ARYAKA NETWORKS, INC.

MASTER SUBSCRIPTION AGREEMENT (MSA)

(Enterprise Flex)

This Master Subscription Agreement ("Agreement") is made and entered into effective ________________, and if no date is filled in, then the Effective date shall be the date of last signature ("Effective Date"), between ________________________________, with offices at ____ ("Customer"), and Aryaka Networks, Inc., having its place of business at 1800 Gateway Drive, San Mateo, California 94404 ("Aryaka"), which are hereinafter referred to collectively as the "Parties" and individually as the "Party".

In consideration of the mutual covenants herein contained, the Parties hereto agree as follows:

1. DEFINITIONS

As used in this Agreement:

(a) "24/7" means twenty-four (24) hours per day, seven (7) days per week.

(b) "Affiliate" of an entity means any other entity, which directly or indirectly controls, is controlled by, or is under common control with such entity. The term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract or otherwise.

(c) "ANAP" means the Aryaka Network Access Point (ANAP), a device that provides bandwidth optimization, SD-WAN capabilities, and application acceleration over a WAN link that is connected to an Aryaka Network point of presence (AN POP or Aryaka POP).

(d) "Aryaka Equipment" means any hardware and equipment provided by Aryaka to Customer, which enables Customer to access the Aryaka Network, including but not limited to the ANAP-1000, ANAP-1500, ANAP-2000, ANAP-2500, ANAP-3000, including ANAPs with "High Availability" (HA), and an Aryaka Router, if provided by Aryaka as part of the access mechanism to the Aryaka Network.

(e) "Aryaka Network" means Aryaka's geographically distributed network of proprietary servers and software.

(f) "Bursting" allows Customer to use bandwidth greater than the purchased bandwidth capacity for the purpose of addressing Customer's seasonal traffic demands.

(g) "Confidential Information" has the meaning set forth in Section 8.1 below.

(h) "Deployment Window" means a predefined window for provisioning timeframe, as mutually agreed to by Aryaka and Customer, and set forth on the Order Form.

(i) “Disclosing Party” has the meaning set forth in Section 8.1 below.

(j) “Force Majeure” means circumstances beyond Aryaka’s reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (excluding those involving Aryaka employees).

(k) “Initial Term” of this Agreement has the meaning set forth in Section 12.1 below.

(l) “Last Mile Circuit” means the physical link (wired or wireless) that is used to connect Customer’s Premise to the closest Aryaka POP. The physical link may be a direct Layer-2 connection or an Internet Circuit. The type of the Last Mile Circuit will be specified in the Order Form.

(m) “Link Monitoring” means the monitoring by Aryaka of Customer’s Last Mile Circuit link to be conducted on a 24x7x365 basis, including reports and support as specified in Exhibit C to this Agreement. Link Monitoring shall be included with the Last Mile Circuit if and as specified in the Order Form together with a letter of authorization from Customer.

(n) “Malicious Code” means viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs.

(o) “Marks” means all registered and common law trademarks, trademark registrations, service marks, trade names, copyrights, licenses, designs, logos, marketing and promotion materials and all intellectual property rights relating thereto, and any similar rights owned, used by or licensed to a party, and any applications currently pending therefor.

(p) “NOC” means network operating center.

(q) “Optimized Capacity” means subscribed bandwidth for all the sites per region.

(r) “Order Form” means the ordering documents for purchases hereunder, including addenda thereto, that are entered into between the Parties from time to time. Each Order Form issued under this Agreement shall become effective when executed by both Parties. Order Forms shall be deemed incorporated into this Agreement by reference and shall list quantity Unit Price, UOM, and Deployment Window. If Last Mile Circuits are ordered, they will be set forth on a separate and distinct Order Form.

(s) “Oversubscription” means a Customer has a temporary need to go beyond its subscription units as set forth in the Order Form. Units may be bandwidth, sites, Last Mile Management, and/or High Availability ANAPs.

(t) “Provision” means that connectivity was successfully brought up between Customer’s site and POP for routing the traffic.

(u) “Receiving Party” has the meaning set forth in Section 8.1 below.

(v) “RFS Date” means the date in which a last mile link has been provisioned.

(w) “SD-WAN” means software-defined wide area network.

(x) "Services" means access to the Aryaka services listed in Section 2 below, including MyAryaka (Aryaka's customer portal), Aryaka Equipment (including, but not limited to, ANAP-1000, ANAP-1500, ANAP-2000, ANAP-2500, or ANAP-3000) with HA, the Aryaka Router (if provided by Aryaka as part of the access mechanism to the Aryaka Network), Link management and Last Mile Circuits and any and all Aryaka downloaded materials (including but not limited to Java Applets, soft-ANAP, and browser/User Interface components), user guides, code, user interface passwords, accessories and other documents, that are purchased by Customer or its Affiliates under a fully executed Order Form, including associated offline components.

(y) "Service Credit" has the meaning set forth in Exhibit A.

(z) "Subscription Term" means the term for the purchased Services, as set forth in the Order Form, which commences upon the first day after the Deployment Window terminates.

(aa) "UOM" means unit of measurement.

(bb) "Unit Price" is the per unit price for bandwidth, site licensing, HA ANAPs, and Links.

(cc) "Users" means individuals who are authorized by Customer to use the Services, or who have been supplied user identifications and passwords by Customer (or by Aryaka at Customer's request). Users may include but are not limited to Customer's or its Affiliates' employees, consultants, contractors and agents; or third parties with whom Customer transacts business or that use its corporate Wide Area Network.

(dd) "Taxes" has the meaning set forth in Section 6.6 below.

(ee) "Customer Data" means all electronic data or information submitted by Customer to the Aryaka Network.

2. SERVICES DESCRIPTION SUMMARY

2.1 "Smart Access" means usage of Aryaka's global network for accelerating remote-access virtual private network (VPN) connectivity with cloud-based management and visibility using MyAryaka.

2.2 "SmartCDN" means usage of either the Web Application Delivery as-a-Service (WADS) or IP Application Delivery-as-a-Service (IADS) which are used for accelerating any web or IP-based public applications over Aryaka's global network using capabilities such as, for example, TCP optimization, caching and compression with cloud-based management and visibility using MyAryaka.

2.3 "SmartCONNECT means Aryaka's global SD-WAN service that combines a global optimized private network, SD-WAN functionality at the edge, L3 VPN connectivity, cloud connectivity, wan optimization capabilities including compression, data deduplication, application acceleration proxies, and SmartLink with cloud- based management and visibility using MyAryaka.

3. SERVICES, RENEWALS, END OF LIFE

3.1 Aryaka shall make the Services available to Customer pursuant to this Agreement and the relevant Order Form during a subscription term which is set forth in each Order Form “Subscription Term”. The Order Form shall automatically renew for additional periods equal to the initial term set forth in the Order Form, unless either party gives the other written notice of non-renewal at least ninety (90) days before the end of the relevant Subscription Term.

3.2 The aggregate pricing during any such renewal Subscription Term shall be the same as that during the prior Subscription Term unless Aryaka has given Customer written notice of a pricing increase at least thirty (30) days before the end of such prior term.

3.3 Customer agrees that its purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by Aryaka regarding future functionality or features.

3.4 It is understood that Aryaka may, in its discretion, at certain times elect to discontinue production, distribution and support of elements or versions of the Aryaka Services, and thereby designate such elements or versions as end of life (“EOL”). In the event that Aryaka elects to announce EOL for any such elements or versions, Aryaka will provide three (3) months prior written notice, which may be by direct notice or posting on Aryaka’s website. Aryaka’s resellers or other third-party providers will have a period of three (3) months after receipt of such notice to upgrade Customers to the last commercially available (non-EOL) version of the Services. During the 3-month notice period (from either Aryaka or Aryaka partner) Customers may continue exercising all of the rights set forth in this Agreement with respect to such EOL Services. Aryaka (either directly or through a third party contractor selected by Aryaka) will continue providing support for the last commercially available version of such EOL Services in accordance with Aryaka’s applicable support terms for a period of one (1) year from the announced EOL date or upon termination of the related SOF (whichever is earlier), provided that Customers continue to pay applicable license and support fees, if any, during the wind down period for the support described above.

4. USE OF THE SERVICES

This Section sets forth the responsibilities of each Party with respect to the Services purchased by Customer together with any terms and conditions that apply to a particular Aryaka Service:

4.1 Aryaka’s Responsibilities. Aryaka shall provide to Customer:

(a) NETWORK AVAILABILITY AND OPERATIONS. Aryaka shall provision, maintain and operate on a 24/7 basis, the Aryaka Network, all network software and peripherals, and Aryaka Network connectivity, as necessary to perform the Services in accordance with this Agreement except for: (i) planned downtime (of which Aryaka shall give at least forty-eight (48) hours prior written notice via email to Customer’s registered technical contacts and which Aryaka shall schedule, to the extent practicable, during the weekend hours from 11:59PM UTC Friday to 11:59PM UTC Sunday or (ii) any unavailability caused by an act of Force Majeure. Aryaka shall staff “NOC” 24/7.

(b) NETWORK SECURITY. Subject to Section 8.3 below, Aryaka shall keep in place with respect to the Aryaka Network and the NOC network security as reasonably necessary to monitor and protect against unauthorized access to Customer Data while on or within the Aryaka Network.

(c) CAPACITY AND RELIABILITY. Aryaka shall maintain adequate capacity on its network during the Subscription Term as necessary to meet Customer's committed network usage set forth in the Order Form. Aryaka's network will remain distributed geographically and Aryaka will keep in place distributed network connections.

(d) ADDITIONAL SERVICES. Aryaka shall provide Customer with such installation, support, training or other additional services as may be specified in the Order Form or as may be requested by Customer, from time to time, during the term and as set forth in a separate schedule or addendum agreed to and executed by both Parties. Standard support for the Services is provided at no additional charge. Aryaka will make the Services available to Customer according to the terms of the Service Level Agreement, attached hereto as Exhibit A, and Aryaka will provide the Services in accordance with applicable laws and government regulations.

