zscaler

ZSCALER DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into between Zscaler, Inc., located at 110 Rose Orchard Way, San Jose, CA 95134, USA ("**Zscaler**" or "**Data Importer**"), and Customer. This DPA is effective on the date that it has been duly executed by both parties.

HOW THIS DPA APPLIES

This DPA is only valid and legally binding if the Customer entity signing it is a party to an Agreement and is a Controller to which Article 3 of the GDPR applies. This DPA forms part of such Agreement.

Zscaler is a party to this DPA for the sole purpose of complying with any obligations that are expressly stated to be Zscaler obligations in this DPA, including assisting Customer to comply with its legal obligations under applicable Data Protection Legislation with respect to Personal Data that Zscaler processes when providing the Products to Customer.

INSTRUCTIONS FOR SIGNING THIS DPA

This DPA consists of this cover page, the DPA Terms, Exhibit A, Exhibit B (which contains two appendices), and Exhibit C. Any modifications to the terms of this DPA (whether handwritten or otherwise) will render this DPA ineffective unless Zscaler has separately agreed to those modifications in writing. To complete this DPA, Customer must:

1. Complete the "data exporter" details on the first page of Exhibit B.
2. Complete and sign each of the four (4) Customer/data exporter signature blocks (pages 6, 13, 15 and 16).
3. Submit the completed and signed DPA to Zscaler by email to privacy@zscaler.com

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

DPA TERMS

1. DEFINITIONS

"**Agreement**" means any agreement between Zscaler and a specific customer or between a specific customer and a Zscaler-authorized partner under which Products are provided by Zscaler and/or a Zscaler-authorized partner to that customer. Such an agreement may have various titles, such as "Order Form", "Quotation", "Purchase Order", "End User Subscription Agreement", or "Master Services Agreement".

"**Controller**", "**data subject**", "**personal data**", "**personal data breach**," "**process**", "**processing**", "**processor**", and "**supervisory authority**" have the same meanings as in the GDPR.

"**Customer**" means the customer that is identified on, and is a party to, the Agreement, and any Customer affiliates.

"Data Exporter" means the Controller who transfers the Personal Data to a Data Importer.

"Data Importer" means the Processor who agrees to receive Personal Data from the Data Exporter intended for Processing on the Data Exporter's behalf after the transfer in accordance with its instructions and the terms of the Standard Contractual Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 45 of the GDPR.

"**Data Protection Legislation**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area (EEA), and their member states, applicable to the processing of Personal Data under the Agreement, as amended or replaced from time to time, including without limitation the General Data Protection Regulation (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 (the "**GDPR**").

"**Personal Data**" means personal data that is submitted to the Products by Customer and processed by Zscaler for the purposes of providing the Products to Customer. The types of Personal Data and the specific uses of the Personal Data are detailed in Exhibit A attached hereto.

"**Privacy Shield**" means the EU-U.S. and the Swiss-U.S. Privacy Shield self-certification programs operated by the U.S. Department of Commerce, as further described in Section 9 of this DPA, providing a mechanism for complying with the GDPR when transferring Personal Data from the European Union and Switzerland to the United States.

"**Products**" means the Zscaler services and products ordered or subscribed to by Customer in an Agreement.

"**Standard Contractual Clauses**" or **"Clauses"** means the Standard Contractual Clauses based on the Commission Decision C(2010)593 Standard Contractual Clauses (processors) document attached hereto as Exhibit B or any such clauses amending, replacing or superseding those by a European Commission decision or by a decision made by any other authorized body.

2. DATA PROCESSING

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Personal Data for the provision of the Products, Customer is the Controller and Zscaler is the Processor.

