DATA PROTECTION ADDENDUM FOR EARLY ACCESS SERVICES

This Data Protection Addendum for Early Access Services ("**EADPA**") forms part of the Design Partnership Program Early Access Agreement between Aryaka and Customer (as applicable, the "**Agreement**") under which Aryaka provides the Early Access Services to Customer. By executing the Agreement, Customer agrees to be bound by the terms of this DPA as in effect at the time of execution. Aryaka may update this DPA from time to time. Continued use of the Early Access Services following the effective date of any update constitutes Customer's acceptance of the revised DPA. Capitalized terms used but not defined in this EADPA will have the meaning set forth in the Agreement.

1. DEFINITIONS

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

1.2 **"Data Protection Laws"** means all laws applicable to the respective Party's Processing of Personal Data.

1.3 **"Data Subject"** means any individual about whom Personal Data may be Processed under this EADPA.

1.4 **"Early Access Services"** means pre-release, beta, pilot, or experimental features, products, or services made available by Aryaka to Customer under the Agreement for evaluation, testing, and feedback purposes.

1.5 **"Feedback Data"** means suggestions, enhancement requests, recommendations, bug reports, or other feedback provided by Customer in connection with the Early Access Services.

1.6 **"Personal Data"** means information that relates to an identified or identifiable natural person that is provided by the Customer to the Early Access Services.

1.7 **"Process"** or **"Processing"** means any operation or set of operations performed on Personal Data or on sets of Personal Data, 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 Data.

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

1.9 **"Production Data"** means Customer Data generated in or derived from Customer's live production environment, including network traffic, configuration data, user information, and any Personal Data contained therein.

1.10 **"Transit Data"** means Personal Data contained within Customer's network traffic that passes through the Aryaka network in connection with the Early Access Services, where Aryaka's role is limited to routing and delivering such traffic.

2. RELATIONSHIP BETWEEN THE PARTIES

2.1 Customer and Aryaka have entered into an Agreement for Early Access Services. The Parties acknowledge that Customer is a Controller for purposes of the Agreement and Aryaka is a Processor. The Parties will Process Personal Data in accordance with the Agreement and applicable Data Protection Laws.

2.2 Customer's Transit Data may pass through the Aryaka network in connection with the Early Access Services. Personal Data contained within such Transit Data is not accessed, used, monitored, stored, or transferred by Aryaka except to the extent strictly necessary to route and deliver such traffic. Transit Data that Aryaka does not access or use beyond network routing is not considered Personal Data Processed under this EADPA. To the extent that any Transit Data is incidentally exposed to or collected by Aryaka through the operation of the Early Access Services (including through security inspection, logging, or caching functions), such data will be treated as Personal Data subject to the terms of this EADPA.

3. CUSTOMER OBLIGATIONS

Customer will provide only Personal Data that is adequate, relevant, and reasonably necessary for Aryaka to perform the Early Access Services. Customer represents and warrants that its collection of Personal Data and disclosure to Aryaka complies with all applicable Data Protection Laws.

4. INSTRUCTIONS

Aryaka will Process the Personal Data only: (i) in accordance with Customer's instructions as documented in the Agreement and further described in Annex IB; (ii) for the purposes of providing and operating the Early Access Services for Customer's evaluation and testing; (iii) for diagnosing, troubleshooting, and resolving issues identified during testing; (iv) for improving and developing the Early Access Services based on performance analysis and Customer Feedback Data; (v) for training, improving, and developing Aryaka's artificial intelligence and machine learning models and algorithms, provided that any Personal Data used for such purposes is first aggregated or de-identified in accordance with applicable Data Protection Laws such that it no longer constitutes Personal Data; (vi) for improving and developing Aryaka's products and services generally, using only aggregated or de-identified data derived from the Early Access Services; and (vii) as needed to comply with applicable law, provided that Aryaka will not be required to act on any Customer instruction that could (in the reasonable opinion of Aryaka) cause Aryaka to breach applicable law. Aryaka will inform Customer if it believes that any Customer instructions regarding Personal Data Processing would violate applicable Data Protection Law.