4.2 Customer's Responsibilities.

(a) Customer shall (i) be responsible for compliance with this Agreement, (ii) be solely responsible for the accuracy, quality, integrity and legality of Customer's Data and of the means by which Customer acquired its Customer Data, (iii) use commercially reasonable efforts to prevent unauthorized access to or use of the Services and Aryaka Equipment, and notify Aryaka promptly of any such unauthorized access or use, (iv) return Aryaka Equipment to Aryaka , at Aryaka's expense, within sixty (60) business days after the termination of this Agreement pursuant to shipping instructions to be provided by Aryaka, and (v) use the Services only in accordance with applicable laws and government regulations. Customer will be charged an amount of $1,000 if Aryaka Equipment is not returned to Aryaka within sixty (60) business days from the termination of the Services.

(b) Customer shall not (i) make the Services available to anyone other than Users, (ii) sell, resell, rent or lease the Services (however, sales or transfers for value to Customer's Affiliates is not prohibited), or provide Services through a service bureau or the like, (iii) use the Services to store, transmit, use or access infringing, libelous, or otherwise unlawful or tortious material, or to store, transmit, use or access material in violation of third-party privacy rights, (iv) use the Services to store, transmit, use or access Malicious Code, (v) interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, (vi) attempt to gain unauthorized access to the Services or their related systems or networks (vii) publish or distribute information about Aryaka's benchmarks, prices, or other data collected outside Customer's organization without express prior written permission from Aryaka, or (viii) connect or otherwise use the Aryaka Network without also using the Services and the Aryaka Equipment.

4.3 Terms of use for SmartConnect Enterprise Flex Services, when such Services are purchased by Customer:

4.3.1 Customer's purchase of the optimized capacity will be on a per region basis and can be allocated only among the sites in a particular region.

4.3.2 The sites can consume capacity in a region subject to availability of the site license required for consuming that capacity.

4.3.3 Customer may add sites, provided that Customer does not exceed the maximum number of site licenses purchased for that capacity tier.

4.3.4 Site moves, bandwidth reallocation and add-on relocations are limited to no more than two (2) changes per site in any given month.

4.3.5 Customer cannot exceed the purchased aggregate SBW, number of site licenses and/or service limits as set forth in the Order Form. Aryaka shall notify Customer, in writing if such event occurs, and the Parties have to agree to enter into an amended order form.

4.4 Terms for use of Smart Access Services, when such Services are purchased by Customer:

4.4.1 Aryaka reserves the right to limit the total number of User sessions if and when the number of simultaneous User sessions exceeds the number of sessions designated in the particular "User Pack" purchased by Customer.

4.4.2 Aryaka reserves the right to limit the maximum network data transfer rates that can be achieved over the Aryaka Network if and when the aggregate data usage exceeds the data usage allocation schedule specified in Table 1 of Exhibit D to this Agreement

4.4.3 It is understood and agreed that the Smart Access Services will be delivered by Aryaka only from the list of POPs set forth in Table 2 of Exhibit D to this Agreement.

4.5 Terms of use of SmartCDN Services, when such Services are purchased by Customer:

4.5.1 Aryaka reserves the right to choose the edge POPs and Origin POPs to deliver the Services on its global network.

4.5.2 Aryaka reserves the right to limit the maximum data transfer rates achieved over the Aryaka network based on the aggregate commits purchased.

4.6 Terms of use of SmartConnect Services, when such Services are purchased by Customer:

4.6.1 Aryaka reserves the right to choose the ANAP device type based on Customer subscription and capabilities desired.

4.6.2 Aryaka reserves the right to choose and or move sites to a POP for connecting a site to its network based on providing optimal service delivery.

4.7 Terms for use of Last Mile Circuits, when such Services are purchased by Customer:

4.7.1 The initial term for the Last Mile Circuit will be as specified in the Order Form. At the end of the initial term, this Agreement (with respect to the Last Mile Circuit terms) shall automatically renew for additional periods equal to one (1) year ("Renewal Period"), unless either Party gives the other written notice of nonrenewal at least ninety (90) days before the end of the Initial Term or any Renewal Period.

4.7.2 If the Customer terminates the Last Mile Circuit before the end of the initial term, as set forth in the Order Form for, or any Renewal Period, in addition to all early termination fees to be remitted to Aryaka, Customer will pay to Aryaka one hundred percent (100%) of the costs and expenses Aryaka incurs with the third-party service providers for early termination of the Last Mile Circuit.

4.7.3 Upon completion of the site survey of Customer's premises, the particular third-party service provider will advise Aryaka if there will be additional charges for providing service above the charges previously quoted to the Customer. In any such case, Aryaka will propose the associated cost changes to the Customer. The Customer has the right to reject the proposed charges within five (5) days of receipt of the proposal. If the Customer rejects the proposal, then the original order for the Last Mile Circuit will be automatically cancelled with no early termination fees. The proposal will be considered accepted if not so rejected by the Customer within the 5-day period.

4.7.4 Upon completion of the site survey of Customer's premises, the third-party service provider will advise Aryaka if there will be "no service available" or equivalent, or if a redesign is required. Aryaka will then undertake to locate an alternate provider for the Last Mile Circuit. Aryaka will propose the alternate Last Mile Circuit together with the associated cost changes to the Customer. The Customer has the right to reject the proposed alternate within five (5) days of receipt of the proposal. If the Customer rejects the proposal, then the original order for the Last Mile Circuit will be automatically cancelled with no early termination fees. The proposal will be considered accepted if not so rejected by the Customer within the 5-day period.

4.7.5 All start or completion dates provided at the time of signing the Last Mile Circuit order are advisory and non-binding. The final service activation date will be provided after the third-party service provider has completed the site survey of Customer's premises.

4.7.6 Aryaka will not be responsible for delays in (i) completion of internal wiring, (ii) the Customer responding to requests for additional information, or (iii) gaining access to the Customer's premises to have the service installed.

4.7.7 All Last Mile Circuit quotes are based on providing connectivity to the Minimum Point Of Entrance (MPOE). All wiring from the MPOE to Customer's facilities or equipment is the responsibility of Customer. Upon request from Customer, Aryaka will advise whether it has the capability to provide the internal wiring, together with an estimate of the associated extra cost.

4.7.8 Notwithstanding Subsection 4.1(d) above, for all Last Mile Circuits, the Mean Time to Repair and the Service Availability Service Level Agreement will, as provided by (or limited by, as the case may be), the particular third-party service provider, depend upon the type of circuit that is ordered. Aryaka will pass through to Customer any service credits that become due to the Customer from the third-party service provider for violations of the service provider's applicable service level agreement.

4.8 Terms for Bursting, when such Services are purchased by Customer:

4.8.1 Bursting is applicable only for bandwidth and is calculated on a monthly basis, for each region, as the amount by which the actual usage exceeds the subscribed bandwidth. The usage for a region is calculated as the sum of the 99th percentile for individual sites in that region.

4.8.2 Customers will pay an additional usage fee, as set forth in the Order Form, for the extra bandwidth used.

4.8.3 A site may burst up to a maximum of 1.5 times it SBW.

4.8.4 The burst rate is limited to a maximum of 100 Mbps.

4.9 Terms for Oversubscription, when such Services are purchased by Customer:

4.9.1 Oversubscription is applicable for bandwidth, sites, Last Mile Management and HA ANAPs.

5. PUBLICITY AND TRADEMARKS. Subject to Customer's logo and trademark usage guide, Customer hereby permits Aryaka to identify Customer as a customer of Aryaka and to display Customer's logo in connection with identifying Customer as a customer of Aryaka. Subject to prior approval of both Parties, within six (6) months of the date of this Agreement, Customer agrees to participate in a joint press release with Aryaka announcing Customer's use of Aryaka's Services, subject to each party's logo and trademark usage guide. Customer may enter into a separate agreement with Aryaka with respect to collaborating and engaging in mutually beneficial marketing activities, subject to the terms and conditions of a co-marketing agreement.

6. FEES AND PAYMENT FOR SERVICES

6.1 Fees. In consideration of all Services provided in accordance with the terms hereof and the applicable Order Form, Customer shall pay all fees specified in all Order Forms. Except as otherwise specified herein or in an Order Form, (a) fees are quoted and payable in United States dollars (b) fees are based on Services purchased and not actual usage, (c) payment obligations are non-cancelable and fees paid are non-refundable (except in case of a material breach of Aryaka).

6.2 Invoicing and Payment. Customer will provide Aryaka with valid and updated credit card information, or with a valid purchase order, or alternative document reasonably acceptable to Aryaka. If Customer provides credit card information to Aryaka, Customer authorizes Aryaka to charge such credit card for all Services listed in the Order Form for the initial subscription term and any renewal subscription terms as set forth in Section 12.1. During the Deployment Window, Aryaka will commence invoicing Customer on a monthly basis, in arrears, for the sites and bandwidth that are Provisioned as of that month. Once the Deployment Window has been completed, Aryaka will invoice Customer quarterly in advance for 100% of the amount set forth in the Order Form. Unless otherwise stated in the Order Form, invoiced charges are due net thirty (30) days from the invoice date. For Last Mile Circuits, if purchased, Aryaka will invoice Customer based on RFS Date and pursuant to terms set forth in the Last Mile Circuits Order Form. For Bursting and Oversubscription, Aryaka will invoice Customer monthly, in arrears during the full term of the Order Form, including period after the Deployment Window. Customer is responsible for keeping Aryaka apprised thereof of any change in billing and contact information.

6.3 Overdue Charges. Notwithstanding Section 6.5 below (Payment Disputes), if any charges are not received from Customer by the due date, then at Aryaka's discretion, (a) such undisputed charges may accrue late interest at the rate of one and one-half percent (1.5%) of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, from the date such payment was due until the date paid, (b) Aryaka may condition future subscription renewals and Order Forms on payment terms shorter than those specified in Section 6.2 (Invoicing and Payment), or (c) both (a) and (b).