2.2 Processing of Personal Data. Zscaler may process Personal Data on behalf of Customer as part the provision of the Products to Customer. Zscaler will process Personal Data as follows:

(a) Zscaler will comply with applicable Data Protection Legislation;

(b) Zscaler will implement appropriate technical, administrative, physical and organizational measures to adequately safeguard and protect the security and confidentiality of Personal Data against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access;

(c) Zscaler will process the Personal Data only in accordance with any documented Customer instructions received by Zscaler with respect to the processing of such Personal Data and in a manner necessary for the provision of the Products by Zscaler which will, for the avoidance of doubt, include processing in accordance with this DPA and the Agreement;

(d) Zscaler will ensure that persons authorized to process Personal Data on behalf of Zscaler have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(e) Zscaler will assist Customer by appropriate technical and organization measures for the fulfillment of Customer's obligations to respond to requests for exercising a data subject's rights with respect to Personal Data under Chapter III of the GDPR;

(f) Zscaler will promptly inform Customer if in its opinion compliance with any Customer instruction would infringe Data Protection Legislation.

(g) Zscaler will assist Customer in complying with its obligations with respect to Personal Data pursuant to Articles 32 to 36 of the GDPR;

(h) Zscaler will, at Customer's option, and subject to the terms of this DPA (i) delete or return all Personal Data to Customer after the end of the provision of the Products, and (ii) delete existing copies of Personal Data unless applicable law of the EU or an EU member state requires retention of the Personal Data;

(i) Zscaler will make available to Customer all information necessary to demonstrate compliance with its obligations as a Processor as specified in Article 28 of the GDPR, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, consistent with Section 8 of this DPA;

(j) Zscaler will maintain a record of all categories of processing activities carried out on behalf of Customer in accordance with Article 30(2) of the GDPR; and

(k) Zscaler and its representatives will cooperate, on request, with the relevant supervisory authority in providing the Products.

2.3 Customer Processing. Customer will, in its use of the Products, process Personal Data in accordance with the requirements of applicable Data Protection Legislation. For the avoidance of doubt, Customer's instructions to Zscaler for the processing of Personal Data will comply with applicable Data Protection Legislation. Customer will have sole responsibility for the accuracy, quality, and legality of Personal Data and for ensuring that the Personal Data was lawfully acquired by Customer. Customer shall ensure that Customer is entitled to transfer the relevant Personal Data to Zscaler so that Zscaler and its Sub-processors (as defined in Section 5.1 of this DPA) may lawfully use, process and transfer the Personal Data in accordance with this DPA and the Agreement on Customer's behalf as a Processor.

2.4 Processing Instructions. Customer instructs Zscaler to process Personal Data for the following purposes: (a) processing necessary for the provision of the Products and in accordance with the Agreement; (b) processing initiated by Customer's end users in their use of the Products; and (c) processing to comply with the other reasonable written instructions provided by Customer to Zscaler (e.g., via email or via support requests) where such instructions are consistent with the terms of the Agreement, as required to comply with applicable Data Protection Legislation, or as otherwise mutually agreed by the parties in writing. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the foregoing is deemed an instruction by the Data Exporter to process Personal Data. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Zscaler to Customer upon Customer's written request.

2.5 Customer Transaction Logs. Customer agrees and understands that Personal Data will be processed by Zscaler from its global data centers depending on where Customer's users are located. However, during the deployment process, Customer may choose to have its transaction logs (**"Customer Logs"**) stored in the EEA and Switzerland using the following hub data centers: (1) Interxion Deutschland GmbH in Frankfurt, Germany; (2) Equinix (Netherlands) B.V. in Amsterdam, Netherlands; and (3) Equinix (Switzerland) GmbH in Zurich, Switzerland. If Zscaler changes the location or provider of these hub data centers, Zscaler shall provide Customer with written notice containing the updated provider name(s) and/or address(es) of the hub data center(s). For purposes of clarity, Zscaler's data centers are not Sub-Processors for purposes of Section 5 of this DPA.

