DATA PROCESSING AGREEMENT

Where applicable, this Data Processing Agreement ("**DPA**") forms part of the Illumio Master Subscription Agreement or other agreement entered into between Illumio, Inc. ("**Illumio**", "**Us**", "**We**", "**Our**") and Customer (collectively, "**You**", "**Your**", or "**Customer**") that governs Customer's use of and access to Illumio Products (the **Agreement**"). Both parties shall be referred to as the "**Parties**" and each, a "**Party**". This DPA forms a binding legal agreement to reflect the Parties' agreement with regard to the Processing of Personal Data (as such terms are defined below).

This DPA between Customer and Illumio contains the legal terms and conditions that apply to the Processing of Personal Data by Illumio Products, where Customer is acting as the Controller of Personal Data and Illumio is acting as a Processor of Personal Data. For the avoidance of any doubt, Illumio's activities as a Controller are governed by our privacy policy. Unless otherwise specified in this DPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event of any inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail.

INSTRUCTIONS FOR CREATING A LEGALLY BINDING DPA:

This DPA has been pre-signed on behalf of Illumio. This DPA supersedes and replaces any prior Data Protection Agreement, or any other prior understanding or agreement, related to the processing of Customer Personal Data in connection with the Agreement.

This DPA, and its Schedules, including Annex 1 to Schedule 1 (Standard Contractual Clauses), where applicable, will become legally binding when Customer:

1. Completes the information in the signature box of this DPA;
2. Signs the DPA in the signature box;
3. Sends the signed DPA to Illumio by email to dpa@illumio.com;
4. Ilumio has received the validly completed and signed DPA via dpa@Illumio.com; (the date of such receipt is the "**DPA Effective Date"**).

1. DEFINITIONS

"**Adequate Country**" means a country providing an adequate level of data protection pursuant to Applicable Laws;

"**Controller**" or "**Business**" as relevant under applicable Data Protection Laws, means the entity which determines the purposes and means of the Processing of Personal Data or such equivalent term under Data Protection Laws.

"**Customer Personal Data**" means any Personal Data which is provided by Customer to illumio and Processed by Illumio on behalf of Customer in order to provide the Products under the Agreement. Customer Personal Data does not include Personal Data that Illumio Processes as a Controller separately from its Processing obligations to Customer under the Agreement.

"**Data Protection Laws**" means all laws and regulations of the European Union, the EEA and their Member States, Switzerland, the United Kingdom, the United States, Australia, Canada, Japan and Singapore, each to the extent applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom the Customer Personal Data relates.

"**EEA**" means the European Economic Area.

"**EU Data Protection Law**" means the GDPR, and the UK GDPR.

"**EU-U.S. Data Privacy Framework**" or "**EU-U.S. DPF**" means the transfer mechanism in terms of Art. 45 of the EU GDPR that enables participating organizations - pursuant to the European Commission's Implementing Decision C(2023) 4745 final of 10.7.2023 and the EU-U.S. Data Privacy Framework Principles1 as set forth by the U.S. Department of Commerce - to Process Customer Personal Data originating from the European Union (EU) and the European Economic Area (EEEA) ("**EU Customer Personal Data**") in the United States (U.S.) in accordance with Chapter V of the EU GDPR;

"**Extended EEA Country**" means a Member State of the EEA, Switzerland or the United Kingdom, and Extended EEA Countries means the foregoing countries collectively.

"**Member State(s)**" means a country that belongs to the European Union and/or the EEA.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier or such equivalent term under Data Protection Laws.

"**Process(ing)**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" or "**Service Provider**," as relevant under applicable Data Protection Laws, means the entity which Processes Personal Data on behalf of the Controller or Business or such equivalent term under Data Protection Laws.
"**Restricted Transfer**" means: (i) any export by Customer of Customer Personal Data from its country of origin to Illumio to a jurisdiction that is not an Adequate Country.

"**Security Program**" means Illumio's Security Program set forth in Section 6 of Exhibit A to the Agreement

"**Standard Contractual Clauses**" means the "standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission decision of 4 June 2021" and published under document number C (2021) 3972 available athttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914&qid=1689513765256, as may be updated, amended or superseded from time to time.

"**Sub-Processor**" means any Processor or Service Provider engaged by Illumio and/or Illumio Affiliate to Process Customer Personal Data.