5. USE OF PRODUCTION DATA

5.1 The Parties acknowledge that Customer's Production Data may be routed through or Processed by the Early Access Services for testing and evaluation purposes. Production Data may include data of all categories and types depending on Customer's network traffic and use of the Early Access Services. This EADPA applies only to Personal Data contained within Production Data; it does not govern Production Data that does not constitute Personal Data. To the extent that Personal Data within Production Data is incidentally exposed to or collected by Aryaka through the operation of the Early Access Services (including through security inspection, logging, or caching functions), such data will be treated as Personal Data subject to the terms of this EADPA, consistent with Section 2.2.

5.2 Aryaka will disclose to Customer any known limitations or security gaps in the Early Access Services that may affect the integrity or confidentiality of Production Data prior to onboarding. Aryaka will update this disclosure throughout the Agreement term.

5.3 Customer is advised to avoid sharing Personal Data through the Early Access Services to the extent possible. Where Customer determines that the use of Personal Data is necessary for the testing objectives, Customer will ensure that such data is limited to the minimum categories and volume required and that appropriate internal approvals have been obtained prior to disclosure to Aryaka. Where feasible, the Parties will prioritize the use of anonymized, pseudonymized, or synthetic data in lieu of Production Data containing Personal Data.

6. FEEDBACK DATA

Feedback Data that does not contain Personal Data is not subject to this EADPA. Where Feedback Data incidentally contains Personal Data, Aryaka will extract and retain only the non-personal elements and will delete the Personal Data component promptly.

7. SECURITY

7.1 Aryaka will take reasonable steps to implement appropriate technical and organizational measures designed to protect Personal Data Processed through the Early Access Services against anticipated threats or hazards to its security, confidentiality, or integrity. Aryaka will ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.2 Aryaka will maintain logical separation of the Early Access environment from Aryaka's production infrastructure, unless the nature of the test requires integration, in which case isolation controls will be documented.

7.3 A description of the technical and organizational security measures implemented by Aryaka is set forth in Annex II.

8. DATA BREACH

Aryaka will notify Customer without undue delay whenever Aryaka learns that there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed through the Early Access Services (each, a "**Data Breach**"), unless prohibited by applicable law or otherwise instructed by law enforcement or a supervisory authority. Taking into account the nature of Processing and the information available to Aryaka, Aryaka will take reasonable steps to assist Customer at Customer's

reasonable request in complying with Customer's notification obligations regarding data breaches as required by applicable law. Aryaka reserves the right to charge a reasonable fee to Customer for any requested assistance.

9. RETURN OR DISPOSAL

9.1 Within thirty (30) days of termination or expiration of the Agreement, Customer may request that Aryaka destroy or return all Personal Data Processed through the Early Access Services, unless applicable law requires storage of the Personal Data by Aryaka.

9.2 Any derived, aggregated, or anonymized data sets created from Production Data during the Early Access period will be permanently stripped of all identifiers before Aryaka retains them for product development purposes.

10. AUDITS; INQUIRIES

Upon Customer's reasonable request (to be exercised no more than once per year, unless a Data Breach has occurred or as required more frequently by a supervisory authority) Aryaka will promptly make available to Customer all information in its possession necessary to demonstrate Aryaka's compliance with its obligations under this EADPA and will allow for and contribute to reasonable audits. All information provided will be Aryaka's Confidential Information and may not be disclosed without Aryaka's prior written consent, except as required by applicable law.

11. SUBCONTRACTING

11.1 Customer authorizes Aryaka to transfer Personal Data to sub-processors for purposes of providing the Early Access Services to Customer. Aryaka will maintain a list of the sub-processors. A current list of sub-processors is included in Annex III. Aryaka will provide Customer fourteen (14) days' prior notice when adding a sub-processor to this list and the opportunity to object to such addition. If Aryaka does not receive an objection within fourteen (14) days of the notice, the sub-processor is deemed to be accepted by Customer.

11.2 If Customer objects to a new sub-processor and the Parties cannot resolve the objection within thirty (30) days, Customer may terminate the Agreement upon written notice to Aryaka.

11.3 Aryaka will enter into an agreement with each sub-processor that includes data protection terms similar to this EADPA.

12. ARYAKA ASSISTANCE

At Customer's reasonable request and taking into account the nature of the Processing, Aryaka will take reasonable steps to assist Customer with Customer's obligation to respond to Data Subjects' requests to exercise their rights under applicable law by taking appropriate technical and organizational measures. Taking into account the nature of the Processing and the information available to Aryaka, Aryaka also will assist Customer at Customer's reasonable request in meeting its compliance obligations regarding carrying out data protection impact assessments and related consultations of supervisory authorities. Aryaka reserves the right to charge a reasonable fee to Customer for such requested assistance.

