SUMO LOGIC SERVICE AGREEMENT
(Federal End User)

This Sumo Logic Service Agreement ("Service Agreement") describe Your rights and responsibilities as a customer of our Services. These Terms are between You and Sumo Logic, Inc., a Delaware corporation ("Sumo Logic", "**we**" or "**us**"). "**You**" and "Your" means the Federal agency customer or Ordering Activity identified in a Federal agency customer order to a Sumo Logic reseller/prime contractor ("Order Form" or "Order").

This Service Agreement, and any addendum (such as a Data Processing Addendum), constitute the entire agreement between Sumo Logic and You (collectively, the "Agreement"), however, these terms and conditions do not alter the prime contract terms and conditions which are between the You and the prime contractor. Sumo Logic is not a party to the prime contract. In the event of a conflict or inconsistency between an Order Form and this Service Agreement, as between You and Sumo Logic, this Service Agreement shall control.

You may not, without Sumo Logic's prior written consent, access or use the Services: (a) if You are a direct competitor; (b) to monitor the availability, performance or functionality of the Services; or (c) for any other benchmarking or competitive purposes.

1. GRANT AND USE RIGHTS

1.1 **Provision of the Services.** Sumo Logic will make available to You the selected internet based services ("**Services**") as specified on the applicable Order Form(s).

1.2 **Support.** During the Subscription Term, Sumo Logic will provide support and maintenance for the Services in accordance with the then current Support and Maintenance Service Addendum. a current version as set forth in Exhibit A to this Services Agreement (the "Support Terms").

1.3 **Software.** Certain Services or features of the Services may require You to install software applications ("**Software**") to access such Services or features. Subject to the terms and conditions of this Agreement, You are granted a limited, non-exclusive, nontransferable, revocable right to use the Software solely for its internal purposes during the Subscription Term.

1.4 **Intellectual Property.** Sumo Logic Technology is made available on a limited access basis, and no ownership right is conveyed to You, irrespective of the use of terms such as "purchase" or "sale". Sumo Logic (and its licensors, where applicable) retains all intellectual property rights relating to the Services or the Software (collectively Services and Software shall be referred to as "**Sumo Logic Technology**"). You will not copy, distribute, reproduce or use any of the foregoing except as expressly permitted under the Agreement.

1.5 **Feedback.** You may from time to time provide suggestions, comments or other feedback to Sumo Logic with respect to Sumo Logic Technology ("**Feedback**"). You will not share any of Your Confidential Information with Sumo Logic when You provide Feedback. You grant to Sumo Logic a nonexclusive, worldwide, perpetual, irrevocable, transferable, sublicensable, royalty-free, fully paid up license to use and exploit the Feedback for any purpose. Sumo Logic acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

1.6 **Training Services.** Sumo Logic may provide basic training services as ("**Training Services**") in connection with implementing the Services as specified on the applicable Order Form. Fees for such Training Services will be included in the applicable Order Form, provided that Sumo Logic may charge additional fees if You request additional or advance Training Services. Any such fees with be negotiated and agreed to by You prior to Sumo Logic providing such additional Training/Migration Services. Subject to the terms and conditions of this Agreement, You are granted a limited, non-exclusive, nontransferable right to use any output in conjunction with such Training/Migration Services solely in connection with this Agreement and during the training purchased by You and conducted by Sumo Logic (hereinafter referred to as "Deliverables").

1.7 **Third-Party Applications.** Sumo Logic may make available third-party applications with pre-defined queries and visualizations/dashboards (each an "**Application**"). Use of such Application is elective, and You grant Sumo Logic the right to share usage information with the third-party Application developer for purposes of improvements and troubleshooting.

1.8 **Suspension.** We may also temporarily suspend Services immediately upon notice for cause if: (a)reserved; (b)reserved; (c) there is reason to believe that the traffic created from Your use of the Services is fraudulent; (d) for scheduled or emergency maintenance; or (e) we reasonably determine that providing the Services is prohibited by applicable law, or how become impractical or unfeasible for any legal or regulatory reason to the provide the Services , and in each instance such suspension is necessary to mitigate any damages resulting from the such actions/causes.

2. RESTRICTIONS AND RESPONSIBILITIES

2.1 **Acceptable Use Policy.** Your access to (and use of) the Sumo Logic Technology is subject to, and conditioned upon, Your acceptance of, and continued compliance with, Sumo Logic's Acceptable Use Policy located at Exhibit B and incorporated herein (the "AUP"). Any entity that directly (or through an affiliate) offers services that compete with the Service will not directly (or indirectly) use or otherwise access the Sumo Logic Technology, unless Sumo Logic provides prior written consent to do so pursuant to a separate document that is signed by an officer of Sumo Logic.