"**Supervisory Authority**" means the competent supervisory authority pursuant to the applicable Data Protection Laws.

"**UK GDPR**" means the GDPR as incorporated into United Kingdom domestic law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR").

"US Privacy Laws" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 along with any associated regulations ("CCPA"); the Virginia Consumer Data Protection Act ("VCDPA"); the Colorado Privacy Act; and any similar U.S. laws governing data privacy and security once effective.

2. CUSTOMER'S PROCESSING OF PERSONAL DATA. Customer shall, in its use of the Products, Process Customer Personal Data in accordance with the requirements of Data Protection Laws. For the avoidance of doubt, Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws. As between the Parties, Customer shall have sole responsibility for the means by which Customer acquired Customer Personal Data. Without limitation, to the extent applicable, Customer shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall have any and all required legal basis in order to collect, Process and transfer to Illumio the Customer Personal Data and to authorize the Processing by Illumio of the Customer Personal Data which is authorized in this DPA.

3. ILLUMIO'S PROCESSING OF PERSONAL DATA.

3.1 Application. As used in clauses 3 – 9 herein, Customer Personal Data refers to Customer Personal Data that is subject to Data Protection Laws.

3.2 Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, (i) Customer is the Controller or Business or, where Customer is acting behalf of its own customers, a Processor, (ii) Illumio is the Processor or Service Provider, and (iii) Illumio or its Affiliates may engage Sub-Processors pursuant to the requirements set forth in Clause 6 below.

3.3 Illumio and its Affiliates (as applicable) shall Process Customer Personal Data only in accordance with Customer's documented instructions, which are set out in the Agreement, as necessary for the provision of the Products and for the performance of the Agreement and this DPA, unless required to otherwise by any applicable law, court of competent jurisdiction or other Supervisory Authority to which Illumio and its Affiliates are subject, in which case, Illumio shall inform Customer of the legal requirement before processing, unless that law prohibits such information. Customer agrees that the Agreement is its complete and final instructions to Illumio in relation to the Processing of Personal Data. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between Illumio and Customer by way of an amendment to the Agreement and may include any additional fees that may be payable by Customer to Illumio for carrying out such instructions. The duration of the Processing, the nature and purposes of the Processing, as well as the types of Customer Personal Data Processed and categories of Data Subjects under this DPA are further specified in Schedule 1 to this DPA.

3.4 To the extent that Illumio or its Affiliates cannot comply with an instruction from Customer and/or its authorized users relating to Processing of Customer Personal Data or where Illumio considers such instruction to be unlawful, Illumio (i) shall inform Customer, providing relevant details of the problem; (ii) may, without any kind of liability towards Customer, temporarily cease all Processing of the affected Customer Personal Data (other than securely storing those data); and (iii) if the Parties do not agree on a resolution to

the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Illumio all the amounts owed to Illumio or due before the date of termination.

4. RIGHTS OF DATA SUBJECTS. If Illumio receives a request from a Data Subject to exercise its rights under Data Protection Laws ("**Data Subject Request**"), Illumio shall, to the extent legally permitted, promptly notify and forward such Data Subject Request to Customer. Taking into account the nature of the Processing, Illumio shall use commercially reasonable efforts to assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws

5. ILLUMIO PERSONNEL. Illumio shall grant access to the Customer Personal Data to persons under its authority (including, without limitation, its personnel) only on a need-to-know basis and ensure that such persons engaged in the Processing of Customer Personal Data have committed themselves to confidentiality.

6. AUTHORIZATION REGARDING SUB-PROCESSORS.

6.1 Customer hereby grants general written authorization to Illumio to appoint Sub-Processors to perform specific Processing activities on Customer Personal Data on its behalf. Illumio's current list of Sub-Processors is included at https://www.illumio.com/legal/sub-processor-list ("**Sub-Processor List**") and is hereby approved by Customer.

6.2 Objection Right for Sub-Processors. Provided that Customer signs up for notifications on the Illumio support portal, Illumio shall provide prior notice of any new Sub-Processors. After being notified, Customer will have ten (10) business days to notify Illumio in writing of any reasonable objection it has to the new Sub-Processor(s). Failure to notify Illumio within this time frame will be deemed approval of the new Sub-Processor(s). In the event Customer provides reasonable objection, Illumio will use reasonable efforts to make a change in the configuration available to avoid Processing of Customer Personal Data by such Sub-Processor. If Illumio is unable to make available such a change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may, as a sole remedy, terminate the applicable Order Form with respect to the affected Products that cannot be provided without use of the rejected Sub-processor, provided that all relevant amounts due under the Agreement before the termination date shall be duly paid to Illumio.