The Customer Logs shall be retained by Zscaler for rolling six (6) month periods during the subscription term. However, Zscaler offers Customer the option to purchase Nanolog Streaming Service (NSS) which allows Customer to stream the Customer Logs in real-time to Customer's premises where the Customer Logs can be sent to multiple Customer systems allowing Customer to customize its retention and deletion of the Customer Logs. With NSS, copies of the Customer Logs are retained and deleted by Zscaler as set forth in the Agreement. Additionally, Zscaler offers its Customer the option to purchase a Private Nanolog Cluster which allows Customer to customize its retention and deletion of the Customer Logs. With the Private Nanolog Cluster, Customer may retain and delete the Customer Logs for a minimum one (1) month period up to a maximum six (6) month period, and Zscaler does not retain copies of the Customer Logs.

3. RIGHTS OF DATA SUBJECTS

Zscaler shall, to the extent legally permitted, promptly notify Customer if Zscaler receives a request from a data subject to exercise the data subject's right of access, right to rectification, restriction of processing, erasure (**"right to be forgotten"**), data portability, objection to the processing, or its right not to be subject to an automated individual decision making (**"Data Subject Request"**). Taking into account the nature of the processing, Zscaler shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Legislation. In addition, to the extent Customer, in its use of the Products, does not have the ability to address a Data Subject Request, Zscaler shall upon Customer's request provide commercially reasonable assistance to Customer in responding to such Data Subject Request, to the extent Zscaler is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any reasonable costs that Zscaler may incur in providing such assistance.

4. DATA TRANSFER REQUIREMENTS

The Standard Contractual Clauses will apply to all processing of Personal Data by Zscaler where the Personal Data is transferred from the EEA to outside the EEA, from a Data Exporter acting as Controller to a Data Importer acting as Processor, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Legislation), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, except that the Privacy Shield (as described in Section 9 of this DPA) will apply to all processing of Personal Data by Zscaler where the Personal Data is transferred from the EEA or Switzerland to the United States.

5. SUB-PROCESSORS

5.1 Sub-processing. The parties acknowledge that applicable Data Protection Legislation permits a Controller to provide the Processor a general written authorization to sub-processing. Accordingly, Customer provides a general authorization to Zscaler, pursuant to Clause 11 of the Standard Contractual Clauses and Article 28(2) and (4) of the GDPR, to engage sub-processors ("**Sub-processors**") to enable Zscaler to fulfill its contractual obligations under the Agreement and to provide support services on Zscaler's behalf, subject to compliance with the requirements in this Section.

For purposes of clarity, Sub-processors may include Zscaler affiliates. The parties agree that copies of any Sub-processor agreements that are provided by Zscaler to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Zscaler beforehand. Such copies will be provided by Zscaler, in a manner to be determined in its discretion, upon written request by Customer.

5.2 Sub-processor Agreements. Zscaler will: (a) enter into a written agreement in accordance with the requirements of Article 28(4) of the GDPR with any Sub-processor that will process Personal Data; (b) ensure that each such written agreement contains terms that are no less protective of Personal Data than those contained in this DPA; and (c) be liable for the acts and omissions of its Sub-processors to the same extent that Zscaler would be liable if it were performing the services of each of those Sub-processors directly under the terms of this DPA.

5.3 Sub-processor List. Information regarding Zscaler's current Sub-processors, including their location and services provided (the "**Sub-processor List**"), can be found at the following link: https://www.zscaler.com/legal/subprocessors. This Sub-processor list may be updated by Zscaler from time to time in accordance with subsection 5.4.

5.4 Changes to Sub-processor List. Zscaler will provide Customer with advance notice before a new Sub-processor processes any Personal Data. Customer may object to the new Sub-processor within fifteen (15) days of such notice on reasonable grounds relating to the protection of Personal Data by following the instructions set forth in the Sub-processor List. In such case, Zscaler shall have the right to cure the objection through one of the following options : (1) Zscaler will cancel its plans to use the Sub-processor with regards to processing Personal Data or will offer an alternative to provide the Products without such Sub-processor; or (2) Zscaler will take the corrective steps requested by Customer in its objection notice and proceed to use the Sub-processor; or (3) Zscaler may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the Product that would involve the use of such Sub-processor. If none of the above options are commercially feasible, in Zscaler's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days after Zscaler's receipt of Customer's objection notice, then either party may terminate the Agreement for cause without a refund of any pre-paid fees. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Sub-processor.