6.4 Suspension of Service and Acceleration. Notwithstanding Section 6.5 below, if any undisputed amount owing by Customer under this or any other agreement for Aryaka's Services is more than thirty (30) days overdue (or ten (10) or more days overdue in the case of amounts Customer has authorized Aryaka to charge to Customer's credit card), Aryaka may, without limiting Aryaka's other rights and remedies, accelerate Customer's unpaid fee obligations under such agreements so that all such obligations become immediately due and payable, and suspend Aryaka's Services to Customer until such amounts are paid in full. Aryaka may require immediate return of Aryaka Equipment upon such suspension of Service.

6.5 Payment Disputes. Aryaka shall not exercise Aryaka's rights under Section 6.3 (Overdue Charges) or 6.4 (Suspension of Service and Acceleration) if the applicable charges are under reasonable and good faith dispute and Customer is cooperating diligently to resolve the dispute.

6.6 Taxes. Unless otherwise stated, Aryaka's fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including but not limited to value-added, sales, use or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with Customer's purchases hereunder. If Aryaka has the legal obligation to pay or collect Taxes for which Customer is responsible under this paragraph, the appropriate amount shall be invoiced to and paid by Customer, unless Customer provides Aryaka with a valid tax exemption certificate authorized by the appropriate taxing authority. However, Aryaka is responsible for taxes assessable based on Aryaka's income, property and employees. All amounts payable to Aryaka must be paid free of and without any rights of counterclaim or set off, and without deduction or withholding for taxes or on any other ground whatsoever. If any such deduction or withholding is required by law or applicable taxing authority, Customer shall: (a) provide such evidence of the relevant deduction or withholding as Aryaka may reasonably require; and (b) pay to Aryaka an aggregate amount to ensure that, after the deduction or withholding has been made, Aryaka will have received a sum equal to the amount that Aryaka would otherwise have received in the absence of the deduction or withholding.

7. PROPRIETARY RIGHTS

7.1 Reservation of Rights. Subject to the limited rights expressly granted hereunder, Aryaka reserves all rights, title and interest in and to the Services, including all related intellectual property rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

7.2 Restrictions. Customer shall not (a) permit any third party to access the Services except as permitted herein or in an Order Form, (b) create derivate works based on the Services, (c) copy, frame or mirror any part or content of the Services, other than copying or framing on Customer’s own intranets or otherwise for Customer’s own internal business purposes or for purposes consistent with this Agreement, (d) reverse engineer the Services, or (e) access the Services in order to (i) build a competitive product or service, or (ii) copy any features, functions or graphics of the Services.

7.3 Ownership of Customer Data. As between Customer and Aryaka, Customer exclusively owns all rights, title and interest in and to all of Customer Data.

7.4 Ownership of Aryaka Equipment. As between Customer and Aryaka, Aryaka exclusively owns all rights, title and interest in and to all Aryaka Equipment that Aryaka provides to Customer for the purpose of providing Services pursuant to the terms of this Agreement. For clarity, Aryaka retains the right to the return by Customer of all such Aryaka Equipment pursuant to the terms set forth in Section 4.2(a) above.

7.5 Suggestions. Notwithstanding Section 8 below, Aryaka shall have a royalty-free, worldwide, transferable, sub-licensable, irrevocable, perpetual license to use or incorporate into the Services any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including Users, relating to the operation of the Services. However, Customer’s name and the identity of any Customer Data will not be used.

8. CONFIDENTIALITY AND DATA PROTECTION

8.1 Definition of Confidential Information. As used herein, “Confidential Information” means all confidential information disclosed by a Party (“Disclosing Party”) to the other Party (“Receiving Party”), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Customer’s Confidential Information shall include Customer’s or its Affiliates’ Data; Aryaka’s Confidential Information shall include the Services; and Confidential Information of each Party shall include the terms and conditions of this Agreement and all Order Forms, as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such Party. However, Confidential Information (other than Customer’s Data) shall not include any information that (a) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (c) is received from a third party without breach of any obligation owed to the Disclosing Party, or (d) was independently developed by the Receiving Party.

8.2 Protection of Confidential Information. Except as otherwise permitted in writing by the Disclosing Party, (a) the Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) not to disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (b) the Receiving Party shall limit access to Confidential Information of the Disclosing Party to those of its employees, contractors and agents who need such access for purposes consistent with this Agreement and who have entered into or are otherwise bound by confidentiality agreements with the Receiving Party containing protections no less stringent than those herein.

8.3 Protection of Customer's Data. Without limiting the above or anything else in this Agreement, Aryaka shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer's Data in or on the Aryaka Network, all subject to and as set forth in the Data Protection Agreement between the parties included in **Exhibit B** attached hereto and made a part of this Agreement. Although the Data Protection Agreement is and addendum to this Agreement, the parties agree to provide the information and execute the Data Protection Agreement as required by the applicable data privacy laws as set forth in the Data Protection Agreement.

8.4 Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior written notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

9. WARRANTIES AND DISCLAIMERS

9.1 Aryaka's Warranties. Aryaka represents and warrants that (a) the Services shall perform materially in accordance with the terms of this Agreement including any Exhibits hereto and the applicable Order Forms during a Subscription Term, and (b) the functionality of the Services will not be materially decreased during a Subscription Term. For any breach of either such warranty, Customer's exclusive remedy shall be as provided in Section 12.2 (Termination for Cause). The foregoing does not diminish Customer's rights and remedies under applicable service level agreements.

9.2 Mutual Warranties. Each party represents and warrants that (a) it has the legal power and authority to enter into this Agreement, and (b) it will not transmit to the other party any Malicious Code.

9.3 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN (INCLUDING THIS AGREEMENT AND ANY EXHIBITS HERETO AND THE ORDER FORM), NEITHER PARTY MAKES ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

10. MUTUAL INDEMNIFICATION

10.1 Indemnification by Aryaka. Aryaka shall indemnify, defend and hold Customer harmless against any claim, demand, suit, or proceeding ("Claim") made or brought against Customer by a third party that the use of the Services as authorized under this Agreement infringes or misappropriates the intellectual property rights in the United States of a third party, and shall indemnify Customer for any damages finally awarded against, and for reasonable attorney's fees incurred by, Customer in connection with any such Claim; provided, that Customer (a) promptly give Aryaka written notice of the Claim; (b) give Aryaka sole control of the defense and settlement of the Claim (provided that Aryaka may not settle any Claim without Customer's prior written consent unless the settlement unconditionally releases Customer of all liability); and (c) provide to Aryaka all reasonable assistance, at Aryaka's expense.

10.2 Indemnification by Customer. Customer shall defend and hold Aryaka harmless against any Claim made or brought against Aryaka by a third party alleging that Customer's Data, or Customer's use of the Services in violation of this Agreement, infringes or misappropriates the intellectual property rights of a third party, or violates applicable law, and shall indemnify Aryaka for any damages finally awarded against, and for reasonable attorney's fees incurred by, Aryaka in connection with any such Claim; provided, that Aryaka (a) promptly give Customer written notice of the Claim; (b) give Customer sole control of the defense and settlement of the Claim (provided that Customer may not settle any Claim without Aryaka's prior written consent unless the settlement unconditionally releases Aryaka of all liability); and (c) provide to Customer all reasonable assistance, at Customer's expense.

10.3 Exclusive Remedy. This Section 10 (Mutual Indemnification) states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of Claim described in this Section 10.

11. LIMITATION OF LIABILITY

11.1 Limitation of Liability. IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER HEREUNDER OR, WITH RESPECT TO EACH SINGLE INCIDENT, THE AMOUNT PAID BY CUSTOMER HEREUNDER IN THE TWELVE (12) MONTHS PRECEDING THE INCIDENT. THE FOREGOING SHALL NOT LIMIT CUSTOMER'S PAYMENT OBLIGATIONS

UNDER SECTION 6 (FEES AND PAYMENT FOR SERVICES) OR EITHER PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 10 (MUTUAL INDEMNIFICATION).

11.2 Exclusion of Consequential and Related Damages. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER SHALL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

12. TERM AND TERMINATION

12.1 Term of Agreement. This Agreement commences on the date Customer accepts it and continues until all Order Forms granted in accordance with this Agreement have expired or been terminated (the "Initial Term"), whichever is later. For clarity, Customer understands and agrees that, except as provided in Section 12.2 (Termination for Cause), Customer may not elect to terminate this Agreement or otherwise "opt out" of this Agreement or Customer's obligations hereunder for any reason during the Initial Term or renewal period. Such "opt out" is available to Customer only in connection with a renewal whereby Customer provides written notice of non-renewal at least ninety (90) days before the end of the relevant term.

12.2 Termination for Cause. A party may terminate this Agreement for cause: (a) upon thirty (30) days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (b) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors, except if any such petition is involuntary and is dismissed within sixty (60) days.

12.3 Return of Aryaka Equipment. At Aryaka's expense, Customer agrees to return all Aryaka Equipment within sixty (60) business days after the termination of this Agreement pursuant to shipping instructions to be provided by Aryaka, provided that the terms of Section 4.2(a) above shall apply in the event that Customer does not return all items of such Aryaka Equipment pursuant to this Section 12.3.

12.4 Surviving Provisions. Section 6 (Fees and Payment for Services), 7 (Proprietary Rights), 8 (Confidentiality), 9.3 (Disclaimer), 10 (Mutual Indemnification), 11 (Limitation of Liability), 14 (Notices, Governing Law and Jurisdiction, Jury Trial) and 15 (General Provisions) shall survive any termination or expiration of this Agreement.

13. ANTI-BRIBERY LAWS. Each Party (including its officers, directors, employees, agents and any person under its control) shall comply with, and shall require its contractors, subcontractors and any contingent workers to comply with, any and all applicable anti-corruption laws and regulations, including, but not limited to, the U.S. Foreign Corrupt Practices Act and the UK Bribery Act 2010. It is the intent of the parties hereto that no payments, offers or transfers of value shall be made or received which have the purpose or effect of public or commercial bribery, acceptance or acquiescence in extortion, kickbacks or other unlawful or

improper means of obtaining or retaining business or directing business to any person or entity. In addition, each party warrants to the other that none of its officers, directors, employees, agents, or representatives is an official or employee of the government of the Territory or of any department or instrumentality of such government, nor is any of them an officer of a political party or candidate for political office who will share, directly or indirectly, any part of the sums due hereunder. Both parties represent and warrant that each will conduct its business operations hereunder in accordance with all applicable U.S. and foreign laws, and regulations, and will not attempt to directly or indirectly improperly influence the sale by payments or other actions contrary to law or regulation.