6.3 In the event Illumio engages a Sub-Processor to carry out specific processing activities on behalf of Customer, Illumio shall place the same or similar obligations on such Sub-Processor to require appropriate technical and organizational measures to meet the requirements of the Data Protection Law. Where such additional Sub-Processor fails to fulfill its data protection obligations, Illumio shall remain fully liable to Customer for the performance of that Sub-Processor's obligations.

7.SECURITY.

7.1 Controls for the Protection of Customer Personal Data. Taking into account the state of the art, Illumio shall maintain industry-standard technical and organizational measures, including as required pursuant to Article 32 of the GDPR and other applicable Data Protection Laws, for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Personal Data), confidentiality and integrity of Customer Personal Data, as set forth in the Security Porgram. Upon Customer's request, Illumio will use commercially reasonable efforts to assist Customer, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR and other applicable Data Protection Laws taking into account the nature of the processing, the state of the art, the costs of implementation, the scope, the context, the purposes of the Processing and the information available to Illumio.

7.2 Third-Party Certifications and Audits. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Illumio shall make available to Customer (or Customer's independent, third-party auditor that is not reasonably objected to by Illumio and that is bound by confidentiality obligations ("**Permitted Auditor**")) a copy of Illumio's then most recent third-party audits or certifications. Any certifications and/or documentation made available by Illumio to Customer in accordance with this Section shall be Illumio's Confidential Information and shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Illumio's prior written approval and upon Illumio's request, Customer shall return all such documentation in Customer's possession or control. To the greatest extent possible, Customer shall utilize Illumio's certifications and other privacy documentation and policies made available to Customer to assess Illumio's compliance with its obligations under this DPA. Only to the extent that Customer is not able to do so, and in any event, no more than once per year (except if otherwise required by applicable law) and following at least 90 days' notice in writing from Customer, at Customer's cost and expense, Illumio shall allow for and contribute to remote audits conducted by Customer or a Permitted Auditor. Customer will promptly reimburse Illumio for expenses incurred by Illumio in connection with audits conducted by Customer or a third-party auditor beyond those that Illumio already conducts, including but not limited to, time reasonably expended for such audits at Illumio's then-current professional services rates (made available to Customer upon request).The Parties shall agree on the scope, methodology, timing and conditions of such audits in advance. Customer shall use reasonable endeavors to ensure that the conduct of each audit does not disrupt Illumio's business. In no event shall Customer be permitted to access any information, including without limitation, data that belongs to Illumio's other customers or such other information that is not relevant to Illumio's compliance with this DPA. Unless otherwise agreed by the Parties, Customer shall use reasonable efforts to carry out the audit of Illumio's compliance with this DPA together with the audit of Illumio's compliance with the Security Program. Customer shall promptly notify Illumio of any non-compliance discovered during the course of any audit; and Illumio will inform Customer if it becomes aware of an instruction by Customer that, in Illumio's opinion, infringes the Data Protection Law.

8. TRANSFERS OF DATA

8.1 Transfers of Customer Personal Data. Illumio may transfer Customer Personal Data outside of its country of origin as reasonably required to provide the Products, in accordance with its operating model and subject to the obligations set forth in this DPA.

8.2 EU Customer Personal Data. Illumio's Processing of EU Customer Personal Data in the U.S. shall adhere to the EU-U.S. Data Privacy Framework Principles. Illumio is certified under the EU-US DPF. Illumio's certification status is available in the U.S. Department of Commerce's Data Privacy Framework List. In the event that Illumio is required to adopt an alternative transfer mechanism pursuant to Chapter V of the EU GDPR for Processing EU Customer Personal Data in the U.S other than the EU-U.S. DPF, then the Parties agree that SCCs as set forth in Schedule 1 shall apply.