You will promptly notify Sumo Logic in writing of any unauthorized use of the Sumo Logic Technology, in each case that comes to Your attention, and promptly take all reasonable steps necessary to terminate such unauthorized use, including collaborating with Sumo Logic to remediate.

2.2 **Credentials.** You will cooperate with Sumo Logic in connection with the performance of this Agreement by making available such personnel and information as may be reasonably required and taking such other actions as Sumo Logic may reasonably request. You will establish a username and password (or any other means required by Sumo Logic) (collectively "**Account Credentials**") for verifying that only designated employees of You have access to any administrative functions of the Services. You are responsible for all activities (including the use of the Services) performed with the account Credentials and will maintain the security of the Account Credentials.

2.3 **Customer Contact.** You will designate an individual who will have the responsibility to, and the authority of You, to make decisions concerning all matters relating to this Agreement ("**Primary Contact**"). You may change the individual designated as Primary Contact at any time by updating the information in the administration console for the Services.

2.4 **Email Selected for Account.** You choose which email address to use when registering for the Services.

2.5 **Security.** During the Term of this Agreement, Sumo Logic will implement and maintain administrative, physical and technical safeguards and measures designed to protect against unauthorized access to Customer Data. Such security program will conform to the Security Exhibit attached as Exhibit C, and is further described the most recent Service Organization Control 2 (SOC2 Type II) (or substantially similar industry standard report). During the Subscription Term, Sumo Logic will not materially diminish the protections provided by the controls in Exhibit C.

2.6 **Administrators.** Through the Services, You may specify certain users as administrators, who have important rights and controls over Your use of the Services (each an "**Administrator**"). This may include entering into Order Forms; creating, de-provisioning, modifying, or monitoring user roles; setting permission levels; configuring the Services; setting retention or deletion policies as applicable; and overall managing access to Your Sumo Logic account.

2.7 **Customer Controls.** The Services provide a number of controls that You may use as technical and organizational measures to assist in connection with Your obligations. These controls are at both the Administrator and user level. Users also participate in this shared responsibility model by determining which types of data they need to send over to the Services and what types of queries to run, including whether the proposed use cases meet their applicable compliance needs. For clarity, You are responsible for the actions of its Administrator(s) and users. If You wish to have a backup of Your log data, then You may, prior to data ingestion, configure the Services to forward a copy of all Your log data (in standard Sumo Logic format) to an AWS S3 bucket ("**Data Forwarding**"). This feature will not work retroactively and must be configured prior to data ingestion. If You choose to utilize Data Forwarding, then You must: (i) purchase and maintain an AWS S3 Bucket, with such terms between You and AWS; and (ii) provide the credentials to the AWS S3 bucket as required by the Sumo Logic Technology prior to the uploading of Your log data.

3. CONFIDENTIALITY

3.1 **Definition of Confidential Information.** Each party (the "**Recipient**") understands that the other party (the "**Discloser**") has disclosed or may disclose information relating to the Discloser's technology or business ("**Confidential Information**").

3.2 **Protection of Confidential Information.** The Recipient will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care applicable to commercial trade secrets) to: (a) not use any Confidential Information of the Discloser for any purpose outside the scope of this Agreement; and (b) limit access to Confidential Information of the Discloser to those of its employees and contractors who need that access for purposes consistent with this Agreement on behalf of Your end use and who have signed confidentiality agreements with the Recipient containing protections not materially less protective of the Confidential Information than those herein. The foregoing will not apply to any information that the Recipient can document: (i) is or becomes generally available to the public without any action by, or involvement of, the Recipient; (ii) was in its possession or known by it prior to receipt from the Discloser and without a duty of confidentiality; (iii) was rightfully disclosed to it without restriction by a third party; or (iv) was independently developed without use of any Confidential Information of the Discloser.

3.3 **Compelled Disclosures.** Nothing in this Agreement will prevent the Recipient from disclosing the Confidential Information pursuant to any judicial order or subpoena, provided that (to the extent permitted by applicable law) the Recipient gives the Discloser reasonable prior notice of such disclosure to contest such order and limits the amount disclosed to only what is legally required.

3.4 **Data.** "**Customer Data"** means the electronic data or information submitted by You to the Services. Except for such Customer Data, Sumo Logic does not wish to receive any Confidential Information from You that is not necessary for Sumo Logic to perform its obligations under this Agreement, and, unless You and Sumo Logic specifically agree otherwise, Sumo Logic may reasonably presume that any unrelated information received from You is not confidential or Confidential Information. Notwithstanding anything to the contrary, Sumo Logic may: (a) collect and process technical and related information about Your use of the Sumo Logic Technology, which may include (without limitation) page views, session duration, number of unique user logins, ingest volume, search congruency, machine-generated data, and other similar data; and (b) create certain aggregated, de-identified information related to the Services, including information about the Sumo Logic Technology environment, performance, configuration, and other usage information. You authorize Sumo Logic to use such information to support and troubleshoot, provide personalized messages and updates, invoice, analyze trends and benchmark, and administer (as well as test and improve) the Sumo Logic Technology.