13. US STATE PRIVACY LAWS

To the extent Aryaka Processes Personal Data of residents of California or other US states with applicable consumer privacy laws, Aryaka will not: (a) sell or share such Personal Data; (b) retain, use, or disclose such Personal Data outside of Aryaka's direct business relationship with Customer or for any purpose other than as specified in this DPA; or (c) combine such Personal Data with personal information received from other sources, except as permitted by applicable law. Aryaka will notify Customer if Aryaka determines it can no longer meet its obligations under applicable US state privacy laws. Customer has the right to take reasonable steps to ensure Aryaka uses Personal Data in a manner consistent with applicable law and to stop and remediate any unauthorized use. Aryaka certifies that it understands and will comply with the foregoing restrictions.

14. DATA TRANSFERS

14.1 Where the transfer of Personal Data from Customer (as data exporter) to Aryaka (as data importer) constitutes a restricted transfer under applicable Data Protection Laws, such transfer will be subject to the following safeguards:

14.1.1 EU/EEA: The EU Standard Contractual Clauses (Module 2, Controller to Processor) adopted under Commission Implementing Decision (EU) 2021/914, incorporated herein by reference and completed using the Annexes to this EADPA, will apply. In Clause 9, Option 2 (general written authorization) applies in accordance

with Section 11. The optional language in Clause 11 is excluded. The EU SCCs will be governed by the laws of the Netherlands, with disputes resolved by the courts of the Netherlands.

14.1.2 Switzerland: The EU SCCs as described in Section 14.1(a) will apply, modified so that references to the GDPR are read as references to the Swiss Federal Act on Data Protection (FADP), governed by the laws of Switzerland, with the Swiss Federal Data Protection and Information Commissioner as the competent supervisory authority.

14.1.3 United Kingdom: The UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022), available at https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf, including Part 2 Mandatory Clauses, is incorporated herein by reference. Either Party may end the UK Addendum in accordance with Section 19 of the Mandatory Clauses.

14.2 The safeguards in Section 14.1 will not apply to the extent a transfer is covered by an adequacy decision adopted by the competent authority with jurisdiction over Customer.

15. ARTIFICIAL INTELLIGENCE

The Early Access Services may incorporate artificial intelligence or machine learning technologies. Each Party will comply with all applicable laws and regulations governing the development, deployment, or use of artificial intelligence in connection with the Early Access Services, including applicable transparency and disclosure obligations. Customer acknowledges and agrees that Aryaka may use aggregated or de-identified data derived from the Early Access Services, including usage patterns, performance metrics, telemetry data, and technical logs, to train, improve, and develop Aryaka's artificial intelligence and machine learning models, algorithms, and related products and services. Aryaka will ensure that any data used for such purposes has been processed in accordance with Section 9.2 such that it does not identify or permit re-identification of Customer or any Data Subject. Aryaka's rights under this Section 15 will survive termination or expiration of the Agreement. In the event that new legislation or regulations are enacted that specifically govern the use of artificial intelligence, the Parties will cooperate in good faith to review and, if necessary, amend this EADPA to ensure continued compliance.

16. LIABILITY

16.1 Customer acknowledges that Early Access Services are pre-release, may contain defects, and are not covered by Aryaka's standard service level commitments. This acknowledgment does not diminish Aryaka's data protection obligations under this EADPA or applicable Data Protection Laws.

16.2 Aryaka will remain liable for any Data Breach or non-compliance with this EADPA caused by defects in the Early Access Services or Aryaka's failure to implement the security measures described in Section 7.

16.3 Customer is responsible for its decision to introduce Production Data into the Early Access environment after receiving Aryaka's disclosure under Section 5.2.

17. TERM

This EADPA will remain in effect for the duration of the Agreement and will automatically terminate upon the earlier of: (a) termination or expiration of the Agreement; or (b) Aryaka's cessation of Processing Personal Data under the Early Access Services. Sections 9 (Return or Disposal), 10 (Audits; Inquiries), and 16 (Liability) will survive termination of this EADPA.