8.3 UK (and Gibraltar) Customer Personal Data. Illumio's Processing of UK (and Gibraltar) Customer Personal Data in the U.S. shall adhere to the UK Extension to the EU-U.S. DPF approved by the UK government in its UK Adequacy Decision. Illumio is certified under the UK Extension to the EU-US DPF. Illumio's certification status is available in the U.S. Department of Commerce's Data Privacy Framework List. In the event that Illumio is required to adopt an alternative transfer mechanism pursuant to Chapter V of the UK GDPR for Processing UK Personal Data in the U.S. other than the UK Extension to the EU-U.S. DPF, then the Parties agree that SCCs and the UK's International Data Transfer Addendum as set forth in Schedule 1 shall apply.

8.4 Swiss Customer Personal Data. Illumio is certified under the Swiss-US DPF. Illumio's certification status is available in the U.S. Department of Commerce's Data Privacy Framework List. the event that Illumio is required to adopt an alternative transfer mechanism pursuant to Chapter V of the UK GDPR for Processing UK Personal Data in the U.S. other than the UK Extension to the EU-U.S. DPF, then the Parties agree that SCCs and the UK's International Data Transfer Addendum as set forth in Schedule 1 shall apply.

8.5 Other Restricted Transfers. Customer will notify Illumio in writing if a Restricted Transfer involving Customer Personal Data requires privacy provisions not already included in this DPA. The Parties will promptly enter into a written amendment to include such provisions, but only to the extent required under applicable law and where this DPA does not provide adequate safeguards. For the avoidance of doubt, by adding such provisions, the Parties do not intend to grant third-party beneficiary rights to Data Subjects not otherwise provided under Applicable Law.

8.6 In the event Customer enables Third Party Applications (as defined in the Agreement) which involve transfers of Customer Personal Data between Illumio and the Third Party Application provider, Customer acknowledges and agrees that (a) such Third Party Application providers are not Sub-Processors of Illumio; (b) such transfers are conducted at Customer's instruction in accordance with an agreement between the Customer and such Third Party Application provider (which Illumio is not a party to); and (c) Customer shall be solely responsible for such transfers and their compliance with Data Protection Laws, including without limitation, executing Standard Contractual Clauses with such Third Party Application providers as required.

9. US PRIVACY LAWS.

9.1 In performing its obligations under the Agreement and this DPA, Illumio shall comply with its obligations under US Privacy Laws, including by providing the level of privacy protection as is required by US Privacy Laws to Customer Personal Data subject to the US Privacy Laws. Illumio will not: (1) "sell" or "share" for purposes of "cross-context behavioral advertising" or "targeted advertising" (as defined by applicable US Privacy Laws) any Customer Personal Data; (2) retain, use, or disclose Customer Personal Data for any purpose other than the contractual business purpose set forth herein or as otherwise permitted under US Privacy Laws or outside of the direct business relationship between Illumio and Customer; or (3) attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Customer Personal Data.

9.2 Illumio will (1) comply with any applicable restrictions under applicable US Privacy Laws on combining Customer Personal Data with Personal Data that Illumio receives from, or on behalf of, another person or persons; and (2) promptly notify Customer if Illumio determines that it (i) can no longer meet its obligations under this DPA or applicable US Privacy Laws; or (ii) in Illumio's opinion, an instruction from Customer infringes applicable US Privacy Laws.

9.3 To the extent required under US Privacy Laws, Customer may take reasonable and appropriate steps to help to ensure that Illumio uses Customer Personal Data in a manner consistent with Customer's obligations under US Privacy Laws and to stop and remediate unauthorized use of the Customer Personal Data.

9.4 Illumio certifies that it understands its obligations in this Clause 9. The Parties agree that Schedule 1 hereto shall satisfy any requirement under applicable U.S. Privacy Law to provide details regarding the nature of the Processing activities related to Customer Personal Data.

10. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION. To the extent required under applicable Data Protection Laws, Illumio shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data (a "**Personal Data Incident**"). Illumio shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Illumio deems necessary, possible and reasonable in order to remediate the cause of such a Personal Data Incident. Customer, will be the party responsible for notifying supervisory authorities and/or concerned Data Subjects (where required by Data Protection Laws).

11. RETURN AND DELETION OF PERSONAL DATA. Subject to the Agreement, upon termination or expiry of the Products, Illumio shall, make available for return the Customer Personal Data via the Products and delete such Customer Personal Data in accordance with Illumio's customer data retention & deletion policy unless applicable law requires storage of the Customer Personal Data. In any event, Customer agrees that Illumio may retain Customer Personal Data in accordance with its standard backup policy, for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or to comply with applicable laws and regulations.

