May 31, 2023

A10 Networks Data Processing Addendum

This A10 Networks Data Processing Addendum ("**Addendum**") supplements and forms a part of the Cloud Subscription Services Agreement, EULA and/or other Terms and Conditions ("**Terms**") between A10 Networks, Inc. ("**A10**") and the person or organization ("**User**") to whom A10 has agreed to provide the services that User ordered from A10 ("**Services**"). If there is any conflict between this Addendum and the Terms, this Addendum will prevail to the extent of the conflict.

1. **Definitions.** The following terms shall have the meanings set out below.

   1.1. "**Applicable Data Privacy Law**" means all laws and regulations that apply to a party's processing of personal information in connection with the provision or receipt of Services.

   1.2. The term "**personal information**" means information about an identified or identifiable individual (the "**data subject**"), and includes information protected as "personal information", "personal data" or any analogous term by Applicable Data Privacy Law.

   1.3. To "**process**" data means to perform any operation or set of operations on the data, including collecting, using, retaining, storing and disclosing it.

   1.4. "**User Data**" means data, information and content that User uploads for storage or processing by the Services.

   1.5. "**User Personal Information**" means personal information contained in User Data.

2. **General Limitation.** A10 will only process User Personal Information on User's documented instructions or as permitted or required by Applicable Data Privacy Law. User agrees that the Terms, User's orders for Services, and any other contracts or written instructions between User and A10 form part of User's documented instructions to A10 to process User Personal Information. If applicable laws and regulations require A10 to process User Personal Information in a manner different from User's documented instructions, A10 will inform User of that legal requirement before proceeding with the processing, to the extent permitted by applicable law.

3. **Subprocessors.** A10 imposes data protection terms on its subprocessors that process User Personal Information on A10's behalf that are no less protective of User Personal Information than those in this Addendum. User authorizes A10 to subcontract its obligations to process User Personal Information to any subprocessor listed here https://www.a10networks.com/wp-content/uploads/Data-Processor-Handout.pdf. A10 will provide reasonable advance notice of any relevant proposed changes to such list of subprocessors and the parties agree to discuss in good faith how to resolve any reasonable objection that User may have to such proposed changes.

4. **Confidentiality.** A10 will ensure that persons authorized to process User Personal Information by or on behalf of A10 have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality with respect to such User Personal Information.

5. **Data Subject Rights Assistance.** If an individual makes a written request to A10 purporting to exercise their rights under Applicable Data Privacy Law in relation to User Personal Information, A10 shall forward the request to User without undue delay and User agrees to address the request in accordance with Applicable Data Privacy Law. On User's written request, A10 will provide User with reasonable assistance (at User's expense if doing so would require A10 to assign significant resources to such effort) to assist User in complying with User's obligations with respect to the request under Applicable Data Privacy Law.

6. **Impact Assessments and Consultations.** A10 will provide User with reasonable assistance (at User's expense if doing so would require A10 to assign significant resources to such effort) in connection with any data privacy

or protection impact assessment or consultations with regulatory authorities that User may be required to undertake in accordance with Applicable Data Privacy Law.

7. **Security Incident Notification.** If A10 discovers or reasonably believes that User Personal Information has been subject to accidental or unlawful destruction, loss or alteration, or unauthorized access, use or disclosure resulting from a breach of A10's security measures (collectively, a "**Security Incident**"), A10 will, to the extent permitted by applicable law, notify User without undue delay, and in any case no later than required under Applicable Data Privacy Law.

8. **Return or Deletion of Personal Information.** A10 will delete User Personal Information from A10's systems after the end of the provision of the relevant Services, unless applicable laws and regulations require further storage or processing of User Personal Information or if such information is necessary to enable A10 to protect its rights under applicable agreements and laws.

9. **Demonstrating Compliance.** A10 periodically self-assesses, or engages third-party professionals at its own expense to assess, A10's measures with respect to its processing of personal information and generate a confidential report regarding the measures it has taken for the purposes of complying with Applicable Data Privacy Law ("**Audit Report**"). On User's written request at reasonable intervals, A10 will make available to User a copy of A10's most recent Audit Report subject to reasonable confidentiality controls. A10 will also use commercially reasonable efforts to answer questions that User has regarding the measures that A10 has taken for the purposes of complying with Applicable Data Privacy Law and will cooperate in good faith with User for the purposes of addressing any concerns User may have that A10 may not be in compliance with Applicable Data Privacy Law.