3.5 **Permitted Disclosures.** Both parties will have the right to disclose the existence of this Agreement, but not any negotiated terms and conditions of the Agreement, unless such disclosure is approved in writing by both parties prior to such disclosure, is required to be disclosed under Freedom of Information Act, 5 U.S.C. 552, or is included in a filing required to be made by a party with a governmental authority (provided such party will use reasonable efforts to obtain confidential treatment or a protective order) or is made on a confidential basis as reasonably necessary to a party's attorneys, accountants, auditors, financial advisers, creditors, insurers, as well as acquirers, investors, financiers and bona fide potential acquirers, investors and financiers of such party, who are subject to an obligation of confidentiality. If the Order Form is issued under a GSA prime contract, Sumo Logic acknowledges that the ability to use this Agreement in advertising is limited by GSAR 552.203-71.

3.6 **Deletion of Confidential Information.** Upon termination of the Agreement, the Recipient will delete Discloser's Confidential Information, but may retain such information pursuant to its policies for: (a) accounting, tax, billing, audit, and compliance purposes; (b) investigating fraud or unlawful use of the Services; or (c) as required by applicable law, provided such retention, use, and disclosure for the foregoing purposes is subject to the confidentiality obligations under this Section 3 (Confidentiality).

3.7 **Totality of Confidentiality.** For clarity, to the extent the parties have entered into (or enter into) a separate non-disclosure agreement regarding the access to (or use of) the Services, You agree that the terms of this Service Agreement supersede and control.

3.8 **Data Processing Addendum.** To the extent Customer Data includes Personal Data, the parties agree to comply with the terms and conditions of the Data Protection Addendum (plus Standard Contractual Clauses, as applicable) available at: https://www.sumologic.com/customer-data-processing-addendum/ (the "DPA"), which is attached hereto and hereby incorporated by reference.

4. PAYMENT OF FEES

4.1 **Payment of Fees.** You will pay the prime contractor the applicable fees for the Sumo Logic Technology and Training Services as set forth on the Order Form (the "**Fees**") If Your use of the Sumo Logic Technology exhausts or exceeds the total amount of capacity or credits set forth in the applicable Order Form ("Volume"), You may purchase additional Volume at the rate set forth in such Order Form and continue to use Sumo Logic Technology during the Subscription Term. If you do not purchase additional Volume for use during the Subscription Term, You may not continue to use the Sumo Logic Technology unless and until You have purchased additional Volume. Pricing for additional Volume shall be as set forth on the Order Form

4.2 Reserved**.**

4.3Reserved**.**

4.4Reserved**.**

4.5 Reserved**.**

4.6 Reserved**.** [

4.7 **Purchase Orders.** No purchase orders sent by You will be deemed to modify or otherwise supplement this Agreement unless Sumo Logic has agreed to such changes, in writing.

4.8 **Resellers.** If You obtain the Services from a reseller authorized by Sumo Logic ("**Reseller**") through an Order Form executed with Reseller, then any fees, including refunds and credits, will solely be by and between Reseller and You. Reseller is not authorized to make any changes to this Agreement or bind Sumo Logic to any additional or different terms or conditions. For the avoidance of doubt, nothing in this Section 4.8 (Resellers) affects suspension rights or deactivation rights for Sumo Logic or a Reseller.

5. TERMINATION

5.1 **Term.** Each Order Form will define the specific duration of access to the Services (each a "**Subscription Term**"). The term of this Agreement commences on the date of the Subscription Term and continues until the Subscription Term for each Order Form has expired or has been terminated (the "**Term**").

5.2 **Renewal.** Except as otherwise specified in Your Order Form, the Subscription Term for an annual plan will be for one year. All renewals are subject to the applicable Services continuing to be offered and will be charged at the then-current GSA Schedule rates.

5.3 **Termination for Cause.** When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Sumo Logic shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer..

5.4 **Effect of Termination.** Upon termination of Agreement, all Your Data will automatically enter the deletion queue or if not technically feasible certified as non-recoverable/non-retrievable. The following Sections survive any expiration or termination of this Agreement: 1.4 (Intellectual Property), 1.5 (Feedback), 2.1 (Acceptable Use Policy), 3 (Confidentiality), 4 (Payment of Fees), 5.4 (Effect of Termination), 6 (Warranties), 7 (Warranty Disclaimer), 8 (Liability), 9 (Indemnification), and 11 (General Provisions).