14. NOTICES, GOVERNING LAW AND JURISDICTION, JURY TRIAL

14.1 Notices. Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be in writing and shall be deemed to have been given upon: (a) personal delivery or (b) written verification of receipt by established overnight courier, or (c) confirmation of email message sent to the designated email address, or (d) upon delivery if sent by US certified mail prepaid return receipt. Notices to Aryaka shall be addressed to: Aryaka Networks, Inc., Attn: Legal, 1800 Gateway Drive, San Mateo, California 94404 USA, email: legal@aryaka.com, with a copy to VP Sales, Aryaka Networks, Inc., 1800 Gateway Drive, San Mateo, California 94404 USA. Notices to Customer shall be addressed to: _______________________, and in the case of billing-related notices, addressed to: ___________________.

14.2 Governing Law and Jurisdiction. This Agreement shall be interpreted under California law without regard to choice or conflicts of law rules, and the parties agree to submit to the exclusive jurisdiction of the applicable state courts in San Mateo County, California, or federal courts of the Northern District of California. ***The Parties expressly disclaim application of the UN Convention on the International Sale of Goods.***

14.3 Waiver of Jury Trial. Each Party hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

15. GENERAL PROVISIONS

15.1 Export Compliance. Each party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Services. Without limiting the foregoing, (a) each party represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports, and (b) Customer shall not permit Users to access or use Services in violation of any U.S. export embargo, prohibition or restriction.

15.2 Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

15.3 No Third-Party Beneficiaries. There are no third-party beneficiaries of this Agreement.

15.4 Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

15.5 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

15.6 Assignment. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld). Notwithstanding the foregoing, either Party may assign this Agreement in its entirety (including all Order Forms), without consent of the other Party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other Party. A Party's remedy for any purported assignment by the other Party in breach of this paragraph shall be, at the non-assigning Party's election, either to void this Agreement or termination of this Agreement immediately upon written notice to the assigning Party. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the Parties, their respective successors and permitted assigns.

15.7 Entire Agreement. This Agreement, including all exhibits and addenda hereto and all Order Forms, constitutes the entire, final, complete and exclusive agreement between the Parties and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and either signed or accepted electronically by both Parties hereto. However, to the extent of any conflict or inconsistency between the provisions in the body of this Agreement and any exhibit or addendum hereto or any Order Form, the terms of such exhibit, addendum or Order Form shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in Customer's purchase order or other order acknowledgment, documentation or the like (excluding Order Forms) shall be incorporated into or form any part of this Agreement, and all such terms or conditions are hereby rejected by Aryaka and shall be null and void.

15.8 Execution and Delivery. This Agreement may be executed in counterpart and signature by scanned image and delivery by electronic mail are authorized.

IN WITNESS WHEREOF, each of the Parties, by its duly authorized representative, has executed this Agreement as of the date first above written.

ARYAKA NETWORKS, INC.

Signature: ______________________________

Printed Name: _________________________

Title: __________________________________

Date: __________________________________

[Customer Name:]

Signature: _____________________________

Printed Name: _________________________

Title: __________________________________

Date: __________________________________

EXHIBIT A

SERVICE LEVEL AGREEMENT

Aryaka provides this SLA subject to the following terms. Aryaka has the right to update these from time to time without notice. The most current version of these SLA terms is set forth at: https://www.aryaka.com/aryaka-service-level-agreement.

1. STANDARD TERMS APPLICABLE TO ALL SERVICE LEVELS OUTLINED HEREIN:

A. DEFINITIONS

i. “Claim” means a claim submitted by Customer to Aryaka pursuant to this SLA that a Service Level has not been met and that a Service Credit may be due to Customer.

ii. “Customer” refers to the organization that has signed a services agreement (“Agreement”) under which it has purchased and deployed Aryaka’s SmartConnect service.

iii. “Customer Support” means the services by which Aryaka may provide assistance to Customer to resolve issues with the Services.

iv. “Incident” means any set of circumstances resulting in a failure to meet a Service Level.

v. “Aryaka” means Aryaka Networks, Inc.

vi. “Service” or “Services” refers to the Aryaka’s SmartConnect service provided to Customer pursuant to the Agreement.

vii. “Monthly Uptime Percentage” is the percentage of uptime per month as measured POP to POP.

viii. “Service Credit” is the daily service fee equivalent to 1/30th of the monthly service fee for the Service that is credited to Customer for a validated Claim.

ix. “Service Level” means standards Aryaka chooses to adhere to and by which it measures the level of service it provides as specifically set forth below.

x. “Excused Outage” means a scheduled maintenance window, for which Customer will be given 48 hours’ notice, or during conditions which constitute a Force Majeure, as described in the Agreement.

B. SERVICE CREDIT CLAIMS

i. Claims must be submitted by the end of the billing month in which the Incident which is the subject of a Claim occurs.

ii. Customer must provide to Aryaka Customer Support all reasonable details regarding the Claim, including but not limited to, detailed descriptions of the Incident(s), the duration of the Incident, and any attempts made by Customer to resolve the Incident.

iii. Only one Claim may be submitted per 24-hour day of service, as defined by GMT midnight, regardless of the number of incidents occurring in that day.

C. SLA EXCLUSIONS

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. During an Excused Outage;
2. Due to missing and/or incorrect configuration in the customer’s network as well as incorrect information entered into MyAryaka portal by the customer;

3. That resulted from Customer's or third-party hardware or software;
4. That resulted from actions or inactions of Customer or third parties;
5. Caused by Customer's use of the Service after Aryaka advised Customer to modify its use of the Service, if Customer did not modify its use as advised;
6. During beta, pilot and trial Services (as determined by Aryaka); Or
7. Attributable to the acts or omissions of Customer or Customer's employees, agents, contractors, or vendors, or anyone gaining access to Aryaka's Service by means of Customer's passwords or equipment.

D. SERVICE CREDITS

i. The amount of Service Credit for each incident will be equal to 1/30th of the Customers monthly Service fees.
ii. Service Credits are Customer's sole and exclusive remedy for any violation of this SLA.
iii. The Service Credits awarded in any billing month shall not, under any circumstance, exceed Customer's monthly Service fees.
iv. Service Credits for this SLA will only be calculated against monthly fees associated with Aryaka's SmartConnect service. This does not include any additional recurring or one-time fees.

2. MONTHLY SMARTCONNECT SERVICE AVAILABILITY LEVEL

a. Aryaka will maintain a Monthly Uptime Percentage of 99.99%.
b. Monthly Uptime Percentage will be measured between Aryaka's points of presence (POP) occurring at 5 minute intervals.
c. An Incident for which Customer may be eligible to submit a Claim is defined as occurring if three consecutive measurements show loss of connectivity between POPs.

3. CLOUD CONNECTIVITY

Aryaka's SmartConnect service provides private connections to IaaS platforms like AWS, Azure and Oracle globally. Aryaka's global network is connected to these IaaS providers using a pair of redundant private links in multiple regions of the world. This connectivity is achieved by using the providers' service like ExpressRoute for Azure, DirectConnect for AWS and FastConnect for Oracle. The following provides an SLA description around that connectivity.

Cloud Connectivity SLA:

A. Aryaka will maintain a Monthly Uptime Percentage of 99.99% on the private connections between its POPs and to the IaaS provider.

B. If Monthly Uptime Percentage falls below 99.99%, Customer is eligible to submit a Service Level Claim for the day where there was an outage.

For Customer to be eligible for this Service Level Claim, Customer cloud locations must be connected over a private connection service supported by Aryaka. Azure-ExpressRoute, AWS-DirectConnect and Oracle-FastConnect are the only currently supported services. Aryaka is not responsible for failures which occur inside the IaaS provider network or service, and it only covers the link that connects Aryaka's network to the IaaS provider. Such Service Level Claims will be submitted pursuant to the terms set forth above in this SLA.

EXHIBIT B

DATA PROTECTION AGREEMENT

ARYAKA NETWORKS, INC. – DATA PROTECTION ADDENDUM – GDPR / CCPA

Preliminary Notes – The following Data Protection Agreement:

- *is drafted to incorporate the terms required by (A) Article 28 of the General Data Protection Regulation (GDPR) 2016/679 between “controllers” and “processors” where Supplier (Aryak is acting as a data processor, and (B) the California Consumer Protection Act of 2018 (CCPA) where Supplier, Customer, or both are acting as a “business”;*
- *is to protect the “Personal Data” of “data subjects” under the GDPR and to protect the “Personal Information” of “consumers” under the CCPA;*
- *is intended for appending as an Addendum or Schedule of the underlying Contract (Master Subscription Agreement) – it is not a stand-alone agreement; and*
- *Requires Customers to select either the categories of Personal Data and Personal Informatio in Annex A to be covered OR the representation in the signature block that these categories not apply.*

DATA PROTECTION AGREEMENT

(Covering European Economic Area (GDPR), California (CCPA) and Elsewhere)

The following terms and conditions of this Supplier Data Protection Agreement (the “**DPA**”) is entered into between [INSERT CUSTOMER ENTITY], (“**Customer**”) on behalf of itself and its Authorized Affiliates and **Aryaka Networks, Inc.** on behalf of itself and its Affiliates (collectively, “**Supplier**”) and applies to and is made part of the Contracts, each a **“Party”**, together the **“Parties”**. For the purposes of this DPA only, and except where otherwise indicated, the term “Customer” shall include Customer and its Authorized Affiliates.

BACKGROUND

A. Supplier has entered into one or more Master Subscription Agreements, purchase orders, contracts, agreements and the like (the “**Contracts**)” with Customer which may include Authorized Affiliates.