10. **Standard Contractual Clauses.** If and to the extent that A10's processing of User Personal Information is subject to the data protection laws of the European Economic Area, the United Kingdom or Switzerland, A10 will process the personal information in accordance with Modules 2 and 3 (as applicable) of the Standard Contractual Clauses 2021 (SCCs) promulgated by Commission implementing decision (EU) 2021/914 of 4 June 2021 and UK International Data Transfer Addendum, the bodies of which are incorporated herein by reference and the Annexes and other customizable components to which User shall complete and submit without delay in the format attached hereto as Annexes I and III below. Where Swiss data protection law applies, references specific to the EEA contained in the EU Standard Contractual Clauses shall be understood to refer to Switzerland. The SCCs shall be governed by the courts and laws of the Netherlands, with Option 2 applying at Clause 9(a) and a time period of 5 days specified therein and without the optional language in Clause 11.

11. **CCPA Terms.** If and to the extent that User Personal Information includes any personal information about California residents, A10 agrees that it will:

    11.1. Not sell or share any of the personal information, as the terms "sell" and "share" are defined in the California Consumer Privacy Act of 2018 and the regulations thereunder ("**CCPA**");

    11.2. Not, except as permitted or required by applicable laws and regulations, process the personal information: (i) for any purpose other than for the specific purpose of providing the Services; or (ii) outside the direct business relationship between User and A10; and

    11.3. Comply with applicable sections of the CCPA and notify User no later than five business days after it makes a determination that it can no longer meet its obligations under the CCPA.

12. **User Processing.** User represents, warrants and agrees that: (i) all User Data has been and at all times will be collected, processed and transferred to A10 in accordance with all applicable laws and regulations; and (ii) User's instructions and requests relating to A10's processing of User Data will not cause A10 to violate any applicable law or regulation. Without limiting the generality of the foregoing, User agrees that it has provided

all necessary notices and obtained all necessary consents from data subjects as required under Applicable Data Privacy Law before providing their personal information to A10. User shall defend, indemnify and hold harmless A10 and its affiliates, and all of their officers, directors, employees, shareholders, legal representatives, agents, successors and assigns, from and against any and all claims, liabilities, suits, demands, damages, losses, judgments, fines, penalties, interest, costs and expenses (including reasonable attorneys' fees and professional and court costs) arising from or relating to any breach of this section by User, or any act or omission of User's, or User's employees or contractors, in activities arising from or relating to User Data. Without prejudice to any other rights or remedies to which A10 may be entitled, A10 reserves the right to suspend or terminate (in A10's sole discretion) all Services where it reasonably believes that User has contravened or will contravene this section.

13. **No Consideration.** User and A10 agree that A10 does not receive any User Data as consideration for any services or other items that A10 provides to User.

14. **Security.** A10 implements technical and organizational security measures in relation to the processing of User Personal Information in accordance with Annex II attached hereto.

15. **Updates.** A10 may update the terms of this Addendum, including where necessary to: (i) comply with updates to Applicable Data Privacy Law; (ii) reflect changes resulting from a merger, acquisition, or other similar transaction; or (iii) address A10's release of new products or services or material changes to any existing Services. A10 will provide User with prior notice of such updates as required by applicable laws and regulations.

[*remainder of this page left blank intentionally*]

ANNEX I OF THE SCCS

A. LIST OF PARTIES

Data exporter(s): the data exporter is Customer.

Name: See customer as identified as a signatory party in relevant order.

Address: See customer's address as identified in the relevant order.

Activities relevant to the data transferred under these Clauses: Provider of personal data as part of commercial relationship with data importer.

Role (controller/processor): Controller for Module 2 and Processor for Module 3

Data importer(s):

Name: A10 Networks, Inc.

Address: 2300 Orchard Parkway, San Jose, California 95131, U.S.A.

