



DATA PROTECTION ADDENDUM

("Reseller")

This Data Protection Addendum ("**DPA**") forms part of the Reseller Agreement between Aryaka and Reseller (the "**Agreement**") under which Reseller markets and resells Aryaka Services to their customers and potential customers. 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, jointly with others or as a Co-Data Controller, 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 Personal Data that relates to an identified or identifiable natural person that is provided to a Party pursuant to the Agreement.

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 under this DPA.

2. Relationship between the Parties. The Parties acknowledge that Reseller and Aryaka are each a Controller for purposes of the Agreement. In order to fulfill the Agreement, the Parties must provide limited Personal Information to each other, such as business contact information. The Parties will Process such Personal Information in accordance with the Agreement and this DPA or otherwise as required by applicable Data Protection Laws. From time to time, as contemplated in the Agreement, Reseller may provide Aryaka with information about its customers in order to facilitate Reseller's provision of services to those customers. In those instances, Aryaka will only Process Personal Information about Reseller's customers on the documented instructions of Reseller. Each Party will be solely responsible for complying with its obligations under applicable 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. For clarity, Aryaka will not retain, use, or disclose Personal Information for any



purpose other than providing Services to Reseller in accordance with the Agreement, including without limitation for any commercial purpose other than providing such Services to Reseller, or as required by applicable Data Protection Laws. Without limiting the foregoing, in no event will Aryaka sell or share such Personal Information to any third party. Aryaka certifies that it understands and will comply with the foregoing restrictions. Should Aryaka determine that it can no longer meet its obligations under applicable Data Protection Laws, it will promptly inform Reseller.

3. Co-Controllers. When the parties are acting as Co-Data Controllers, each party is an independent Data Controller and shall be individually and separately responsible for complying with the obligations that apply to it as a Data Controller under the Data Protection Laws. When acting as a Co-Controller, each party will individually determine the purposes and means of its Processing of Personal Data.

4. Confidentiality. The parties will require their personnel to protect the confidentiality of Personal Information.

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

6. Security Incident. If a security incident is experienced by either party that compromises Personal Information, the party experiencing the security incident will notify the other party without undue delay, and in any event within forty-eight (48) hours, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Considering the nature of the processing and the information available about the security incident, the party experiencing the security incident will upon the reasonable request of the other party provide reasonable assistance and cooperation to the other party with respect to any notifications that party is legally required to provide to affected Data Subjects or regulators with respect to such a Security Incident. The parties reserve the right to charge a reasonable fee to the other party for such requested assistance, to the extent permitted by applicable law.

7. Data Subject Requests. Given the nature of the Agreement, the parties agree that Reseller is the appropriate party to respond to Data Subject Requests. Aryaka will promptly notify Reseller, 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 Reseller; 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. Reseller is responsible for responding to Data Subject requests. At Reseller's request and taking into account the nature of the processing, Aryaka will assist Reseller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of obligations Reseller may have under applicable Data Protection Laws to respond to such Data Subject requests. Aryaka reserves the right to charge a reasonable fee to Reseller for such requested assistance, to the extent permitted by applicable law.

8. Subprocessors. Both parties agree that the other party may disclose Personal Information to its Processors and subcontractors for purposes of providing Services under the Agreement ("Subprocessors"), provided that both parties will impose substantially similar obligations on its

Subprocessors regarding the security and confidentiality of Personal Information as those set forth in this DPA. Upon request, both parties will (a) make available a list of its Subprocessors and provide a mechanism to receive notice of any changes to this list. Both parties will be liable for the acts or omissions of any Subprocessors to the same extent as if the acts or omissions were performed by the entity that hired the Subprocessor.

9. Data Location. In connection with the performance of the Agreement, either party may transfer Personal Information to various locations, which may include locations both inside and outside of the United Kingdom (“UK”), European Economic Area (“EEA”) or Switzerland. To the extent such transfer involves a transfer of Personal Information originating in the UK, EEA or Switzerland to a location in countries outside the UK, EEA or Switzerland that have not received a binding adequacy decision, the Parties agree that when the parties are acting as Co-Controllers, the European Union Standard Contractual Clauses (Controller to Controller), attached here to at Appendix 1, will apply to such transfer, and such transfer is described in Annex 1. Where the relationship between the parties is that of Controller to Processor, the European Union Standard Contractual Clauses (Controller to Processor), attached hereto at Appendix 2, will apply to such transfer, and such transfer is described in Annex 1.

10. Audit. Upon either party’s request, the other party will make available 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 such Third-Party Report was obtained or (b) if the party has not obtained a Third-Party Report, it will provide responses to any written questions reasonably submitted for purposes of verifying compliance with this Agreement (“**Written Responses**”). Any such Third-Party Reports and Written Responses will be the submitting party’s confidential information and may not be disclosed without that party’s prior written consent, except as required by law. If a party responds to the other party’s request by providing Written Responses rather than a Third-Party Report, and the requesting party reasonably determines following receipt of the Written Responses that further assessment is required by law, the requesting party may request upon 30 days’ prior notice to perform a review at that party’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 Resellers. Reseller shall have the right to stop and take reasonable steps to remediate any unauthorized use of Personal information.