6. SECURITY MEASURES

Zscaler implements the physical, technical, and organizational security measures set forth in Exhibit C of this DPA with respect to the Personal Data ("Security Measures") to ensure a level of security appropriate to the risk in accordance with the standards of Article 32 of the GDPR. Zscaler is certified under ISO 27001 and System and Organization Controls (SOC) 2, Type II standards and is audited annually by a third party to ensure its ongoing compliance with these certifications. Zscaler regularly tests, assesses and evaluates the effectiveness of the Security Measures. Upon written request, and subject to appropriate confidentiality protections being in place, Zscaler agrees to provide Customer with a copy of its most recent ISO 27001 certificate and/or SOC 2, Type II report. Zscaler will not materially decrease the overall security of the Products during the term of the Agreement. Zscaler will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance.

7. SECURITY INCIDENT NOTIFICATION

The parties agree that Zscaler's obligations under Clause 5(d)(ii) of the Standard Contractual Clauses and under Article 28(3)(f) of the GDPR with respect to Customer's compliance with Articles 33 and 34 of the GDPR will be carried out in accordance with this Section 7. If Zscaler becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer's Personal Data, including any "personal data breach" as defined in the GDPR ("**Security Incident**"), Zscaler will notify Customer without undue delay after becoming aware of and confirming the Security Incident. Zscaler will take reasonable steps to: (a) identify the cause of the Security Incident; and (b) take any actions necessary and reasonable to remediate the cause of such Security Incident to the extent such remediation is within Zscaler's reasonable control. Zscaler will also reasonably cooperate with Customer with respect to any investigations and with preparing potentially required notices, and provide any information reasonably requested by Customer in relation to the Security Incident.

8. AUDITS

The parties agree that the audits described in Clauses 5(f) and 12(2) of the Standard Contractual Clauses and Article 28(h) of the GDPR (the "**Audit**") will be carried out in accordance with the following conditions:

(a) An Audit of its data processing facilities may be performed no more than once per year during Zscaler's normal business hours, unless (i) otherwise agreed to in writing by Customer and Zscaler, (ii) required by a regulator or under applicable Data Protection Legislation, or (iii) there is a Security Incident;

(b) Customer will provide Zscaler with at least thirty (30) days' prior written notice of an Audit, which may be conducted by Customer or an independent auditor appointed by Customer that is not a competitor of Zscaler ("**Auditor**");

(c) The Auditors will conduct Audits subject to any appropriate and reasonable confidentiality restrictions requested by Zscaler;

(d) The scope of an Audit will be limited to Zscaler systems, processes and documentation relevant to the processing and protection of Personal Data;

(e) Prior to the start of an Audit, the parties will agree to reasonable scope, time, duration, place and conditions for the Audit, and a reasonable reimbursement rate payable by Customer to Zscaler for Zscaler's Audit expenses;

(f) If available, Zscaler will provide an Auditor, upon request, with any third-party certifications pertinent to Zscaler's compliance with its obligations under this DPA (for example, ISO 27001 and/or SOC 2, Type II); and

(g) Customer will promptly notify and provide Zscaler with full details regarding any perceived non-compliance or security concerns discovered during the course of an Audit.