5.5 **Refund or Payment upon Termination.** If this Agreement is terminated by, then Sumo Logic will refund You any prepaid Fees covering the remainder of the Subscription Term after the effective date of the termination.

6. WARRANTIES

6.1 **Mutual Warranty.** Each party represents that it has validly entered into this Agreement and that it has the power and authority to do so.

6.2 **Sumo Logic Warranty.** Sumo Logic warrants that the Training Services will be performed using commercially reasonable care and skill in all material respects. YOUR SOLE AND EXCLUSIVE REMEDY FOR SUMO LOGIC'S BREACH OF THIS WARRANTY WILL BE THE CORRECTION OF THE DEFICIENT TRAINING SERVICES THAT CAUSED THE BREACH OF THE WARRANTY, OR, IF SUMO LOGIC CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALLY REASONABLE MANNER, YOU MAY TERMINATE THE APPLICABLE ORDER FORM(S) FOR THE TRAINING SERVICES. SUMO LOGIC WILL HAVE NO OBLIGATION WITH RESPECT TO A WARRANTY CLAIM UNLESS NOTIFIED OF SUCH CLAIM WITHIN FIVE (5) DAYS OF THE FIRST INSTANCE OF ANY MATERIAL PROBLEM. THE WARRANTIES SET FORTH IN THIS SECTION 6.2 (SUMO LOGIC WARRANTY) ARE MADE TO AND FOR THE BENEFIT OF YOU ONLY. SUCH WARRANTIES WILL ONLY APPLY IF THE APPLICABLE SERVICES HAS BEEN UTILIZED IN ACCORDANCE WITH THIS AGREEMENT AND APPLICABLE LAW.

6.3 **Customer Warranty.** You represent and warrant that You have not relied on any other warranties or representations concerning Sumo Logic or the Sumo Logic Technology.

7. WARRANTY DISCLAIMER

EXCEPT AS OTHERWISE EXPRESSLY STATED IN THIS AGREEMENT (OR OTHERWISE REQUIRED BY APPLICABLE LAW WITHOUT POSSIBILITY OF CONTRACTUAL WAIVER): SUMO LOGIC AND ITS LICENSORS AND THIRD PARTIES EXPRESSLY DISCLAIM AND EXCLUDE ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE OR USE, AND WARRANTIES IMPLIED FROM A COURSE OF DEALING OR COURSE OF PERFORMANCE OR USAGE OF TRADE; AND, THE SUMO LOGIC TECHNOLOGY, REPORTS, AND ANY OTHER INFORMATION IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OR CONDITION OF ANY KIND. WITHOUT LIMITING THE FOREGOING, SUMO LOGIC AND ITS LICENSORS AND THIRD PARTIES DO NOT REPRESENT OR WARRANT TO YOU THAT: (A) YOUR USE OF THE SUMO LOGIC TECHNOLOGY WILL MEET YOUR REQUIREMENTS OR EXPECTATIONS, (B) YOUR USE OF THE SUMO LOGIC TECHNOLOGY WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR, (C) ALL ERRORS WILL BE CORRECTED, AND (D) DATA PROVIDED THROUGH THE SUMO LOGIC TECHNOLOGY WILL BE ACCURATE. SUMO LOGIC AND ITS LICENSORS AND THIRD PARTIES ARE NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SUMO LOGIC TECHNOLOGY THAT ARISE FROM YOUR DATA, OR THIRD-PARTY DATA, OR SERVICES PROVIDED BY THIRD PARTIES, OR TRANSMISSION OF DATA OVER NETWORKS THAT SUMO LOGIC DOES NOT OWN, OPERATE OR CONTROL.

8. LIABILITY

8.1 **Limitation of Liability.**

IN NO EVENT WILL EITHER PARTY'S TOTAL AND CUMULATIVE LIABILITY, FOR ALL CLAIMS OF ANY NATURE ARISING OUT OF THIS AGREEMENT (INCLUDING ANY ANCILLARY AGREEMENT) EXCEED THE TOTAL FEES PAID BY THE PRIME CONTRACTOR OR RESELLER TO SUMO FOR THE PRODUCT(S) OR SERVICES ON THE ORDER GIVING RISE TO THE CLAIM UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PROCEEDING THE OCCURRENCE OF THE FIRST EVENT GIVING RISE TO A CLAIM UNDER THIS AGREEMENT. FOR CLARITY, THE EXISTENCE OF MORE THAN ONE CLAIM WILL NOT ENLARGE THIS LIMIT. TO THE EXTENT THAT YOUR LIABILITY IS LIMITED IN ANY WAY, INCLUDING, FOR EXAMPLE, UNDER THE ANTI-DEFICIENCY ACT, SUMO LOGIC'S LIABILITY WILL BE LIMITED TO THE SAME AMOUNT.

