri

Title: VP, Associate General Counsel

Signature: DocuSigned by: Shaun Ghafouri AD9C0A33307E4F6...

Date Signed: December 8, 2022 | 9:02 AM PST

B. Description of Transfers

a. Nature of the Processing

The processing by Data Importer shall be to enable (1) the performance of the Product which includes facilitating access for customer administrators of the Products; (2) to provide any technical and customer support as requested by data exporter, and (3) to fulfil all other obligations under the Agreement.

b. Categories of Data Subjects

Employees and other authorized users of the Data Exporter.

c. Categories of Personal Data

Personal Data provided by the Data Exporter to facilitate the Data Importer's provision of Products to the Data Exporter, as specified in *<u>Exhibit A</u>* *to the DPA.*

d. Sensitive Data

Any sensitive data that may be visible or exposed in Data Exporter's traffic flowing through the Products is incidental and dependent on the Data Exporter's use of the Products.

e. Frequency and Duration of Processing of the Transfers

Transfers will occur on a continuous basis on the Data Exporter's use of the Products. The Processing will continue until the expiration or termination of the Agreement.

f. Retention of Personal Data Transferred

Personal Data will be retained as specified in Exhibit A of the DPA during the Subscription Term.

g. Transfers to Sub-processors

i. Nature of the Processing

The processing by sub-processors shall be to enable (1) the performance of the Product which includes providing data centers to host the Products; (2) to provide any technical and customer support as requested by data exporter, and; (3) to fulfil all other obligations under the Agreement.

ii. Frequency and Duration of Processing of the Transfers

Transfers will occur on a continuous basis during the Data Exporter's use of the Products. The Processing will continue until the expiration or termination of the Agreement.

C. Competent Supervisory Authority

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

Annex II

The Exhibit B (Zscaler Data Protection and Information Security) of the DPA will form part of the EU SCCs and serve as the Annex II.

Appendix 1 to the EU SCCs:

This Appendix forms part of the EU SCCs. All references to the GDPR in the EU SCCs should be understood as references to the Federal Act on Data Protection ("FADP") of Switzerland insofar as the data transfers are subject to the FADP.

Insofar as the data transfers are subject to the FADP, the EU SCCs will be governed by the law of Switzerland.

The term "Member State" in the EU SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of claiming their rights in their habitual place of residence (Switzerland) in accordance with Clause 18(c) EU SCCs.

Appendix 2 to the EU SCCs

If Personal Data is transferred outside of the United Kingdom to a country that is not recognized to offer an adequate level of protection for Personal Data and is not covered by a suitable framework recognized by relevant authorities or courts that offer an adequate level of protection for Personal Data, then the Parties agree to amend the EU SCCs in accordance with the UK Addendum as attached herein in **Exhibit D** (**UK Addendum to the EU Commission Standard Contractual Clauses**). By signing Annex I of the **Exhibit C** (**EU Standard Contractual Clauses (EU SCCs)**), the parties agree and accept the UK Addendum.

zscaler

Exhibit D
UK Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The day of the last signature of Annex I of the EU SCCs.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Annex I of the EU SCCs Trading name (if different): Main address (if a company registered address): See Annex I of the EU SCCs Official registration number (if any) (company number or similar identifier):	Full legal name: See Annex I of the EU SCCs Trading name (if different): Main address (if a company registered address): See Annex I of the EU SCCs Official registration number (if any) (company number or similar identifier):
Key Contact	Contact details including email: See Annex I of the EU SCCs	Contact details including email: See Annex I of the EU SCCs
Signature (if required for the purposes of Section 2)	See Appendix 2 of the EU SCCs	See Appendix 2 of the EU SCCs

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The day of the last signature of Annex I of the EU SCCs. Reference (if any): Exhibit C (EU SCCs) of the DPA Other identifier (if any): N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Annex I of the EU SCCs
Annex 1B: Description of Transfer: Annex I of the EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Exhibit B of the DPA

Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.

Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

    > “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”;

    c. Clause 6 (Description of the transfer(s)) is replaced with:

    > “The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

    d. Clause 8.7(i) of Module 1 is replaced with:

    > “it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

    > “the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

    f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

    i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

    l. In Clause 16(e), subsection (i) is replaced with:

    > “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

    m. Clause 17 is replaced with:

    > “These Clauses are governed by the laws of England and Wales.”;

    n. Clause 18 is replaced with:

    > “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

    o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

DocuSign

Certificate Of Completion

Envelope Id: F6F3FDBFC48842ADA6B8295EF9B435FE		Status: Completed
Subject: Complete with DocuSign: Zscaler DPA Amendment (SCCs and UK Addendum)(December 2022).docx		
Source Envelope:		
Document Pages: 26	Signatures: 2	Envelope Originator:
Certificate Pages: 1	Initials: 0	Addison Brown
AutoNav: Enabled		Addison.Brown@zscaler.com
EnvelopeId Stamping: Enabled		IP Address: 76.100.131.214
Time Zone: (UTC-08:00) Pacific Time (US & Canada)		

Record Tracking

Status: Original 12/8/2022 8:12:15 AM	Holder: Addison Brown Addison.Brown@zscaler.com	Location: DocuSign

Signer Events	Signature	Timestamp
Shaun Ghafouri sghafouri@zscaler.com VP, Associate General Counsel Zscaler Inc. Security Level: Email, Account Authentication (None)	DocuSigned by: Shaun Ghafouri AD9C0A33307E4F6... Signature Adoption: Pre-selected Style Using IP Address: 199.168.150.9	Sent: 12/8/2022 8:17:40 AM Viewed: 12/8/2022 9:02:39 AM Signed: 12/8/2022 9:02:46 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Addison Brown addison.brown@zscaler.com Security Level: Email, Account Authentication (None)	COPIED	Sent: 12/8/2022 9:02:48 AM Resent: 12/8/2022 9:02:52 AM Viewed: 12/8/2022 9:04:24 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	12/8/2022 8:17:40 AM
Certified Delivered	Security Checked	12/8/2022 9:02:39 AM
Signing Complete	Security Checked	12/8/2022 9:02:46 AM
Completed	Security Checked	12/8/2022 9:02:48 AM

Payment Events	Status	Timestamps