9. PRIVACY SHIELD

Zscaler has self-certified to and complies with the EU-U.S. and the Swiss-U.S. Privacy Shield as set forth by the U.S. Department of Commerce and the European Commission and Swiss Administration regarding the collection, use and retention of Personal Data transferred from the EEA and Switzerland, respectively, to the United States. Zscaler's GDPR and Privacy Shield Policy is available at https://www.zscaler.com/gdpr-and-privacy-shield-policy. As required under the Privacy Shield certifications, Zscaler agrees:

(a) To process EEA and Swiss Personal Data only for the limited and specified purposes consistent with the consent provided by the Customer;
(b) To provide at least the same level of protection for EEA and Swiss Personal Data as is required by the Privacy Shield;
(c) To notify Customer promptly if Zscaler makes a determination that it can no longer meet Customer's obligation to protect EEA or Swiss Personal Data as required by the Privacy Shield;
(d) Upon making the determination specified in subsection (c) above, to cease processing EEA or Swiss Personal Data or take other reasonable and appropriate steps to remediate unauthorized processing; and
(e) To authorize Customer to provide a summary or a copy of the relevant privacy provisions of the Agreement and this DPA to the U.S. Department of Commerce upon written request.

10. GENERAL

10.1 Term and Termination. This DPA will remain in force until (i) it is replaced or repealed by mutual agreement of Customer and Zscaler, or (ii) the Agreement is terminated or expires.

10.2 Liability. Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Agreement. Zscaler's liability to Customer under this DPA will be limited to the same extent as Zscaler's liability to Customer under the Agreement. For the avoidance of doubt, the total liability of Zscaler and its affiliates for all claims by Customer arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA. In no event will either party limit its liability with respect to any data subject rights under the Standard Contractual Clauses or the GDPR.

10.3 Governing Law. Without prejudice to clause 7 (Mediation and Jurisdiction) and clause 9 (Governing Law) of the Standard Contractual Clauses: (i) the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
(ii) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

10.4 Changes in Data Protection Legislation. Zscaler and Customer may, by written notice to the other party, propose to amend the Standard Contractual Clauses or this DPA as required as a result of any change in, or decision of a competent authority under, applicable Data Protection Legislation, to allow processing of Personal Data to be done (or continue to be done) without breach of such Data Protection Legislation. The parties agree to make any such required amendment, which shall be in writing and signed by both parties.

10.5 Counterparts. This DPA may be executed in any number of counterparts, each of which will be deemed to be an original and all of which taken together will comprise a single instrument. This DPA may be delivered by facsimile or electronic document format (e.g. PDF), and facsimile or electronic copies of executed signature pages will be binding as originals.

10.6 Entire Agreement. This DPA, together with the Agreement, constitutes the entire agreement between the parties and supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. In case of conflict or inconsistency between this DPA, the Agreement, and the Standard Contractual Clauses, the following order of precedence shall govern to the extent of the conflict or inconsistency: (i) the Standard Contractual Clauses; (ii) this DPA; and (iii) the Agreement.

10.7 Severability. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed and the remainder of terms will remain in full effect.

[SIGNATURE PAGE TO FOLLOW]

By signing below, you represent and warrant that you are an authorized representative with authority to sign this DPA.

CUSTOMER

Signature: ________________________________

Printed Name: ____________________________

Title: ____________________________________

Date Signed: ______________________________

ZSCALER, INC.

