DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") forms part of the Agreement between Aryaka and Customer (the "**Agreement**") under which Aryaka provides the Services to Customer. Capitalized terms used but not defined in this DPA shall have the meaning as set forth in the Agreement.

1. DEFINITIONS

1.1 "**Data Controller**" means the entity which, alone or jointly with others, determines the purposes and means of Processing of Personal Information.

1.2 "**Data Processor**" means the entity which Processes Personal Information on behalf of the Data Controller.

1.3 "**Data Protection Laws**" mean all laws applicable to the Processing of Personal Information.

1.4 "**Data Subject**" means any individual about whom Personal Information may be Processed under this DPA.

1.5 "**Personal Information**" or "**Personal Data**" means Customer Data that relates to an identified or identifiable natural person, which Aryaka Processes on Customer's behalf through the Services.

1.6 "**Process**" or "**Processing**" means any operation or set of operations performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of Personal Information.

1.7 "**Security Incident**" means a breach of security of the Services leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Information transmitted, stored or otherwise Processed by Aryaka under this DPA.

2. Instructions. Customer acknowledges that, in the ordinary course of providing Services, Aryaka does not require access to Personal Information, but instead provides a proprietary software-defined wide area network (SD-WAN) over which data is carried. Customer will be solely responsible for complying with its obligations under Data Protection Laws with respect to the Processing of Personal Information, including for providing any necessary notices to, and obtaining any necessary consents from, Data Subjects or other individuals with respect to the Processing of Personal Information. To the extent Aryaka Processes Personal Information on behalf of Customer, Aryaka will Process such Personal Information in accordance with the Agreement or other documented instructions of Customer (whether in written or electronic form) provided in accordance with the Agreement, or as otherwise required by applicable law. For clarity, Aryaka will not retain, use, or disclose Personal Information for any purpose other than providing Services to Customer in accordance with the Agreement, including without limitation for any commercial purpose other than providing such services to Customer, or as required by applicable law. Without limiting the foregoing, in no event will Aryaka sell such Personal Information to any third party. Aryaka certifies that it understands and will comply with the foregoing restrictions.

3. Confidentiality. Aryaka will require its personnel to protect the confidentiality of Personal Information.

4. Security. Aryaka will maintain reasonable administrative, physical and technical safeguards designed to protect the security, confidentiality and integrity of Customer Data in or on the Aryaka Network against unauthorized loss, destruction, alteration, access, or disclosure, including the measures listed in Appendix 2.

5. Security Incident. Aryaka will notify Customer without undue delay, and in any event within forty-eight (48) hours, in the event Aryaka discovers that a Security Incident has occurred, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. At Customer's request and considering the nature of the processing and the information available to Aryaka, Aryaka will provide reasonable assistance and cooperation to Customer with respect to any notifications that Customer is legally required to provide to affected Data Subjects or regulators with respect to such a Security Incident. Aryaka reserves the right to charge a reasonable fee to Customer for such requested assistance, to the extent permitted by applicable law.

6. Data Subject Requests. Aryaka will promptly notify Customer, unless prohibited by applicable law, if Aryaka receives: (i) any requests from a Data Subject with respect to Personal Information Processed by Aryaka, including but not limited to opt-out requests, requests for access and/or rectification, blocking, erasure, requests for data portability, and all similar requests, and will not respond to any such requests unless expressly authorized to do so by Customer; or (ii) any complaint relating to the Processing by Aryaka of Personal Information, including allegations that such Processing infringes on a Data Subject's rights. For avoidance of doubt, Customer is responsible for responding to Data Subject requests. At Customer's request and taking into account the nature of the processing, Aryaka will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of obligations Customer may have under applicable Data Protection Laws to respond to such Data Subject requests. Aryaka reserves the right to charge a reasonable fee to Customer for such requested assistance, to the extent permitted by applicable law.

7. Subprocessors. Customer agrees that Aryaka may disclose Personal Information to its subcontractors for purposes of providing Services to Customer ("**Subprocessors**"), provided that Aryaka will impose substantially similar obligations on its Subprocessors regarding the security and confidentiality of Personal Information as those set forth in this DPA. Aryaka will, upon request, (a) make available to Customer a list of its Subprocessors and provide Customer with a mechanism to receive notice of any changes to this list. Aryaka will be liable for the acts or omissions of any Subprocessors to the same extent as if the acts or omissions were performed by Aryaka.

8. Data Location. In connection with the performance of the Agreement, Aryaka may transfer Personal Information to various locations, which may include locations both inside and outside of the European Economic Area ("**EEA**"). To the extent such transfer involves a transfer of Personal Information originating from Customer in the EEA or Switzerland to Aryaka or its Subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision, the Parties agree that the European Union Standard Contractual Clauses (Controller to Processor) currently available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087, which are hereby incorporated into this DPA by reference, will apply to such transfer, and such transfer is described in Appendix 1.