B. In delivering the services under the Contracts (the “**Services**”), Supplier may process Customer Personal Data or Consumer Personal Information controlled by Customer or its respective customers, suppliers, or business partners.

C. As part of their privacy programs and contractual arrangements, the Parties have provided certain assurances to its employees, independent contractors, candidates, customers, consumers, suppliers or business partners to ensure the appropriate protection of Customer Personal Data and Consumer Personal Information.

D. Therefore, the Parties desire to be subject to certain data protection laws, rules and regulations in the European Economic Area, California USA, and all other applicable areas of the world (the **"Applicable Privacy Laws"**) pursuant to this DPA.

AGREEMENT

1. DEFINITIONS

1.1 "Affiliate" means any entity that is directly or indirectly controlled by, controlling or under common control with a Party. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2 "Applicable Privacy Laws" means (a) all worldwide data protection and privacy laws and regulations applicable to the Customer Personal Data and Consumer Personal Information in question, (b) including, where applicable, EEA Data Protection Law and (c) the California Consumer Protection Act.

1.3 "Authorized Affiliate" means any of Customer's Affiliates permitted to or otherwise receiving the benefit of the Services pursuant to the Contracts.

1.4 "Authorized Persons" means any person who processes personal data or personal information under this DPA on a Party's behalf, including that Party's employees, officers, directors, partners, principals, agents, representatives, contractors, and in the case of Supplier, its Sub-Processors.

1.5 "Business" or "business" means, under the CCPA, any for-profit legal entity that does business in the state of California and collects and controls consumers' personal information and satisfies one or more of the following thresholds: (a) annual gross revenues in excess of $USD25 million, (b) alone or in combination buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households or devices on an annual basis, and (c) derives 50% or more of its annual revenues from selling consumers' personal information. A "business" also includes any entity that controls or is controlled by a business that satisfies these criteria. For the avoidance of doubt, "Customers" that are also controllers under the GDPR are included as "Businesses" for purposes of this Agreement.

1.6 "California Consumer Protection Act" or "CCPA" means the California Consumer Protection Act of 2018, in particular 2017 California Assembly Bill No. 375, California 2017-2018 Regular Session (amending Part 4 of Division 3 of the California Civil Code), amended by 2017 California Senate Bill No. 1121, that defines the "personal information" subject to its protection and grants consumers extensive rights to control that information, to become effective approximately January 1, 2020 and enforceable on and after approximately June 1, 2020 (as superseded, amended or replaced).

1.7 "Consumer" or "consumer" means, under the CCPA, any natural person who is a California resident to who Personal Information relates, but does not include sole proprietorships, partnerships, limited liability companies or corporations, and certain other legal entities specified in the CCPA.

1.8 "Customer Personal Data" or "Customer Data" means and includes all Personal Information and Personal Data except where specified otherwise (i) provided to Supplier by or at the direction of Customer in connection with the Services; (ii) created or obtained by Supplier on behalf of Customer in the performance of Services; or (iii) which Supplier accesses at the direction of Customer, in the course of Supplier's performance under the Contracts, it being understood that the Services do not, and in the ordinary course of providing Services Supplier does not, access Personal Information or Personal Data or any personally identifiable information, but instead provides a proprietary software-defined wide area network (SD-WAN) over which data is carried. For the avoidance of doubt, "Customers" that are also controllers under the GDPR are included as "Businesses" for purposes of this Agreement.

1.9 "Controller" means the entity that determines the purposes and means of the processing of Personal Data or Personal Information.

1.10 "C2C Model Clauses" means the Standard Contractual Clauses for Controllers as approved by the European Commission and available at http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_set_ii_c2004-5721.doc (as amended, superseded or updated from time to time). The current version (as of the Effective Date) of these clauses is set forth in **Schedule 1.8** to this DPA.

1.11 "C2P Model Clauses" means the Standard Contractual Clauses for Processors as approved by the European Commission and available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. (as amended, superseded or updated from time to time). The current version (as of the Effective Date) of these clauses is set forth in Schedule 1.9 to this DPA.

1.12 "Data Subject" or "data subject" means the identified or identifiable person to whom Personal Data relates.

1.13 "EEA Data Protection Law" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Customer Personal Data and on the free movement of such data (the "Directive"); and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Customer Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) the e-Privacy Directive (Directive 2002/58/EC); and (iii) any national data protection laws made under or pursuant to (i) or (ii) (in each case, as superseded, amended or replaced).

1.14 "Personal Data", "Personal Information", "processing", "process", "sell", "collect" and "supervisory authority" shall have the meanings, respectively, given in the Applicable Privacy Law.

1.15 "Privacy Shield" means the EU-US and Swiss-US Privacy Shield Frameworks, as administered by the U.S. Department of Commerce.

1.16 "Privacy Shield Principles" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive, details of which can be found at www.privacyshield.gov/eu-us-framework.

1.17 "Processor" means the entity that processes Personal Data or Personal Information on behalf of the Controller.

1.18 "Processor Binding Corporate Rules" means the Binding Corporate Rules Processor (or BCR-P) of the Supplier that have been approved by a supervisory authority.

1.19 “Security Incident” means any unauthorized or unlawful breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to Personal Data or Personal Information transmitted, stored or otherwise processed by Supplier or its Sub-Processors.

1.20 “Sub-Processor” means any Processor engaged by Supplier or its Affiliates to assist in fulfilling its obligations with respect to providing the Services that processes Customer Data.

2. SCOPE, GDPR / CCPA REQUIREMENTS, RIGHTS AND REMEDIES

2.1 **Scope.** ***This Agreement covers protection under the GDPR of Personal Data of data subjects that is controlled or processed by data controllers and processors, and protection under the CCPA of Personal Information of consumers that is collected or used by businesses. Data controllers and data processors are considered to be “businesses” under this Agreement.*** Specifically: (a) With respect to the GDPR: Applies to processing of personal data: (i) relating to EU or non-EU data subjects in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not, and (ii) of EU data subjects by controllers or processors located outside of the EU if the processing activities are related to the offering of goods or services to, or monitoring the behavior of, individuals residing in the EU. (b) With respect to the CCPA: Applies to businesses located within or outside of California if personal information of California consumers is collected. For clarity, the protections of the CCPA are associated with California residents. Accordingly, any business that "does business" in California, regardless of its physical location, may become covered by the CCPA due to its interaction with California residents.

2.2 **Roles of the Parties and Details of Processing.** Supplier shall process Personal Information and Personal Data under the Contracts as a Processor acting on behalf of Customer. Supplier agrees that it will process Personal Information and Personal Data as described at **Annex A**, which forms an integral part of this DPA.

2.3 **Supplier’s Processing of Data and Information.** Supplier shall at all times process the Personal Information and the Personal Data only for the purpose of providing the Services to Customer under the Contracts and in accordance with Customer's documented instructions.

2.4 **Supplier’s Notification Obligations Regarding Customer Instructions.** Supplier shall promptly notify Customer in writing, unless prohibited from doing so under Applicable Privacy Law, if:

(a) It becomes aware or believes that any data processing instruction from Customer violates Applicable Privacy Law;
(b) It is unable to comply with Customer’s data processing instructions for any reason; or
(c) It is unable to comply with the terms of the Contracts (including this DPA) as they relate to or govern the processing of Personal Information or Personal Data or the security of Personal Information or Personal Data for any reason.

2.5 **Information Requirements:**

(a) With respect to the CCPA: (i) Upon receipt of a consumer's request for any disclosure of the categories and specific pieces of Personal Information that a business has collected about that consumer, the business shall deliver such information to the consumer free of charge within 45 days of receipt of a verifiable request. The time period for disclosure may be extended once by an additional 45 days upon the provision of notice to the consumer. The delivery of information may be made by mail or electronically. However, electronic disclosures must be provided in portable format to the extent feasible. (ii) Businesses that collect a consumer's Personal Information shall, either at or before the point of collection, inform consumers as to the categories of Personal Information to be collected and the purposes for which the categories of Personal Information shall be used. Businesses shall not collect additional categories of Personal Information, or use collected information for additional purposes, without providing notice to the consumer. (iii) Businesses shall include the information set forth in 2.5(a)(i) and 2.5(a)(ii) in the business' privacy policy and update the policy at least once every 12 months.

(b) With respect to the GDPR: (i) A list of information shall be provided to data subjects (A) at the time their Personal Data is obtained if their Personal Data was collected directly from them, or (B) within 30 days or other applicable timeframes afterwards specified in the Applicable Privacy Law if their Personal Data was not collected directly from them, unless provision of such data would be impossible or involve a disproportionate effort. (ii) The list of information to be provided includes the identity and contact details of the controller, the contact details of the data protection officer, the purposes for processing and legal bases for processing, the recipients of the Personal Data, the Personal Data retention period, the data subjects' rights, and appropriate safeguards used to transfer the Personal Data out of the EU. (iii) The information set forth in 2.5(b)(i) and 2.5(b)(ii) shall be included in a policy or notice such as the controller's or processor's privacy policy notice or a GDPR-specific policy.

2.6 **Consent Requirements:**

(a) With respect to the CCPA: In order to comply with consumer opt-out provisions, businesses must make available two or more designated methods for submitting requests for disclosure of information including, at minimum, a toll-free telephone number and a public website. Business' websites must provide a clear and conspicuous link on their websites titled *"Do Not Sell My Personal Information"* that enables consumers to opt-out of the sale of their Personal Information. In addition, businesses must provide a description of consumers' right to opt out of the sale of their Personal Information, along with the above-described website link, in their website privacy policies or in any California-specific description of consumers' privacy rights. Businesses must also disclose in a form that is reasonably accessible to consumers and in accordance with a specified process that consumers have a right to request that their Personal Information be deleted.