8.2 **Liability Exclusions.**

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN SECTION 8.1 (LIMITATION OF LIABILITY), AND SUBJECT TO THE ANTI-DEFICIENCY ACT, NOTHING SHALL RESTRICT (OR OTHERWISE LIMIT) THE LIABILITY FOR: (A) INDEMNIFICATION OBLIGATION UNDER SECTION 9 (INDEMNIFICATION), (B) BREACH OF SECTION 1.4 (INTELLECTUAL PROPERTY), (C) BREACH OF SECTION 2.1 (ACCEPTABLE USE POLICY), AND (D) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE, WILLFUL MISCONDUCT OR FRAUD.

8.3 **Reseller Liability.**

NOTWITHSTANDING ANYTHING TO THE CONTRARY, SUMO LOGIC WILL HAVE NOT LIABILITY FOR ANY REFUND THAT, IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT, IS TO BE PAID BY RESELLER.

8.4 **Exclusion of Consequential Damages and Related Damages.**

IN NO EVENT WILL EITHER PARTY BE LIABLE FOR DAMAGES FOR LOSS OF PROFIT OR REVENUE, DATA THAT IS LOST OR CORRUPTED, LOSS OF GOODWILL, OR ANY OTHER SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES SUFFERED BY THE OTHER PARTY OR OTHERS.

THE PARTIES ACKNOWLEDGE THAT THE FEES, EXCLUSIONS, DISCLAIMERS AND LIMITATIONS OF LIABILITY SET FORTH IN THIS AGREEMENT ARE ESSENTIAL COMPONENTS OF THIS AGREEMENT AND FORM THE BASIS FOR DETERMINING THE PRICE CHARGED FOR THE SERVICES, AND THAT EACH PARTY WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON ITS LIABILITY. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

9. INDEMNIFICATION

9.1 **Sumo Logic Indemnity.** Sumo Logic will have the right to intervene to defend You against any third-party claim, action, proceeding or suit, to the extent that the Services infringes or misappropriates the intellectual property rights of any person and will pay for the resulting costs and damages finally awarded against You to such third party by a court of competent jurisdiction or agreed to in settlement by Sumo Logic. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

9.2 **Conditions.** Sumo Logic will have no obligation or liability with respect to the foregoing for any actual or alleged infringement to the extent arising from or relating to: (a) Free Products; (b) Your Data or Your breach of this Agreement; (c) use of the Sumo Logic Technology other than in accordance with this Agreement; (b) modification of the Sumo Logic Technology by someone other than Sumo Logic; (d) combination of the Sumo Logic Technology with any other products, services, or materials, or (e) Your failure to implement required updates to the Sumo Logic Technology as requested by Sumo Logic. If Sumo Logic believes Your use of the Sumo Logic Technology may be enjoined, then Sumo Logic may, at its sole option and expense and as Your sole remedy, either (i) procure for You a license to continue using the Sumo Logic Technology in accordance with the terms of this Agreement; (ii) replace or modify the allegedly infringing Sumo Logic Technology to avoid the infringement; or (iii) terminate the applicable Order Form(s), directly or thru the applicable Reseller, and refund any unused prepaid Fees paid by You under the applicable Order Form(s). SECTION 9.1 (SUMO LOGIC INDEMNITY) AND SECTION 9.2 (CONDITIONS) STATE THE ENTIRE LIABILITY OF SUMO LOGIC AND THE SOLE REMEDY FOR YOU IN CONNECTION WITH ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

9.3 **Exclusion.** Sumo Logic will have no obligation or liability with respect to the foregoing for any actual or alleged infringement if the total aggregate Fees received with respect to the Services in the twelve (12) month period immediately preceding the first claim is less than fifty thousand US dollars ($50,000.00 USD).

9.4 **Exclusion in Lieu of Indemnity.** Sumo Logic and its directors, employees, licensors and agents will have no liability to You or any third party for any Losses arising from or relating to Your unauthorized use of the Services or Sumo Logic Technology, violation of any applicable law or violation of any third party right.