9. Audit. Upon Customer's request, Aryaka will make available to Customer up to once per year (a) a copy of a third-party assessment, such as a Service Organization Controls 1, Type 2 report or comparable report ("**Third-Party Report**"), if Aryaka has obtained such a Third-Party Report or (b) if Aryaka has not obtained a Third-Party Report, responses to any written questions that Customer may reasonably submit for purposes of verifying Aryaka's compliance with this Agreement ("**Written Responses**"). Any such

Third-Party Reports and Written Responses will be Aryaka's confidential information and may not be disclosed without Aryaka's prior written consent, except as required by law. If Aryaka responds to Customer's request by providing Written Responses rather than a Third-Party Report, and Customer reasonably determines following receipt of Aryaka's Written Reponses that further assessment is required by law, Customer may request upon 30 days' prior notice to perform a review at Customer's own expense, with a scope to be mutually agreed by the parties, of relevant policies, procedures, and related documentation of the Services, to the extent that such review does not compromise confidentiality obligations to any of Aryaka's other customers.

10. Return or Disposal. Upon request, Aryaka will promptly delete Customer Data from its systems, unless applicable law requires storage of the Customer Data.

Appendix 1
Description of Transfer

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

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

Data exporter
The data exporter is: Customer, as defined in the Agreement, which uses the global networking services provided by Aryaka.

Data importer
The data importer is: Aryaka, which provides global networking services via Aryaka's proprietary software-defined wide area network (SD-WAN) over which data is carried.

Data subjects
The personal data transferred concern the following categories of data subjects: Customer decides, in its sole discretion, what data to transmit through Aryaka's services. Depending on the data the Customer processes and transmits, this may include personal data about data subjects such as its current and former employees, contractors, consumers and customers, suppliers, and other business partners or business contacts. Notwithstanding the forgoing, in the Agreement with the Customer, Customer warrants that all of its activities with respect to the Services shall be in accordance with applicable law.

Categories of data
The personal data transferred concern the following categories of data (please specify): Customer decides, in its sole discretion, what data to transmit through Aryaka's services. Depending on the data the Customer processes and transmits, such data may include data subjects' contact information (such as name, email, telephone numbers), human resource information (such as employee names, address, salary, job title, position, responsibilities), and personal data contained in commercial records (such as credit card information, and other financial and invoicing data). Notwithstanding the forgoing, in the Agreement with the Customer, Customer warrants that all of its activities with respect to the Services shall be in accordance with applicable law.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data: Customer decides, in its sole discretion, what data to transmit through Aryaka's services. Aryaka does not require or seek to receive any special categories of data. Notwithstanding the forgoing, in the Agreement with the Customer, Customer warrants that all of its activities with respect to the Services shall be in accordance with applicable law.

Processing operations
The personal data transferred will be subject to the following basic processing activities: Aryaka will process Personal Information as necessary to perform the Services pursuant to the Agreement, namely by enabling Customer to transfer data using Aryaka's proprietary software-defined wide area network (SD-WAN), as further specified in the Agreement, it being understood that, in the ordinary course of providing Services, Aryaka does not require access Personal Information, but instead provides Aryaka's SD-WAN over which data is carried. Notwithstanding the forgoing, in the Agreement with the Customer, Customer warrants that all of its activities with respect to the Services shall be in accordance with applicable law.

Appendix 2
Security Standards

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

Aryaka maintains various policies, standards and processes designed to secure Personal Information and other Customer Data within Aryaka's services. Following is a description of some of the core technical and organisational security measures implemented by Aryaka.

Physical Access Controls

Aryaka implements and maintains measures designed to prevent unauthorized persons from gaining physical access to Aryaka locations that house data processing equipment used to process Customer Data.

Technical Access Controls

Aryaka implements and maintains measures designed to prevent unauthorized persons from gaining access to Aryaka's data processing systems, including:

- Integrated DDoS protection with hybrid cloud attack mitigation, network edge security, Internet traffic cloud security, and virtual firewalls;
- Hybrid DDoS protection integrating detection and mitigation (on-premises or in the cloud) with cloud-based volumetric DDoS attack prevention, scrubbing, and 24x7 Emergency Response Team (ERT) support; and
- Network edge security providing advanced perimeter security solutions that are built into Customer's SD-WAN appliance.

Data Access Controls

Aryaka implements and maintains measures to restrict access to its data processing system to individuals who need such access within the scope and to the extent covered by their respective access permission (authorization) and takes measures to prevent Customer Data from being read, copied or modified or removed without authorization.

Input Controls

Aryaka implements and maintains measures designed to prevent Customer Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof.

Job Controls

Arkaya implements and maintains measures designed to ensure that Customer Data being processed in the performance of the Services for the Customer is processed solely in accordance with the Agreement.

Availability Controls

Aryaka implements and maintains measures designed to protect Customer Data against disclosure, accidental or unauthorized destruction or loss.