Signature: ____ DocuSigned by: Jugnu Bhatia 23126CBC57A6432... __________

Printed Name: Jugnu Bhatia

Title: Chief Accounting Officer

Date Signed: May 25, 2018

Exhibit A

<table>
<tr><td><b>Subject Matter of Processing</b></td><td>The subject matter of Processing is the Products pursuant to the Agreement.</td></tr>
<tr><td><b>Duration of Processing</b></td><td>The Processing will continue until the expiration or termination of the Agreement.</td></tr>
<tr><td><b>Categories of Data Subjects</b></td><td>Employees and other authorized users of Customer.</td></tr>
<tr><td><b>Nature and Purpose of Processing</b></td><td>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.</td></tr>
<tr><td><b>Types of Personal Data</b></td><td>Personal Data provided by Customer to facilitate Zscaler’s provision of the Products to Customer, including but not limited to:
<table>
<tr><th>Type of Personal Data</th><th>Summary</th><th>Controls</th></tr>
<tr><td>User IDs</td><td>Fetched from Customer’s corporate directory and identifying the user, group and department for policy enforcement and reporting</td><td>• Customer can opt-in for user level tracking
• User names can be tokenized and obfuscated</td></tr>
<tr><td>Customer Logs</td><td>For all Internet based transactions processed by Zscaler for Customer, identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.)</td><td>• Transaction content is not written to disk
• All enforcement done in-memory</td></tr>
<tr><td>Public IP Addresses</td><td>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</td><td>• Required only if static GRE tunnels are used for forwarding traffic
• ZApp and VPN based traffic forwarding do not require public IP information</td></tr>
<tr><td>SSL Certificates and Keys</td><td>To allow Zscaler to intercept SSL encrypted transactions in order to provide security and policy enforcement</td><td>• Customer can opt-in for SSL interception
• Customer can use their own root certificate authorities
• All key information is strongly encrypted (audited and compliant with stringent standards)</td></tr>
</table>
</td></tr>
</table>

Exhibit B
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC and Article 44 of the Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of data exporting organization:	
Address:	
Tel.:	
Fax:	
Email:	

The data exporting organisation identified in the table above
(the "**data exporter**")

- And –

Name of data importing organization:	Zscaler, Inc.
Address:	110 Rose Orchard Way, San Jose, CA 95134 USA
Tel.:	(408) 533-0288
Fax:	(408) 868-4089
Email:	privacy@zscaler.com

Zscaler, Inc.
(the "**data importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Signature: __________________________________ (affix stamp of organisation below, if any)

Printed Name: ______________________________

Title: _______________________________________

Data Exporter Name: ________________________

Date Signed: ________________________________

Other information necessary in order for the contract to be binding (if any): _______________________

On behalf of the data importer:

Signature: ___ DocuSigned by: Jugnu Bhatia 23126CBC57A6432... _________

Printed Name: Jugnu Bhatia

Title: Chief Accounting Officer

Data Importer Name: Zscaler, Inc.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Capitalized terms used in this Appendix which are otherwise undefined in these Clauses have the meanings given to them in the DPA to which these Clauses are attached.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

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) and Switzerland that have ordered or subscribed to Products through one or more Agreement(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Zscaler, Inc. is a provider of cloud-based Internet security solutions which processes Personal Data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees and other authorized users of the Data Exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Personal Data provided by the Data Exporter to facilitate the Data Importer's provision of Products to the Data Exporter, including but not limited to:

Type of Personal Data	Summary	Controls
User IDs	Fetched from Customer's corporate directory and identifying the user, group and department for policy enforcement and reporting	• Customer can opt-in for user level tracking • User names can be tokenized and obfuscated
Customer Logs	For all Internet based transactions processed by Zscaler for Customer, identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.)	• Transaction content is not written to disk • All enforcement done in-memory
Public 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	• Required only if static GRE tunnels are used for forwarding traffic • ZApp and VPN based traffic forwarding do not require public IP information
SSL Certificates and Keys	To allow Zscaler to intercept SSL encrypted transactions in order to provide security and policy enforcement	• Customer can opt-in for SSL interception • Customer can use their own root certificate authorities • All key information is strongly encrypted (audited and compliant with stringent standards)

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

None.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing of the personal data by Data Importer shall be to enable (1) the performance 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.

On behalf of the data exporter:

Signature: ________________________________ (affix stamp of organisation below, if any)

Printed Name: ____________________________

Title: ____________________________________

Data Exporter Name: _______________________

Date Signed: ______________________________

Other information necessary in order for the contract to be binding (if any): ______________________

On behalf of the data importer:

Signature: ___ DocuSigned by: Jugnu Bhatia 23126CBC57A6432... ________

Printed Name: Jugnu Bhatia

Title: Chief Accounting Officer

Data Importer Name: Zscaler, Inc.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

*The data importer will maintain appropriate physical, technical, and organizational safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of Personal Data provided to it by the data exporter in connection with the Clauses. Such Security Safeguards are described in the DPA to which these Clauses are attached.*

On behalf of the data exporter:

Signature: ________________________________ (affix stamp of organisation below, if any)

Printed Name: ____________________________

Title: ____________________________________

Data Exporter Name: ______________________

Date Signed: ______________________________

Other information necessary in order for the contract to be binding (if any): ______________________

On behalf of the data importer:

DocuSigned by:

Signature: ___ Jugnu Bhatia _______

23126CBC57A6432...