12. TERMINATION. This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Products are provided, provided that, to the extent Illumio retains any Customer Personal Data following termination or expiration of the Agreement, this DPA shall survive for such period that Illumio retains Customer Personal Data. Clauses 2, 3.4 and 13 shall survive the termination or expiration of this DPA for any reason. This DPA cannot, in principle, be terminated separately to the Agreement, except where the Processing ends before the termination of the Agreement, in which case, this DPA shall automatically terminate.

13. RELATIONSHIP WITH AGREEMENT. Subject to any provisions in Schedule 1regarding governing law and choice of forum of the Standard Contractual Clauses, the governing law and choice of forum provision in the Agreement shall apply to this DPA. In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement. For the avoidance of doubt each Party's and its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, the Standard Contractual Clauses, Data Protection Laws and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. NOTWITHSTANDING THE FOREGOING, IF CUSTOMER IS USING THE PRODUCTS FOR A FREE TRIAL, ILLUMIO'S MAXIMUM AGGREGATE LIABILITY TO CUSTOMER UNDER OR RELATED TO THIS DPA SHALL BE CAPPED AT ONE THOUSAND DOLLARS US ($1,000 US).

14. AFFILIATES. Any Illumio obligation hereunder may be performed (in whole or in part), and any Illumio right (including invoice and payment rights) or remedy may be exercised (in whole or in part), by an Affiliate of Illumio. To the extent that any of Customer's Affiliate(s): (a) is subject to the Data Protection Laws; (b) provides Customer Personal Data to Illumio in the context of the Products; and (c) is permitted to use the Products pursuant to the Agreement but has not signed its own agreement with Illumio and is not a "Customer" as defined under the Agreement, the Parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, in the name and on behalf of such Affiliates, subject to the following: (a) each Affiliate agrees to be bound by the obligations under this DPA and any violation of this DPA by an Affiliate shall be deemed a violation by Customer; (b) Customer shall remain exclusively responsible for coordinating all communication with Illumio under the Agreement and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates; and (c) Affiliates shall not be entitled to bring a claim directly against Illumio. If an Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or other forms of complaints or proceedings against Illumio ("**Affiliate Claim**"): (i) Customer must bring such Affiliate Claim directly against Illumio on behalf of such Affiliate, unless Data Protection Laws require the Affiliate be a party to such claim; and (ii) all Affiliate Claims shall be considered claims made by Customer and shall be subject to the limitation of liability set forth in the Agreement.

15. CHANGES IN LAWS. In the event that changes to this DPA are required as a result of changes in Data Protection Laws, including to update any Schedules or transfer mechanisms, the Parties shall co-operate in good faith to implement such changes to ensure that this DPA complies with such Data Protection Laws.

The Parties by their duly authorized representatives have executed this DPA to be effective as of the DPA Effective Date.

Customer:	**Illumio, Inc.**
By:	By: Thien Dinh (May 21, 2026 15:27:23 PDT)
Name:	Name: Thien Dinh
Title:	Title: Sr. Legal Counsel
Date:	Date: May 21, 2026

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

1. Incorporation and interpretation of the Standard Contractual Clauses

1.1. In relation to Restricted Transfers to Illumio by Customer of Customer Personal Data which are subject to Data Protection Laws of the Extended EEA Countries, the parties agree that Module Two (*Transfer controller to processor*) or Module 3 (*Transfer processor to processor*) of the Standard Contractual Clauses shall apply, as applicable.

1.2. The Parties acknowledge that the information required to be provided in the Standard Contractual Clauses, including the appendices, is set out in Appendix 1 below.

1.3. If there is a conflict between the provisions of this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail, provided that, except to the extent prohibited by applicable law, the Standard Contractual Clauses shall be interpreted in accordance with and subject to this DPA and the Agreement, including without limitation, the provisions on limitation of liability, instructions, storage, erasure and return of Personal Data, audits and engagement of Sub-Processors.
1.4. If any provision or part-provision of this DPA or the Agreement causes the Standard Contractual Clauses to become an invalid export mechanism in the relevant Extended EEA Country, it shall be deemed deleted but that shall not affect the validity and enforceability of the rest of this Agreement and the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

1.5 Where requested by Illumio, Customer shall provide reasonable assistance to Illumio and be responsible for issuing such communications to Data Subjects and/or the Controller (to the extent Module Three applies) as are required in order for Illumio to comply with its obligations under the Standard Contractual Clauses.