(b) With respect to the GDPR: If the grounds for processing Personal Data is based the consent of the data subject, the controller or processor understand and agree that any such consent must be as defined in the Applicable Privacy Law, as follows: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

2.7 **Data Retention Requirements:**

(a) With respect to the CCPA: Businesses are not required to retain Personal Information collected for a single, one-time transaction if the information is not sold or retained by the business. However, businesses that sell or retain Personal Information shall provide disclosures to consumers regarding the collection and use of their Personal Information covering the preceding 12-month period from the date of receipt of the request.

(b) With respect to the GDPR: Personal Data must be retained in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed, except as provided in the Applicable Privacy Law. Information about the period for which Personal Data will be stored, or if that is not possible, the criteria used to determine that period, shall to be included as part of the information requirements (see Section 2.5(b) above).

2.8 **Individual Rights:**

(a) With respect to the CCPA: Subject to exemptions or conditions in the Applicable Privacy Law, if any, each consumer shall have the right to: (i) request that a business delete Personal Information that it has collected on such consumer; (ii) request and receive information about, and specific items of, Personal Information on such consumer that has been collected or sold or disclosed to third parties by a business; (iii) opt out of the sale of a consumer's Personal Information; and (iv) not be discriminated against due to the exercise of any right established by the CCPA.

(b) With respect to the GDPR: Subject to exemptions or conditions in the Applicable Privacy Law, if any, each data subject shall have the right to: (i) request that a data controller or data processor delete Personal Data that it has collected on such data subject; (ii) request and receive information about, and specific items of, Personal Data of such data subject that has been collected or sold or disclosed to third parties by a data controller or data processor; (iii) request that Personal Data be rectified; (iv) have the processing of Personal Data restricted; (v) have Personal Data provided to it and transferred to another organization; (vi) object to the processing of its Personal Data; (vii) withdraw consent to the processing of its Personal Data; (viii) complain to a regulator concerning the processing of its Personal Data; and (ix) not be subject to a decision based solely on certain forms of automatic processing, including profiling.

2.9 **Opt Out:**

(a) With respect to the CCPA: Any business that proposes to sell consumers' Personal Information shall disclose this fact to such consumers, who shall have the right to opt out of the sale of their Personal Information. For consumers under the age of 16, the parents of any such consumer have the right to opt-in to any sale of such consumer's personal information.

(b) With respect to the GDPR: Data subjects may seek to enforce their rights described in Section 2.8(b) with regard to any selling of their Personal Data.

2.10 **Remedies:**

(a) With respect to the CCPA: (i) The CCPA provides a private right of action for any consumer whose non-encrypted or non-redacted Personal Information was subject to an unauthorized access and exfiltration, theft or disclosure as a result of a business' failure to implement and maintain reasonable security procedures. Statutory damages are provided in the Applicable Privacy Law and also injunctive and declaratory relief and any other relief deemed proper by the court. (ii) The CCPA also provides for administrative enforcement, including by authorizing the attorney general of California to bring actions for civil penalties against any business that fails to cure an alleged violation of the Applicable Privacy Law within 30 days of being notified of such violation.

(b) With respect to the GDPR: Data subjects have the right to: (i) A judicial remedy against a legally binding decision of a regulator. (ii) A judicial remedy against a controller or processor. (iii) Compensation from a controller or processor. Regulators may also impose fines on controllers or processors as provided in the Applicable Privacy Law.

2.11 **Limited Supplier Rights.** Except as expressly set forth to the contrary in this DPA or the Contracts, Supplier acknowledges that it has no right, title or interest in Personal Information or Personal Data and may not sell, rent or lease Personal Information or Personal Data to anyone.

3. SUBPROCESSING

3.1 Appointment of Sub-Processors. Supplier shall not subcontract any processing of the Personal Data or Personal Information to a Sub-Processor without the prior written consent of Customer. Such consent will not be unreasonably withheld, delayed or conditioned. Notwithstanding this, Customer hereby consents to Supplier engaging Sub-Processors to process the Personal Data and Personal Information provided that:

(a) Notification of New Sub-Processors. Supplier provides at least 30 days prior written notice to Customer of any change in its Sub-Processors (including details of the processing, location and any other information reasonably required by Customer) and Supplier shall update the list of all Sub-Processors engaged to process Personal Data and Personal Information under this DPA at Annex C and send such updated version to Customer prior to the change of Sub-Processor;

(b) Objection Right for New Sub-Processors. Customer may object to the appointment or replacement of a Sub-Processor within 10 days after Customer first receives prior notice of such change, provided such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss in good faith commercially reasonably alternative solutions;

(c) Data Protection Terms for Sub-Processors. Supplier imposes the same data protection terms contained in this DPA on any Sub-Processor it engages; and

(d) Liability. Supplier remains fully liable for the acts or omissions of its Sub-Processors to the same extent Supplier would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

4. RIGHTS OF DATA SUBJECTS AND CONSUMERS AND COOPERATION

4.1 **Data Subject or Consumer Request.** Supplier shall, taking into account the nature of the processing, reasonably cooperate with Customer to enable Customer to respond to any requests, complaints or other communications from Data Subjects or Consumers or regulatory or judicial bodies relating to the processing of Personal Data or Personal Information, including requests from Data Subjects or Consumers seeking to exercise their rights under Applicable Privacy Laws (“**Data Request”**). In the event a Data Request is made directly to Supplier, Supplier shall promptly notify the Customer of the request and shall not respond to such communication without Customer's express authorization.

4.2 **Subpoenas and Court Orders.** If Supplier receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data or Personal Information, Supplier shall not disclose any information but shall immediately notify Customer in writing of such request, and reasonably cooperate with Customer if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

4.3 **Data Privacy Impact Assessments (“DPIA’s”)**. To the extent Supplier is required under Applicable Privacy Laws, Supplier will assist Customer (or its third-party Controller) to conduct a data protection impact assessment (DPIA) and, where legally required, consult with applicable data protection authorities in respect of any proposed processing activity conducted in connection with the Services and the performance of the Contracts that may present a high risk to Data Subjects or Consumers with respect to unauthorized disclosures of data.

5. DATA ACCESS & SECURITY MEASURES

5.1 Confidentiality and Limited of Access. Supplier shall ensure that any Authorized Person is subject to a duty of confidentiality (whether a contractual or statutory duty) and that they process Personal Data and Personal Information only for the purpose of delivering the Services under the Contracts to Customer. Supplier shall ensure that Supplier’s access to Personal Data and Personal Information is limited to those personnel performing the Services.

5.2 Security Measures. Supplier will implement and maintain all appropriate technical and organizational measures to protect any Personal Data and Personal Information from Security Incidents and to preserve the security and confidentiality of such Personal Data and Personal Information. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. At a minimum, Supplier agrees to the Security Measures identified at Annex B related to the protection of Personal Data and Personal Information.

6. SECURITY INCIDENTS

6.1 Notification of Security Incidents. In the event of a Security Incident, Supplier shall inform Customer without undue delay, and in any event no later than 24 hours of becoming aware of such Security Incident, and provide written details of the Security Incident, including the type of data affected and the identity of affected persons as soon as such information becomes known or available to Supplier.

6.2 Supplier Obligations Following Security Incident. In the event of a Security Incident, Supplier shall:

(a) Provide all timely information and cooperation as Customer may reasonably require to fulfill Customer's data breach reporting obligations under (and in accordance with the timeframes provided by) Applicable Privacy Laws or to comply with or respond to any inquiries by a data protection authority or any lawsuit arising from the Security Incident, including collecting and preserving all evidence pertaining to the Security Incident and any investigation conducted by Supplier. Such information shall include, without limitation:

(i) the nature of the Security Incident including, where possible, the categories and approximate number of Data Subjects and Consumers concerned and the categories and approximate number of records concerned;

(ii) the name and contact details of the contact point within Supplier (or Supplier's Sub-processor's as applicable) who can provide more information on the Security Incident;

(iii) a description of the likely consequences of the Security Incident based on Supplier’s reasonable assessment; and

(iv) a description of the measures Supplier (or its Sub-processor's, as applicable) will take, proposes to take, or suggests that Customer takes to address the Security Incident, including, where appropriate to mitigate its possible adverse effects.

(b) Promptly take all such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident and shall keep Customer informed about all developments in connection with the Security Incident; and

(c) Reasonably assist Customer, at Customers expense and if requested by Customer, to prepare and send all notifications that are legally required or reasonably necessary with respect to each Data Security Incident involving Personal Data and Personal Information.

6.3 The content and provision of any notification, public and regulatory communication, or press release concerning the Security Incident shall be solely at Customer’s reasonable discretion, except as otherwise required by Applicable Privacy Laws.

7. SECURITY REPORTS & INSPECTIONS

7.1 Supplier Security Standards. Supplier shall maintain records of its security standards. Upon request, Supplier shall provide to Customer copies of relevant external certifications, audit report summaries or other documentation maintained or obtained by Supplier in order to verify Supplier's compliance with this DPA.

7.2 Right of Inspection. While it is the Parties' intention ordinarily to rely on Supplier's obligations set forth in Section 7.1 to verify Supplier's compliance with this DPA, Customer (or its appointed representatives) may, at Customer’s sole expense, carry out an inspection of the Supplier's operations and facilities where Customer considers it necessary or appropriate (for example, without limitation, where Customer has reasonable concerns about Supplier's data protection compliance, following a Security Incident or following instruction from a data protection authority). With respect to any such inspection, Supplier shall make available all information reasonably necessary to demonstrate compliance with Applicable Privacy Laws. Notwithstanding the foregoing, any such inspection shall be (a) limited to the provision of Supplier's then-current technical documentation which relates to the processing of Personal Data and Personal Information unless otherwise required by a data protection authority, (b) subject to Supplier's confidentiality, security and safety terms and policies, and (c) conducted during ordinary business hours and after reasonable advance written notice

8. INTERNATIONAL TRANSFERS

8.1 **International Transfers.** Supplier or its Affiliates shall not process or transfer any Personal Data or Personal Information in or to a territory other than the territory in which the Personal Data and Personal Information was first collected (nor permit such data to be so processed or transferred) unless it takes all such measures as are necessary to ensure such processing or transfer is in compliance with Applicable Privacy Laws (including such measures as may be communicated by Customer to Supplier) and in accordance with any applicable transfer mechanism provisions set forth in Section 8.3 below. However, Customer's execution of each Contract shall be deemed to be Customer's instructions to Supplier with respect to the transfer of Personal Data and Personal Information pursuant to the Services provided under the Contracts. Except with respect to such transfers under the Contracts, Supplier shall inform Customer of any international transfers of Personal Data and Personal Information in advance of making the transfer and shall assist Customer in assessing the parties' respective obligations to comply with Applicable Privacy Laws.