11. Return or Disposal. Upon request at the conclusion of the Agreement, either party will promptly delete Personal Data from its systems, unless applicable law requires storage of the Personal Data.

Appendix 1

Standard Contractual Clauses (2021)
Controller-to-Controller
incorporated by reference into this DPA and accessed here:
www.aryaka.com/SCC2021-Controller-to-Controller/

ANNEX 1

A. LIST OF PARTIES

Data exporter(s): The data exporter is: Reseller, as defined in the Agreement

[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: See Order Form between Reseller and Aryaka

Address: See Order Form between Reseller and Aryaka

Contact person's name, position, and contact details: See Order Form between Reseller and Aryaka

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

Role (controller/processor): Controller

,

Data importer(s): The data importer is: Aryaka.

Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: Aryaka Networks, Inc.

Address: 1850 Gateway Drive, Suite 500, San Mateo, CA 94404 USA

Contact person's name, position, and contact details: Edward Frye, CISCO/IT, edward.frye@aryaka.com

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

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Business contacts at the Reseller and Aryaka.

Categories of personal data transferred

Business contact information, such as name, title, email address, telephone numbers, physical address.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As needed to perform the Services under the Agreement and maintain the commercial relationship.

Nature of the processing

Aryaka will process Personal Information as necessary to fulfill perform the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Transfer to Aryaka’s business offices located outside of the UK, EEA, or Switzerland. Aryaka will process Personal Information as necessary to fulfill perform the Services pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Type	Number of Years Retained
Sales Records	5 years
Invoices	7 years
General Ledger	Permanent

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The following Sub-processors may be deployed for the following services/at the following Processing locations:

Salesforce:

Use: Customer Relationship Management

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States, India, Germany, United Kingdom, Canada, Australia, Japan, The Netherlands, South Korea, and Switzerland

NetSuite:

Use: Accounting

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States and India

Zuora:

Use: Billing

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States and India

Marketo:

Use: Marketing and Messaging

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States, United Kingdom and India

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The UK Information Commissioner’s Office.

Appendix 2

Standard Contractual Clauses (2021)
Controller-to-Processor
incorporated by reference into this DPA and accessed here:
www.aryaka.com/SCC2021-Controller-to-Processor/

ANNEX 1

A.LIST OF PARTIES

Data exporter(s): The data exporter is: Reseller, as defined in the Agreement

[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: See Order Form between Reseller and Aryaka

Address: See Order Form between Reseller and Aryaka

Contact person's name, position and contact details: See Order Form between Reseller and Aryaka

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

Role (controller/processor): Processor

Data importer(s): The data importer is: Aryaka.

Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: Aryaka Networks, Inc.

Address: 1850 Gateway Drive, Suite 500, San Mateo, CA 94404 USA

Contact person's name, position and contact details: Edward Frye, CISCO/IT, edward.frye@aryaka.com

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

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Reseller's Customer information as needed to provide the Services, including providing customer support.

Categories of personal data transferred

Business contact information, such as name, title, email address, telephone numbers, physical address.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As needed to perform the Services under the Agreement and maintain the commercial relationship.

Nature of the processing

Aryaka will process Personal Information as necessary to fulfill perform the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Transfer to Aryaka’s business offices located outside of the UK, EEA, or Switzerland. Aryaka will process Personal Information as necessary to fulfill perform the Services pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Type	Number of Years Retained
Sales Records	5 years
Invoices	7 years
General Ledger	Permanent

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The following Sub-processors may be deployed for the following services/at the following Processing locations:

Salesforce:

Use: Customer Relationship Management

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States, India, Germany, United Kingdom, Canada, Australia, Japan, The Netherlands, South Korea, and Switzerland

NetSuite:

Use: Accounting

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States and India

Zuora:

Use: Billing

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States and India

Marketo:

Use: Marketing and Messaging

Location where instance is resident: United States

Accessed by Aryaka Personnel from:

United States, United Kingdom and India

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The UK Information Commissioner’s Office.

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):

The parties maintain various policies, standards and processes designed to secure Personal Information and other Personal Data. Following is a description of some of the core technical and organisational security measures implemented by both parties.

Physical Access Controls

Measures designed to prevent unauthorized persons from gaining physical access to physical locations that house data processing equipment used to process Personal Data.

Technical Access Controls

Measures designed to prevent unauthorized persons from gaining access to the party's data processing systems, including:

- Hybrid 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
- Network edge security providing advanced perimeter security solutions that are built into Reseller's SD-WAN appliance.

Data Access Controls

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 Personal Data from being read, copied or modified or removed without authorization.

Input Controls

Measures designed to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof.

Job Controls

Measures designed to ensure that Personal Data being processed is processed solely in accordance with the Agreement.

Availability Controls

Measures designed to protect Personal Data against disclosure, accidental or unauthorized destruction or loss.