Printed Name: Jugnu Bhatia

Title: Chief Accounting Officer

Data Importer Name: Zscaler, Inc.

Exhibit C
Zscaler Security Measures

1. Preventing unauthorized persons from gaining access to data processing systems (physical access control)

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

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

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

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

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

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

2. Preventing personal data processing systems from being used without authorization (logical access control)

(a) Zscaler maintains a separate authentication system for accessing production systems and access to production systems is controlled and maintained by Zscaler.

(b) Access is role based and granted after demonstrated business need and must be approved by the employee´s manager and the Operations team.

(c) Account Login parameters follow these rules:
i. Accounts are not shared
ii. Accounts are locked after 3 failed log-in attempts

(d) Strong Password configurations adhere to the following rules:
i. Must be at least 8 characters in length
ii. Has at least one numerical character
iii. Has at least one lower case character
iv. Has at least one upper case character
v. May not include part of the login username
vi. Must be different than the previous 10 passwords

3. Ensuring that persons entitled to use a data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control)

(a) For production access, Zscaler maintains segmented development and production environments, using technical and physical controls to limit network and application-level access to live systems. Employees have specific authorizations to access development and production systems.

(b) Zscaler utilizes a centralized log monitoring solution in combination with a SIEM to aggregate and correlate logged events.

(c) In order to protect against unauthorized access and modification, Zscaler captures network logs, OS-related logs, and intrusion detections.

(d) Zscaler identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never exceeded.

4. Ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control)

(a) All management connections to the servers occur over encrypted Secure Shell (SSH), Secure Sockets Layer (SSL), 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.

5. Ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from personal data processing (entry control)

(a) Zscaler utilizes a centralized log monitoring solution to aggregate and correlate logged events into a SIEM.

(b) In order to protect against unauthorized access and modification, Zscaler captures network logs, OS-related logs, and intrusion detections. Zscaler identifies, periodically reviews, and as needed, expands storage capacity to ensure that sufficient capacity always exists and is never exceeded.

(c) Application audit logs are available for customers from the application's interface.

6. Ensuring that Personal Data is processed solely in accordance with the Instructions (control of Instructions)

(a) Anyone who is found to violate Zscaler's Code of Conduct and/or other Zscaler policies may be subject to disciplinary action including termination of employment or contract.

(b) Employees are required to sign a Non-Disclosure Agreement or other confidentiality agreement upon employment.

(c) Zscaler conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services.

(d) Zscaler maintains segmented development and production environments for all Zscaler Services, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

(e) Zscaler obtains background check reports for employment purposes. The specific nature and scope of the report that Zscaler typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law.

7. Ensuring that Personal Data is protected against accidental destruction or loss (availability control)

(a) Zscaler monitors all productions systems 24/7 to ensure the integrity of the data.

(b) Zscaler uses multiple layers of network and host-based security.

(c) Zscaler maintains disaster recovery processes to allow for continuation of data collection and to provide an effective and accurate recovery.

8. Ensuring that Personal Data collected for different purposes can be processed separately (separation control)

(a) Data is separated based upon Zscaler product and how it is collected. Zscaler is a multi-tenant architecture with Customer Data logically segregated. The only access to these servers and databases is via secure access by the application or via jump servers with access restricted to authorized operations personnel via multi-factor authentication.

(b) Zscaler maintains testing environments separate from production environments to avoid use of Customer Data in testing environments.