1.6. Notwithstanding anything to the contrary, where the applicable Extended EEA Country where the data exporter is established or from where the transferred personal data originated is the UK, template Addendum B.1.0 issued by the UK ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, (the "UK Approved Addendum") shall amend the Standard Contractual Clauses in respect of such transfers and Part 1 of the UK Approved Addendum shall be populated as set out below:

Table 1. The "start date" will be the date this DPA enters into force. The "Parties" are Customer as exporter Illumio as importer.

Table 2. The "Addendum EU SCCs" are the modules and clauses of the Standard Contractual Clauses selected in relation to a particular transfer in accordance with paragraphs 1.1 and 1.2 of this Schedule.

Table 3. The "Appendix Information" is as set out in Appendix 1 to this Schedule.

Table 4. Neither party may end the UK Approved Addendum in accordance with its Section 19.

1.7. Except where paragraph 1.7 above applies, but notwithstanding anything else to the contrary, where the applicable Extended EEA Country where the data exporter is established or from where the transferred personal data originated is not a Member State of the European Union, references in the Standard Contractual Clauses to:

(a) "Member States of the European Union" shall refer to the applicable Extended EEA Country in which the data exporter is established or from where the transferred Personal Data originated (as applicable);

(b) "the GDPR" shall refer to the Data Protection Laws of the Extended EEA Country in which the data exporter is established or from where the Personal Data originated; and

(c) "supervisory authority" shall refer to the data protection authority in the Extended EEA Country as determined in Annex I(C) below.

Appendix 1 – Completion of the Standard Contractual Clauses

ANNEX I

Where applicable, this schedule serves as Annex 1 to the Standard Contractual Clauses and Part 1 to the UK International Data Transfer Addendum issued by the UK ICO.

A. LIST OF THE PARTIES	
Data Exporter:	Name and address: Customer, as set out in the Agreement, and its Affiliates Contact details: As set out in the Agreement Activities relevant to the data transferred under these Clauses: Use of Illumio Products, as set out in the Agreement and this DPA. Role: Controller
Data Importer:	Name and address: Illumio, as set out in the Agreement, and its Affiliates Contact details: privacy@illumio.com Activities relevant to the data transferred under these Clauses: Provision of Illumio Products, as set out in the Agreement and this DPA Role: Processor
B. DETAILS OF PROCESSING/DESCRIPTION OF TRANSFER	
CATEGORIES OF DATA SUBJECTS	Natural persons who interact with the Products, which may include (but are not limited to) data exporter's employees, contractors, Authorized Users and customers as determined by data exporter.
CATEGORIES OF PERSONAL DATA	Customer may submit personal data to the Products, the extent of which is determined by Customer. This may include the following, solely to the extent Illumio is capable of associating them with an identifiable individual: • device identifiers, IP addresses; • names, emails, phone numbers; • firmware versions, operating system, time zone, language, MAC addresses, and other information about computing systems, applications and networks; • information about activity on computing systems, applications and networks; • file and communications content and metadata, antivirus and other malware statistics and files; • system logs and traffic; and • information provided to Illumio through dashboards or portals associated with the security and firewall solutions of the Illumio Products, such as troubleshooting requests and security inquiries regarding files, systems and URLs.
SPECIAL CATEGORIES OF DATA (IF APPLICABLE)	Not applicable
FREQUENCY OF THE TRANSFER	On a regular basis during the Agreement term as required to provide the Products.
NATURE AND PURPOSE OF THE PROCESSING	• Providing maintenance and technical support. • Providing Updates and Upgrades. • Addressing security and business continuity issues. • Analyzing and improving the Products. • Enforcing the legal terms that govern the Products. • Complying with law and protect rights, safety and property.