18. CONFLICTS; ENFORCEABILITY

If any provision of this EADPA is held to be invalid or unenforceable by any court of competent jurisdiction, such holding will not invalidate or render unenforceable any other provision of this EADPA or any other contract between Customer and Aryaka. This EADPA supplements the Agreement. This EADPA will control in the event of any inconsistency between the Agreement and this EADPA. Any other provisions of or obligations under the Agreement that are otherwise unaffected by this EADPA will remain in full force and effect. If this EADPA, or any actions to be taken or contemplated to be taken in performance of this EADPA, do not or would not satisfy either Party's obligations under the laws applicable to each Party, the Parties will negotiate in good faith upon an appropriate amendment to this EADPA.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: See Order Form or EA Agreement between Customer and Aryaka.

Address: See Order Form or EA Agreement between Customer and Aryaka.

Contact person's name, position and contact details: See Order Form or EA Agreement between Customer and Aryaka.

Activities relevant to the data transferred under these Clauses: See Agreement between Customer and Aryaka.

Role: Controller

Data importer(s):

Name: Aryaka Networks, Inc.

Address: 4699 Old Ironsides Drive, Suite 470, Santa Clara, CA 95054 USA

Contact person's position and contact details: Privacy Officer at privacy@aryaka.com.

Activities relevant to the data transferred under these Clauses: See Agreement between the Parties.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Customer's designated administrators and authorized users of the Early Access Services.

Categories of personal data transferred:

Account registration and contact information of designated administrators and authorized users (name, email address, job title). Technical identifiers necessary to operate the Early Access Services, including IP addresses, device identifiers, and network protocol data. Any additional Personal Data incidentally exposed to or collected by Aryaka through the operation of the Early Access Services (including through security inspection, logging, or caching functions) as described in Section 2.2 of this EADPA

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

None expected. However, any sensitive data that may be visible or exposed in Customer's traffic flowing through the Early Access Services is incidental and dependent on the Customer's use of those services.

The frequency of the transfer*:* Continuous during the EA Agreement term.

Nature of the processing:

Account management, authentication, logging, and performance analysis in connection with the Early Access Services, together with product development analysis, debugging, and feedback analysis.

Purpose(s) of the data transfer and further processing:

Provision of the Early Access Services for evaluation and testing, diagnosing and resolving issues, and improving and developing the Early Access Services based on performance analysis and Customer Feedback Data.

The period for which the personal data will be retained:

Personal Data will be deleted or returned within thirty (30) days of termination of the Agreement, unless applicable law requires storage by Aryaka. Derived or aggregated data will be permanently de-identified before retention.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*:* See description above.

C. COMPETENT SUPERVISORY AUTHORITY

The data protection authority where Customer is located is the competent supervisory authority.

ANNEX II: SECURITY MEASURES

Aryaka maintains various policies, standards, and processes designed to secure Personal Data. Following is a description of core technical and organizational security measures implemented by Aryaka for the Early Access Services.

Physical Access Controls

Aryaka implements and maintains measures designed to prevent unauthorized persons from gaining physical access to Aryaka locations.

Technical Access Controls

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

(a) Hybrid Distributed Denial-of-Service (DDoS) protection integrating detection and mitigation (on-premises or in the cloud) with cloud-based volumetric DDoS attack prevention, and 24x7 Emergency Response Team (ERT) support; and

(b) Network edge security providing advanced perimeter security solutions that are built into Customer's Software Defined Wide Area Network (SD-WAN) appliance.

Data Access Controls

Aryaka implements and maintains measures designed 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).

Job Controls

Aryaka implements and maintains measures designed to ensure that Personal Data being Processed in the performance of the Early Access Services for the Customer is Processed solely in accordance with the Agreement.

Availability Controls

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

Early Access Environment Controls

In addition to the controls above, the Early Access environment will include:

(a) Logical separation from Aryaka's production infrastructure, unless the nature of the test requires integration, in which case isolation controls will be documented and provided to Customer;

(b) Logging and monitoring of access to the Early Access environment;

(c) Regular vulnerability assessments of the Early Access environment during the testing period; and

(d) A documented register of known security limitations or differences from Aryaka's generally available services, maintained and updated throughout the Agreement term.

aryaka

ANNEX III: LIST OF SUB-PROCESSORS

Google Cloud

Use: Sentiment Analysis

Sophos

Use: Data Loss Protection

Webroot

Use: Categorize and score domains and IP addresses

Azure AI (Promptshield)

Use: Input Risk Detection