Contact person's name, position and contact details: Sean Pike, Chief Security Officer A10 Networks, Inc. Address: 2300 Orchard Parkway, San Jose, California 95131, U.S.A. e-mail: spike@a10networks.com.

Activities relevant to the data transferred under these Clauses: Recipient of personal data as part of commercial relationship with data exporter.

Role (controller/processor): Processor for Modules 2 and 3

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred.

Individuals located in the European Economic Area, United Kingdom or Switzerland

Categories of personal data transferred.

Data about usage of online systems and services

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.

Sensitive data contained in data about usage of online systems and services, which A10 Networks, Inc. protects in accordance with its Data Processing Addendum

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

Continuous

Nature of the processing

Collection, analysis, storage and disclosure for the purposes of providing the services that the User has engaged A10 Networks, Inc. to provide, which may include load balancing, traffic management, security and analytics services.

Purpose(s) of the data transfer and further processing

To provide the services that the User has engaged A10 Networks, Inc. to provide, which may include load balancing, traffic management, security and analytics services.

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

A10 Networks, Inc. will delete, return or anonymize the personal data after it has finished providing the processing services.

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

Sub-processors assist A10 Networks, Inc. with respect to the provision of its services.

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred.

Same as Module Two.

Categories of personal data transferred.

Same as Module Two.

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.

Same as Module Two.

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

Same as Module Two.

Nature of the processing

Same as Module Two.

Purpose(s) of the data transfer and further processing

Same as Module Two.

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

Same as Module Two.

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

Same as Module Two.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

The Dutch Data Protection Authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

A10 maintains a comprehensive Information Security Program ("**Security Program**") to manage information within A10 that includes administrative, technical, and physical safeguards designed to protect the confidentiality, integrity and availability of User Data. A10's Security Program includes following elements:

1. **Policies and Procedures**

A10 maintains policies and procedures to ensure the confidentiality, integrity, and availability of User Data and protect it from accidental, unauthorized or improper disclosure, use, alteration or destruction.

2. **Access Controls**

A10 maintains policies, procedures, and operational processes that:

2.1. limit physical access to User Data and the facility or facilities in which it is stored to properly authorized persons;
2.2. ensure that all members of the A10 workforce (including contractors) who require access to User Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access;
2.3. authenticate and permit access only to authorized individuals and prevent members of A10 workforce from providing User Data or information relating thereto to unauthorized individuals;
2.4. assign a unique ID to each person with computer access to User Data;
2.5. restrict access to User Data to only those people with a "need-to-know" for a permitted purpose;
2.6. regularly review the list of people and services with access to User Data, and remove accounts that no longer require access;
2.7. maintain and enforce "account lockout" by disabling accounts with access to User Data when an account exceeds a threshold number of consecutive incorrect password attempts;
2.8. regularly review access logs for signs of malicious behavior or unauthorized access.

3. **Security Awareness and Training**

A10 maintains an ongoing security awareness and training program for all members of A10's workforce (including contractors and management).

4. **Security Incident Procedures**

A10 maintains policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into User Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes. If A10 becomes aware of any security incident that leads to a data breach impacting User Data, A10 will:

4.1. notify customer without undue delay;
4.2. reasonably cooperate with the impacted User to investigate and remediate the breach and mitigate any further risk to User Data.

5. **Contingency Planning**

A10 maintains policies, procedures, and operational processes for responding to an emergency, or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages User Data or systems that contain User Data.

6. **Device and Media Controls**

A10 does not permit User Data to be downloaded, or otherwise stored on laptops or other portable devices, unless they are subject to all of the protections required herein. Such protective measures shall include, at a minimum, that all devices accessing User Data shall be encrypted and use up-to-date anti-malware detection prevention software.

7. **Audit Controls**

A10 maintains hardware, software, services, platforms and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

8. **Storage and Transmission Security**

A10 maintains technical security measures to guard against unauthorized access to User Data that is being transmitted over an electronic communications network. A10 will:

8.1. maintain a working and up-to-date network firewall to protect data accessible via the Internet;
8.2. use anti-malware software at all times and will keep the anti-malware software up-to-date;
8.3. maintain technical and security measures to encrypt User Data in transit and at rest;
8.4. regularly review access logs for signs of malicious behavior or unauthorized access;
8.5. keep A10's systems and software up-to-date with the latest applicable upgrades, updates, new versions and other modifications necessary to ensure security of User Data.