9.5 **Indemnification Process.** The obligations set forth in this Section 9 (Indemnification) apply only if: (a) the indemnified party notifies the indemnifying party in writing of any claim promptly upon learning of or receiving the same; (b) the indemnified party provides the indemnifying party with reasonable assistance requested by the indemnifying party, at the indemnifying party's reasonable and documented expense, for the defense and settlement, if applicable, of any claim; and (c) the indemnified party provides the indemnifying party with the exclusive right to control and the authority to settle any claim, provided, however, that: (i) the indemnifying party will not settle any claim that admits fault or liability of the indemnified party without the indemnified party's prior written consent (which shall not be unreasonably withheld, conditioned or delayed); and (ii) the indemnified party will have the right to participate in the matter at its own expense. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

10. GOVERNMENT MATTERS

10.1 **Export Compliance.** The Sumo Logic Technology is subject to export restrictions by the United States government and may be subject to import restrictions by certain foreign governments. You will comply with applicable export and import laws and regulations (including "deemed export" and "deemed re-export" regulations). You will not (and will not allow any third-party to) remove or export from the United States or allow the export or re-export of any part of the Sumo Logic Technology or any direct product thereof: (a) into (or to a national or resident of) any embargoed or terrorist-supporting country; (b) to anyone on the U.S. Commerce Department's Denied Persons, Entity, or Unverified Lists or the U.S. Treasury Department's list of Specially Designated Nationals and Consolidated Sanctions list (collectively, "**Prohibited Persons**"); (c) to any country to which such export or re-export is restricted or prohibited, or as to which the United States government or any agency thereof requires an export license or other

governmental approval at the time of export or re-export without first obtaining such license or approval; or (d) otherwise in violation of any export or import restrictions, laws or regulations of any United States or foreign agency or authority. You represent and warrant that (i) it is not located in, under the control of, or a national or resident of any such prohibited country and (ii) no Customer Data is controlled under the U.S. International Traffic in Arms Regulations or similar Laws in other jurisdictions. You also certify that it is not a Prohibited Person nor owned, controlled by, or acting on behalf of a Prohibited Person. You will not to use or provide the Sumo Logic Technology for any prohibited end use, including (without limitation) to support any nuclear, chemical, or biological weapons proliferation, or missile technology, without the prior permission of the United States government.

10.2 U.S. Government Rights. The Sumo Logic Technology and Deliverables are "commercial products" and "commercial services" as defined at FAR 2.101. If You are the US Federal Government (Government) Executive Agency (as defined in FAR 2.101), Sumo Logic provides the Sumo Logic Technology and Deliverables, including any related technical data, and/or professional services in accordance with the following: If acquired by or on behalf of any Executive Agency (other than an agency within the Department of Defense (DoD), the Government acquires, in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software), only those rights in technical data and software customarily provided to the public as defined in this Agreement. If acquired by or on behalf of any Executive Agency within the DoD, the Government acquires, in accordance with DFARS 227.7202-3 (Rights in commercial computer software or commercial computer software documentation), only those rights in technical data and software customarily provided in this Agreement. In addition, DFARS 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by DoD agencies. Note, however, that Subpart 227.72 does not apply to computer software or computer software documentation acquired under GSA schedule contracts. Any Federal Legislative or Judicial Agency shall obtain only those rights in technical data and software customarily provided to the public as defined in this Agreement. If any Federal Executive, Legislative, or Judicial Agency has a need for rights not conveyed under the terms described in this Section, it must negotiate with Sumo Logic to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement to be effective. If this Agreement fails to meet the Government's needs or is inconsistent in any way with Federal law, and the parties cannot reach a mutual agreement on terms for this Agreement, the Government agrees to terminate its use of the Sumo Logic Licensed Technology and any Deliverables and return the Licensed Technology and Deliverables, including documentation and any other software or technical data delivered as part of the Sumo Logic Technology and Deliverables, unused, to Sumo Logic. This U.S. Government Rights clause in this Section is in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in computer software or technical data under this Agreement.

11. GENERAL PROVISIONS

11.1 **Betas.** From time-to-time, Sumo Logic may offer certain Sumo Logic Technology at no charge, including alphas, betas, non-GA, limited release, developer preview, and any such similarly designated services, product features, or documentation (collectively "**Betas**"). Such Betas are subject to the agreement that accompany such Betas and not part of the procurement. You may, at Your option, elect to participate in Betas. In the event You so elect, then Your use of Betas is subject to the agreement accompanying such Betas and is only permitted during the designated term of such Beta (which in any event will terminate to the extent a Beta is made generally available). Betas may be modified or terminated at any time and for any reason in Sumo Logic's sole discretion, without liability. You acknowledge that Betas are still under development, may be inoperable or incomplete, and are likely to contain more errors and bugs than generally available Sumo Logic Technology. There is no commitment that: (a) any Beta will be made generally available; or (b) if made generally available, that it will be substantially similar to the Beta. You will use commercially reasonable efforts to notify Sumo Logic of any bugs or issues in the Betas. All information regarding a Beta is Sumo Logic Confidential Information.