	Other purposes requested or permitted by Customers or Authorized Users or as reasonably required to perform Illumio's business.
RETENTION PERIOD	Illumio will retain Personal Data to fulfill the purposes for which it was collected and as necessary to comply with business requirements, legal obligations, resolve disputes, and enforce its rights.
TRANSFER TO (SUB)PROCESSORS	As set out in Illumio's Sub-Processor List

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses. Where an EU Representative has not been appointed by data exporter, the competent supervisory authority shall be the supervisory authority of the Republic of Ireland.

D. OTHER

Where the Standard Contractual Clauses identify optional provisions (or provisions with multiple options) the following will apply:

For Clause 7 (Docking Clause), the optional provision will apply.
For Clause 9(a), option 2 (General Written Authorisation) will apply and the time period for prior notice of Sub-Processor changes shall be as set out in this DPA.
For clause 17 (Governing Law), option 1 and the laws of the Republic of Ireland will apply.
For clause 18 (Choice of Forum and Jurisdiction), the Republic of Ireland will apply.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. For the avoidance of any doubt, Importer will apply the technical and organisational measures set forth in this Annex II to all Customer Data (as defined in the Agreement), including but not limited to Customer Data that qualifies as personal data.

At a minimum, Importer's security program shall include include reasonable industry best practices designed to: (i) protect against anticipated threats or hazards to the security or integrity of personal data; protect against unauthorized access to or use of personal data that could result in substantial harm to any individual; ensure the proper disposal of personal data; (ii) keep and maintain all personal data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure; (iii) not create, collect, receive, access, or use personal data in violation of law; or (iv) use and disclose personal data solely and exclusively for the purposes for which the personal data, or access to it, is provided pursuant to the terms and conditions of the Agreement.

At a minimum, importer's safeguards for the protection of personal data shall include: (i) limiting access of personal data to authorized personnel; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) strictly segregating personal data from information of importer or its other customers so that personal data is not commingled with any other types of information; (vii) conducting risk assessments, penetration testing, and vulnerability scans; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to importer employees.

Importer shall constantly monitor for any attempted unauthorized access to, or use or disclosure of, any of such materials and shall immediately take all necessary and appropriate action in the event any such attempt is discovered, promptly notifying exporter of any material or significant breach of security with respect to any such materials. In the event of a Security Incident, importer shall provide exporter with full cooperation and assistance in dealing with the Security Incident, including: (i) resolving any data privacy or security issues involving any Customer personal data and (ii) making any appropriate notifications to individuals affected by the Security Incident or to the competent supervisory authority. Importer shall take all steps to contain, remediate, and investigate the Security Incident in the most expedient time possible and shall then provide exporter as soon as possible with complete information relating to a Security Incident, including, without limitation, the nature of the Security Incident, the nature of the Customer personal data affected, the categories and number of data subjects concerned (if applicable), the categories and number of personal data records concerned (if applicable), the possible consequences of the Security Incident, the measures taken to, or proposed to be taken, to address the Security Incident and mitigate its possible effects and any other information that exporter may reasonably request concerning the Security Incident. Importer shall maintain a log of Security Incidents including facts, effects, and remedial action taken. Illumio shall take all steps to restore, re-constitute and/or reconstruct any Customer personal data which is lost, damaged, destroyed, altered, or corrupted including as a result of a Security Incident as if they were importer's own data at its own cost with all possible speed and shall provide exporter with all reasonable assistance in respect of the same.

Importer performs scans internally using a third-party platform to detect Common Vulnerabilities and Exposures (CVE's) in open-source components used by the Platform. Additionally, vendor security advisories are monitored by importer for updates that would potentially impact importer products and services. Importer will install patches and remediate exploitable vulnerabilities within business, legal, and regulatory requirements.

Customer Data "at rest" is encrypted by Importer using strong encryption consistent with security industry best practices. Backups of Customer Data have the same controls as production data. Customer Data is not replicated to non-production environments unless same controls applied to production data is in place or the sensitive data is scrubbed using industry best practice measures like data masking.

Customer Data "in transit" to or from Customer/Exporter will be encrypted using strong encryption consistent with security industry best practices (e.g. SFTP, HTTPS/TLS 1.2). Customer Data sent over a browser will utilize TLSv1.2 or better.

Importer will align and maintain its security practices to ISO 27001 and/or NIST and will maintain relevant security certifications applicable to the Services, including but not limited to ISO 27001:2013 and SOC 2, Type II. Importer will provide Exporter copies of its then current third-party certifications upon request.