9. **Assigned Security Responsibility**

A10 has a designated security official responsible for the development, implementation, and maintenance of the Security Program.

10. **Testing**

A10 regularly tests key controls, systems and procedures of A10's Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified.

11. **Third Party Vendor Management**

A10 may use third party vendors in support of A10's services to User. A10 performs a security and privacy risk-based assessment of prospective vendors before working with vendors to validate that they meet A10's privacy and security standards.

12. **Disclosure by Law**

In the event A10 is required by law, regulation, or legal process to disclose any User Data, A10 will (a) give customer, to the extent possible, reasonable advance notice prior to disclosure so customer may contest the disclosure or seek a protective order, and (b) reasonably limit the disclosure to the minimum amount that is legally required to be disclosed.

13. **Updates**

A10 continually monitors, evaluates, and adjusts, as appropriate, the Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the User Data, and internal or external threats to User Data.

ANNEX III

Parts 1 and 2 of the UK International Data Transfer Addendum
to the EU Commission Standard Contractual Clauses

Part 1: Parties

Start date	Date of the last signature shown in Annex I.A above.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Annex I.A above. Trading name (if different): Main address (if a company registered address): See Annex I.A above. Official registration number (if any) (company number or similar identifier):	Full legal name: See Annex I.A above. Trading name (if different): Main address (if a company registered address): See Annex I.A above. Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): See Annex I.A above Job Title: See Annex I.A above Contact details including email: See Annex I.A above	Full Name (optional): See Annex I.A above Job Title: See Annex I.A above Contact details including email: See Annex I.A above
Signature (if required for the purposes of Section 2)	See Annex I.A above.	See Annex I.A above.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☑ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: See Annex I.A above Reference (if any): Other identifier (if any): Or

	☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex I.A above.
Annex 1B: Description of Transfer: See Annex I.B above.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II above.
Annex III: List of Sub processors (Modules 2 and 3 only): Data importer has made such list available.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party

Schedule 1

Subprocessors

As of June 1, 2023 A10 Networks secures data processing services from the following entities to facilitate its provision of support services:

Processor	Product	Location	Processing Activity	Privacy Policy
SlapFive	Marketing Platform	United States	Marketing integration and automation	https://www.slapfive.com/privacy_policy/
ZoomInfo	SalesOS	United States	Customer file enrichment	https://www.zoominfo.com/privacy-center
Adobe	Marketo Engage	United States	Marketing automation	https://www.adobe.com/privacy.html
Experian	Address Validation	United States	Customer file enrichment	https://www.experian.com/business/solutions/regulatory-compliance/gdpr-compliance-solution
Clari	Clari Revenue Platform	United States	Revenue operations	https://www.clari.com/gdpr/
Clozd	Clozd Platform	United States	Customer feedback analysis	https://www.clozd.com/privacy/gdpr
Impartner	Afinity Partner Portal	United States	Partner relationship management	https://info.impartner.com/privacy-policy.aspx
Salesforce	SFDC	United States	Customer relationship management	https://compliance.salesforce.com/en/gdpr
Oracle	Oracle Cloud Infrastructure	United States	Platform-as-a-Service provider	https://www.oracle.com/uk/security/gdpr/
Crowdstrike	Falcon	United States	Endpoint detection and response	https://www.crowdstrike.com/why-crowdstrike/crowdstrike-compliance-certification/
Microsoft	O365, Azure AD, Defender	United States	Email and related services	https://www.microsoft.com/en-ww/trust-center/privacy/gdpr-faqs?market=af
Atlasian	Atlasian Cloud, Jira	United States	IT service management	https://www.atlassian.com/trust/privacy/country/europe-and-gdpr
Incedo	Engineering and Managed Services	India	Product engineering and IT related services	https://www.incedoinc.com/privacy-policy/

These sub-processors provide networking and connectivity services. This list may be updated https://www.a10networks.com/wp-content/uploads/Data-Processor-Handout.pdf from time to time as noted in Article 3 of the DPA to which this Schedule is attached.