11.2 **Free Products.** We may offer certain Sumo Logic Technology to You at no charge, including free accounts, trial use, and Betas (collectively "**Free Products**"). Use of Free Products is subject to the agreement accompanying such Free Products and not part of the procurement. We may modify or terminate Your right to use Free Products at any time and for any reason in our sole discretion, without liability to You. Sumo Logic will have no liability whatsoever for any harm or damage arising out of or in connection with Free Products. The Free Products are provided "as is" without any warranty. SUMO LOGIC EXPRESSLY DISCLAIMS ALL OBLIGATIONS OR LIABILITIES WITH RESPECT TO FREE PRODUCTS, INCLUDING ANY SUPPORT, WARRANTY AND INDEMNIFICATION OBLIGATIONS. NOTWITHSTANDING ANYTHING TO THE CONTRARY, SUMO LOGIC'S MAXIMUM AGGREGATE LIABILITY TO YOU IN RESPECT TO FREE PRODUCTS WILL BE ONE HUNDRED DOLLARS ($100.00 USD).

11.3 **Entire Agreement.** This Agreement constitutes the entire agreement between You and Sumo Logic with respect to the subject matter and supersedes and merges all prior proposals, understandings and contemporaneous communications by and between us, however, these terms and conditions do not alter the prime contract terms and conditions which are between You and the prime contractor. Sumo Logic is not a party to the prime contract. This Agreement may not be modified except by written agreement of both parties.

11.4 **Assignment.** You will not assign the Agreement (or any of Your rights or obligations), except with the express written consent of Sumo Logic, and any attempted assignment in violation of this paragraph is void**.** Subject to the requirements of FAR 42.12, Sumo Logic may assign the Agreement or delegate its obligations under this Agreement without restriction. Sumo Logic may utilize subcontractors in the performance of its obligations under the Agreement.

11.5 **Relationship of the Parties.** The parties are independent contractors; and, this Agreement does not create or imply any partnership, agency or joint venture.

11.6 **Publicity.** During the Term of the Agreement, Sumo Logic may reference You as a customer in marketing, promotional materials and public statements, subject to trademark and logo usage guidelines provided by You. If the Order Form is issued under a GSA prime contract, Sumo Logic acknowledges that the ability to use this Agreement in advertising is limited by GSAR 552.203-71.

11.7 **Severability; No Waiver.** If any provision (or any part thereof) of this Agreement is unenforceable under or prohibited by any present or future law, then such provision (or part thereof) will be amended, and is amended, so as to be in compliance with such law, while preserving to the maximum extent possible the intent of the original provision. Any provision (or part thereof) that cannot be so amended will be severed from this Agreement; and, all the remaining provisions of this Agreement will remain unimpaired. A waiver of any provision of this Agreement must be signed by the waiving party; and, one waiver will not imply any future waiver.

11.8 **Force Majeure.** In accordance with FAR Clause 52.212-4(f), Neither party will be liable for, or be considered to be in breach of or default under this Agreement on account of, any delay or failure to perform as required by this Agreement (other than monetary obligations) as a result of any cause or condition beyond such party's reasonable control including, but limited to, acts of God, labor disputes or other industrial disturbances, electrical or power outages, utilities or other telecommunication failures, fires, floods, acts of terror, earthquakes, storms or other elements of nature, blockages, embargoes, riots, acts or orders of governments, acts of terrorism, or war.

11.9 **Changes to this Service Agreement.** Sumo Logic may request modification to the terms and conditions of this Service Agreement from time-to-time, with notice to You and such modifications will not be effective until agreed to by You, in writing. **(i) Free Products.** You must accept the modifications to continue to use the Free Products. If You object to the modifications, Your exclusive remedy is to cease using the Free Products. **(ii) Paid Subscriptions.** Modifications to this Service Agreement will take effect upon Your acceptance of the modified terms.

11.10 **Changes to Services.** You acknowledge that the Services are on-line, subscription-based products, and that in order to provide improved customer experience Sumo Logic may make changes to the Services, and may update the applicable documentation accordingly, however, such changes will not materially change the Services purchased by You during the then-current Subscription Term.

11.11 **Governing Law and Venue.** This Agreement will be governed by and construed in accordance with the Federal laws of the United States, without regard to or application of any conflicts of law rules or principles and without regard to the United Nations Convention on the International Sale of Goods.

11.12 **Dispute Resolution and Arbitration.** Disputes between You and Sumo Logic are governed by the Contract Disputes Act.

11.13 **Injunctive Relief.** Notwithstanding the provisions of Section 11.11 (Governing Law and Venue) and 11.12 (Dispute Resolution and Arbitration), nothing in this Agreement will prevent Sumo Logic from seeking injunctive relief with respect to a violation of intellectual property rights, confidentiality obligations or enforcement or recognition of any award or order in any appropriate jurisdiction.