8.2 Privacy Shield Flow Downs. To the extent that Customer or the Authorized Affiliates are self-certified to the Privacy Shield, Supplier represents and warrants that it shall:

(a) Provide at least the same level of protection to such Customer Personal Data as is required by the Privacy Shield Principles and the Security Measures set forth in Section 5.2 of this DPA; and

(b) Promptly notify Customer if it makes a determination that it can no longer meet its obligations under Section 8.2(a) above, and in such event, to work with Customer and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by Section 8.2(a).

8.3 **Transfer Mechanisms.**

(a) **Supplier Self-Certification to Privacy Shield.** To the extent Supplier or its US Affiliates are self-certified to Privacy Shield, Supplier agrees: (i) that it or its US Affiliates (as applicable) shall maintain such Privacy Shield certification; and (ii) with respect to Customer Personal Data that is protected by EEA Data Protection Law or that originates from Switzerland, it or its US Affiliates (as applicable) shall comply with the Privacy Shield Principles when handling such data.

(b) **Processor Binding Corporate Rules.** To the extent Supplier has adopted Processor Binding Corporate Rules, Supplier agrees that it shall maintain such Processor Binding Corporate Rules when handling Customer Personal Data.

(c) **Incorporation of Model Clauses.** In the event Supplier or its Affiliates are not utilizing the transfer mechanisms set forth in 8.3 (a) or (b), then the Parties further agree: (i) the Model Clauses are incorporated by reference and form an integral part of this DPA; (ii) Supplier or its Affiliates (as applicable) shall be the "data importer" and Customer (acting on behalf of itself and all Affiliates) is the "data exporter" (notwithstanding that Customer may be located outside the European Economic Area or Switzerland and may itself be a Processor acting on behalf of third party Controllers); and (iii) Annexes A and B of this DPA will take the place of Appendixes 1 and 2 of the Model Clauses, respectively.

8.4 **Disclosure of DPA.** Each Party acknowledges that the other Party or its Affiliates may disclose this DPA and any relevant privacy provisions in the Contracts to the US Department of Commerce, the Federal Trade Commission, European data protection authority, or any other US or EU judicial or regulatory body upon their legitimate and authorized request.

9. DELETION AND RETURN OF PERSONAL DATA

9.1 Upon Customer's request, or upon termination or expiry of this DPA, Supplier shall destroy or return to Customer all Personal Data and Personal Information (including copies) in its possession or control, if any (including any Personal Data and Personal Information processed or controlled by its Sub-Processors). This requirement shall not apply to the extent that Supplier is required by any applicable law to retain some or all of the Personal Data or Personal Information, or with respect to Personal Data or Personal Information it has archived on back-up systems, in which event Supplier shall protect the Personal Data and Personal Information from any further processing except to the extent required by such law.

10. LIABILITY

10.1 The liability of Customer and each Authorized Affiliate pursuant to this DPA and the Model Clauses shall be several and the other Customer companies shall not be liable for any liability of such Customer company incurred under this DPA or the Model Clauses.

10.2 In any event, no Supplier or Supplier Affiliate shall be able to claim more than once for the same loss or damage when such a claim has already been made by such Supplier company against one of the other Customer companies.

10.3 The liability of each Supplier and each Supplier Affiliate pursuant to this DPA and the Model Clauses shall be several and the other Supplier companies shall not be liable for any liability of such Supplier company incurred under this DPA or the Model Clauses:

10.4 In any event, no Customer of Authorized Affiliate shall be able to claim more than once for the same loss or damage when such a claim has already been made by such Customer company against one of the other Supplier companies.

11. GENERAL

11.1 The obligations placed upon the Parties under this DPA shall survive so long as Supplier or its Sub-Processors processes Personal Data or Personal Information on behalf of Customer. The provisions contained in this DPA and its attachments, annexes, exhibits and schedules that by their context are intended to survive termination or expiration will survive accordingly.

11.2 This DPA may not be modified except by a subsequent written instrument signed by both Parties.

11.3 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

11.4 Except for the changes made by this DPA, the Contracts shall remain unchanged and in full force and effect. In the event of any conflict or inconsistency between this DPA and any other term or terms of the Contracts, this DPA shall prevail in respect of the subject matter (i.e. the protection of Personal Data or Personal Information). This Agreement including annexes, schedules, exhibits and the like, together with the Contracts, constitute the entire, final, exclusive and complete agreement with respect to such subject matter.

11.5 Clause headings and other headings in this DPA are for convenience of reference only and shall not constitute a part of or otherwise affect the meaning or interpretation of this DPA. Attachments, annexes, exhibits and schedules to this DPA shall be deemed to be an integral part of this DPA to the same extent as if they had been set forth verbatim herein.

11.6 This DPA shall be governed by and construed in all respects in accordance with the governing law and jurisdiction provisions set out in the Contract that is the Master Subscription Agreement, unless required otherwise by Applicable Privacy Laws.

11.7 Nothing in this DPA shall be deemed to: (a) constitute a Customer company the agent of any Supplier company, nor authorise a Customer company to make or enter into any commitments for or on behalf of any Supplier company; or (b) constitute a Supplier company the agent of any Customer company, nor authorise a Supplier company to make or enter into any commitments for or on behalf of any Customer company; or (c) create a partnership, joint venture or other relationship.

11.8 Each Party warrants that it has authority to act on behalf of itself and its Affiliated companies, including such companies that may be added as a Party to this DPA by either Party.

11.9 This DPA may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The Parties may sign and deliver this DPA by email transmission.

By signing below, each party acknowledges that it has read and understood the terms of this DPA and agrees to be bound by them.

NOTE: Customer is requested to review and complete Annex A following this page to designate the categories of Personal Data and Personal Information to be covered. If Customer elects to sign this Agreement without completing Annex A then Customer is hereby representing that NONE of the "Types of Personal Data and Personal Information Processed" apply to Customer or this Agreement, and Supplier is entitled to rely on this representation.

[Keywords]	**[INSERT NAME OF CUSTOMER SIGNING ENTITY]**
By:________________________________	By:________________________________
Name:______________________________	Name:______________________________
Title:_______________________________	Title:_______________________________
Effective Date:______________________	Date:_______________________________

ANNEX A

DETAILS OF THE PROCESSING

Customer as the Controller:

As between the parties and for the purposes of this DPA, Customer, its Customer Affiliates or their respective customers, consumers, suppliers or other business partners shall be the Controller of certain Personal Data and Personal Information provided to Supplier to provide the Services.

Nature of Services provided by Supplier:

Supplier will process Personal Data and Personal Information as necessary to perform the Services pursuant to the Contracts, namely by enabling and authorizing Customer to transfer data using Supplier's proprietary software-defined wide area network (SD-WAN), and as further specified in the Contracts, and as may instructed by Customer in its use of the Services, it being understood that the Services do not, and in the ordinary course of providing Services Supplier does not, access Personal Data, Personal Information or any personally identifiable information, but instead provides Supplier's SD-WAN over which data is carried.

Duration of processing:

Subject to Section 9 of the DPA, Supplier will process Personal Data and Personal Information for the duration of the Contracts, unless otherwise agreed upon in writing.

Types of Customer Personal Data processed:

Supplier will process, on behalf of Customer, the following types of Personal Data and Personal Information:

Please check all that apply. *If any of the examples apply, check the box for that Data Category unless instructions provide otherwise.*

	Data Category	Data Category/Examples of Personal Data/Information Category
□	**Name**	First Name, Last Name/Surname, Middle Name, Full Name, Maiden Name
□	**Contact Details Professional/Work**	Professional/Work email address, postal address, fixed or mobile number
□	**Contact Details – Person**	Personal email address, home postal address, personal fixed or mob number

❒	**Customer's Business Da Technologies and Produ / Projects**	Any digital or digitized information used in Customer's business to produce products or services, and the products and services themselves, and otherwise used in conduct of business or associated activities.
❒	**Government Identificati**	National ID (other than SSN), visa/work permit information, citizensh information, residency information *Check this box if any of the examples above apply. Check the boxes below only if they apply.*
	❒	**Passport Number/Passport Information**
	❒	**Social Security Number (SSN)**
	❒	**Driver's License information**
❒	**Financial Information**	*Check specific boxes below as applicable or check this box if all of the below apply.*
	❒	**Bank account information**
	❒	**Credit card information**
❒	**Authentication Information**	Login credentials (username/password), validation details, secret questions
❒	**Background Information Che**	*Check specific boxes below as applicable or check this box if all of th below apply.*
	❒	**Civil action information**
	❒	**Criminal conviction history details (also mark in Special Categories**
	❒	**"Pass/Fail" criminal conviction results (also mark in Special Categories)**
	❒	**Drug/alcohol testing information (also mark in Special Categories)**
	❒	**"Pass/Fail" drug/alcohol testing information (also mark in Special Categories)**
	❒	**Credit check information**
	❒	**Driver Record information**

❒	**Benefits/Entitlement**	Benefits enrollment information, beneficiary designations, spouse/dependent information
❒	**Customer Information**	Incorporated Customer registration, Customer Tax ID number
❒	**Consent**	Consent tracking information, preferences
❒	**Employment Information**	Absence records (if for illness/medical reasons, mark in Special Categories), employee complaints/grievances, employee ID number employment contracts/offer letters, job title, job application details training records, salary information, hours worked, workers' compensation claims
❒	**Employee Performance**	Performance appraisals, performance improvement plans, disciplina records
❒	**Job Search, Resume/ Related Information**	Resume/CV, employment history, professional memberships, professional awards, education and training/certification history, security clearance information, references and reference informatio
❒	**Media**	Pictures, CCTV
❒	**Personal Attributes**	Gender, family and marital status, military/veteran's status, hair col eye color, height, weight, personal activities/interests (beyond wha listed in the resume/CV)
❒	**Personal Identification**	Place of birth, date of birth, vehicle registration, license plate information *Check this box if any of the examples above apply. Check the boxes below if they specifically apply.*
	❒	**Date of birth**
	❒	**Place of birth**
❒	**Personality Test Results**	e.g., Myers-Briggs, Harrison Assessment
❒	**Skills/Competency Test Results**	
❒	**Signature**	
❒	**Technical Information**	IP address, pages visited, unique device ID, operating system information, browser type, links clicked, geo-location information, internet surfing behavior or user preferences using persistent cooki

❒	**Travel Information**	Hotel/airline/car rental membership information, travel itinerary details, travel preferences including dietary restrictions (if dietary restriction information, also mark in Special Categories)

Special Categories of Customer Personal Data and Personal Information (if applicable):

Supplier will process on behalf of Customer the following Special Categories of data (please select all the apply or if none, select "None of the above"):

❒ Racial or ethnic origin information
❒ Political opinion information
❒ Religious or philosophical belief information
❒ Trade-union/Works Council membership information
❒ Health or sex-life information (e.g., information about sick leave/absences, medical information)
❒ Criminal Conviction Information
❒ Biometric information (e.g., fingerprints, retinal scans)
❒ Genetic information

OR

❒ None of the above

Categories of Data Subjects:

Supplier will process on behalf of Customer, its Authorized Affiliates or their respective customers, consumers, suppliers or other business partners Personal Data and Personal Information belonging to the following Data Subjects and Consumers:

[Please check all that apply]

❒ Internal Employees
❒ Client Billable Employees
❒ Applicants
❒ California Resident Consumers
❒ Households of Such Consumers
❒ Devices Possessed or Controlled by Such Consumers
❒ Sole Trader/Sole Proprietor/1099-Unincorporated
❒ Incorporated Independent Contractors
❒ Permanent Placement/Search Candidates
❒ Customers
❒ Customer's Client/End User/Employee
❒ Suppliers

□ Children

Nature and Purposes or Processing

As a Processor, Supplier shall process Personal Data and Personal Information only for the following purposes: (i) the performance of the Services described in more detail in the Contracts; (ii) processing to perform any steps necessary for the performance of the Contracts; and (ii) processing to comply with other reasonable instructions provided by Customer that are consistent with the terms of the Contracts. **However, it is understood that the Services do not, and in the ordinary course of providing Services Supplier does not, access Personal Data or Personal Information or any personally identifiable information, but instead provides Supplier's SD-WAN over which data is carried.**

~~~~~~~~~~~~~~~

ANNEX B

SECURITY MEASURES

Supplier agrees to implement the following Security Measures as referenced in Paragraph 5.2 of the DPA. Supplier, at its option, may attach or reference additional information regarding its Security Measures.

Physical Access Control

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process Personal Data or Personal Information. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Supplier and do not gain access to the Personal Data or Personal Information themselves.

System Access Control

Data processing systems must be prevented from being used without authorization.

Data Access Control

Persons entitled to use a system that is processing Personal Data or Personal Information shall gain acces only to the data to which they have a right of access, and Personal Data and Personal Information must n be read, copied, modified or removed without authorization in the course of processing.

Data Transmission Control

Personal Data and Personal Information must not be read, copied, modified or removed without authorization during transfer or storage, and it shall be possible to establish to whom Personal Data and Personal Information was transferred.
~~~~~~~~~~~~~~~

Data Entry Control

The Supplier shall be able retrospectively to examine and establish whether and by whom Personal Data and Personal Information have been entered into data processing systems, modified or removed.

Job Control

Personal Data and Personal Information being processed in the performance of the Services for the Customer shall be processed solely in accordance with the Contracts and in accordance with the instructions of the Customer.

Availability Control

Personal Data and Personal Information shall be protected against disclosure, accidental or unauthorized destruction or loss.

Organizational Requirements

The internal organization of Supplier shall meet the specific requirements of data protection. In particular Supplier shall take technical and organizational measures to avoid the accidental mixing of Personal Data, the mixing of Personal Information, or both.

Description of the technical and organizational security measures implemented by Supplier as the data importer in accordance with Clauses 4(d) and 5(c) of Model Clauses set forth in Schedule 1.9:

Technical and organizational security measures will be implemented as applicable to the Personal Data and Personal Information processed and as appropriate in accordance with commercially available best practices. The measures will be continuously reviewed to ensure they are appropriate to the profile of the data being processed. These measures include:

- Integrated DDoS protection with hybrid cloud attack mitigation, network edge security, Internet traffic cloud security, and virtual firewalls.
- The hybrid DDoS protection integrates always-on detection and mitigation (on-premises or in the cloud) with cloud-based volumetric DDoS attack prevention, scrubbing, and 24x7 Emergency Response Team (ERT) support.
- Network edge security provides advanced perimeter security solutions that are built into Customer's SD-WAN appliance (the "ANAP"). The ANAP includes a virtual stateful firewall with an on-premises next-generation firewall.
- The Internet traffic cloud security utilizes combined solutions that do not require additional on-premises hardware, appliances, or software. This includes a cloud-based security infrastructure for global enterprises to create and deploy consistent security policies across the entire organization together with secure local Internet breakouts for all ports and protocols, without appliances.
- Virtual firewall security is provided for enterprises with heavy deployments of Amazon Web Services (AWS) and Microsoft Azure, by providing an additional layer of security hosted in cloud computing environments to protect data and applications hosted in cloud instances.

~~~~~~~~~~~~~~~~

ANNEX C

LIST OF SUPPLIER'S SUB-PROCESSORS

List all Sub-Processors here

(Including any and all Supplier Affiliates processing Personal Data or Personal Information).

Name	Nature of processing	Territory(ies)
~~~~~~~~~~~~~~~~

SCHEDULE 1.8

Model Clauses – EEA Controller to Non-EEA Controller

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers):

Data transfer agreement between

(name)

(address and country of establishment)

hereinafter “data exporter”

and

(name)

(address and country of establishment)

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

(a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) “the data exporter” shall mean the controller who transfers the personal data;

(c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

(d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfill the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfill its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions (1) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data (2), or

(iii) the data processing principles set forth in Annex A."

Data importer to indicate which option it selects:

Initials of data importer:

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law."

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

(1) "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

(2) However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected."

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required.

In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred."

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated:

FOR DATA IMPORTER FOR DATA EXPORTER

________________________ __________________________

________________________ __________________________

ANNEX A

(to Model Clauses, Controller-To-Controller)

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties."

or

(b) where otherwise provided by the law of the data exporter.

ANNEX B

(to Model Clauses, Controller-To-Controller)

DESCRIPTION OF THE TRANSFER

(Completed by the parties)

LLUSTRATIVE COMMERCIAL CLAUSES (OPTIONAL)

Indemnification between the data exporter and data importer:

“The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the “indemnified party(ies)”) promptly notifying the other party(ies) (the “indemnifying party(ies)”) of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim."

Dispute resolution between the data exporter and data importer (the parties may of course substitute any other alternative dispute resolution or jurisdictional clause):

“In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be [ ]. The number of arbitrators shall be [ ].”

Allocation of costs:

“Each party shall perform its obligations under these clauses at its own cost.”

Extra termination clause:

“In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter’s choice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonably objected to by the data importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours.”

SCHEDULE 1.9

Model Clauses – EEA Controller to Non-EEA Processor

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

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

Name of the data exporting organisation: ________________________________ on behalf of itself and its Affiliates
Address: ____
Tel.: N/A; fax: N/A ; e-mail: _______________@______________.com
Other information needed to identify the organisation: N/A

…………………………………………………………

(the data exporter)

And

Name of the data importing organisation: Aryaka Networks, Inc.

Address: 1800 Gateway Drive, Suite 200, San Mateo, CA 94404
Tel.: 408-273-8420; fax: N/A; e-mail: legal@aryaka.com
Other information needed to identify the organisation: N/A

……………………………………………………………

(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 Annex A to the DPA.

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.

EXHIBIT C

LINK MONITORING

If Aryaka receives an executed Letter of Authorization (LOA) from Customer, Aryaka will proceed with the following link monitoring services as part of the Last Mile Circuit Management:

- Monitor the last mile link 24x7x365 by pinging between Aryaka's POP and the end-user device.
- Pings occur once per second and Aryaka reports average packet loss and latency by the minute.
- Aryaka monitoring team to be alerted when the rolling average for either latency or packet loss exceeds the applicable thresholds set forth in the SLA.
- As specified in the Last Mile Management SLA terms, in the event of an incident where latency or packet loss exceed the applicable thresholds, or the last mile tunnel becomes unavailable, Aryaka will follow up with Customer, Customer's Internet Service Provider (ISP), or both.
- In working with each ISP, Aryaka will comply with any incident resolution priority or escalation matrix provided by the ISP.

Aryaka disclaims responsibility for any ISP failing to restore service in accordance with the ISP's SLA. Aryaka is not responsible for procuring ISP links or other non-Aryaka links for Customer.

EXHIBIT D
SMART ACCESS TABLES

TABLE 1 – DATA USAGE ALLOCATION SCHEDULE

User Pack	Data Usage Allowed (Limit)
50	100 GB
100	200 GB
250	500 GB
500	1 TB
1000	2 TB
>1000	No Limit

TABLE 2 – LIST OF POPS FOR DELIVERY OF SMART ACCESS SERVICES

San Jose	Ashburn
Miami	Chicago
Dallas	London
France	Amsterdam
Johannesburg	Dubai
Seoul	Tokyo
Beijing	Shanghai3
Sydney	Hong Kong
Taipei1	Tel Aviv
Sao Paulo	Bangalore
Chennai	Delhi
Frankfurt	Los Angeles
Mumbai	Seattle
Singapore	Tokyo
Toronto	