11.14 **Notices.** Any notice or other communication under this Agreement given by any party to any other party must be in writing and will be effective upon delivery as follows: (a) if to You, (i) when delivered via registered mail, return receipt requested, to the address specified in the Order or otherwise on record for You; or (ii) when sent via email to the email address specified in an Order Form (or otherwise on record for You); and (b) if to Sumo Logic, when sent via registered mail, return receipt requested, to Sumo Logic at Sumo Logic, 855 Main St., Suite 100 Redwood City, CA 94063 or such other address which Sumo Logic may specify from time to time, with a copy to legal@sumologic.com.

Exhibit A
SUPPORT AND MAINTENANCE SERVICES ADDENDUM

This Support and Maintenance Services Addendum ("**Support Addendum**") amends the terms and forms part of the Sumo Logic Terms of Use, Master Service Agreement, or other applicable agreement governing access to the Services (collectively, the "**Master Agreement**") entered into between Sumo Logic, Inc. ("**Sumo Logic**") and Customer.

Effective as of May 27, 2020

1. DEFINITIONS. Capitalized terms not defined in this Support Addendum have the same meaning as in the Master Agreement.

- "**Business Days**" are Monday to Friday during Business Hours, excluding Sumo Logic company holidays.
- "**Business Hours**" are Pacific Time (PT): 6am – 6pm; Greenwich Mean Time (GMT): 8am – 5pm; and Australian Eastern Time (AEST): 8am – 5pm.
- "**Certified Support Contact**" means an individual designated as the Customer contact person who will be: (a) a point of contact responsible for all communications with Sumo Logic regarding Support, including Error submission and resolution; (b) a certified support contact should possess level 1 Fundamentals Certification and level 2 Search Mastery Certification (or their then equivalent Sumo Logic certifications); (c) have the necessary expertise and administrative access to help diagnose and resolve Errors with the direction of Sumo Logic Support; and (d) authorized by Customer to request and receive Support for the Services on behalf of Customer.
- "**E-mail support**" means the ability provided Customer to make requests for technical support assistance by e-mail at any time concerning the use of the then current release of a Product. Any requests submitted by email will receive a default priority of P3 - Normal.
- "**Error**" means a reproducible issue or problem affecting the functionality of the Services for Customer.
- "**First Level Support**" means any support relating to calls or questions from Customer's customers, users, or general resolution of user errors, network errors, provisioning errors, or Internet delays or malfunctions.
- "**Initial Response Time**" means the targeted time period within which Sumo Logic will use commercially reasonable efforts to acknowledge receipt of an Error reported by Customer.
- "**Online Support**" means information available through Sumo Logic's website (https://support.sumologic.com), including frequently asked questions, and error reporting.
- "**Open Source Software**" means any software that is licensed under any open source, freeware, shareware, or similar licensing or distribution models.
- "**Services**" means the internet-based services specified on the applicable Order Form(s).
- "**Sumo Logic Technology**" means the Services and any software applications provided by Sumo Logic to Customer.
- "**Support**" means the support services to be provided by Sumo Logic to the Customer in accordance with the Support Level selected by Customer for the Subscription Term.
- "**Support Level**" means the level of Support (Standard Support formerly known as Professional Support, Enterprise Support or Premium Support) that has been selected by the Customer on the Order Form.
- "**Workaround**" means a change in the procedures followed or data supplied by Customer to avoid an Error without substantially impairing Customer's use of the Service.

2. ERROR PRIORITY DEFINITIONS. Upon receipt of an Error report from a Certified Support Contact, Sumo Logic will: (i) work with Customer to set a priority level; (ii) analyze the Error and verify the existence of the problem; and (iii) provide Customer direction and assistance in resolving a confirmed Error. Priority levels may initially be set by Customer. Sumo Logic may reclassify priority levels based on the current impact on the Sumo Logic Technology. Response and remediation of any reported Errors is dependent upon Customer's timely cooperation as well as accuracy and completeness of information provided regarding the Error. In order to validate and address Errors, Sumo Logic also depends upon Customer following guidance on problem determination, analysis and remediation.

- Priority 1 – Urgent ("**P1**") means an Error that is: (a) preventing all users from accessing the Services; (b) no procedural workarounds exist; (c) and one of the following is true:
    - Services are completely down and unavailable (excluding a scheduled downtime).
    - All data ingest to the Customer has stopped.
    - The ability to search is unavailable, where all search queries performed by users result in an error and/or no data is returned for any queries.
- Priority 2 – High ("**P2**") means an Error that (a) is impacting a majority of Customer's users; (b) users are able to perform their job responsibilities in a limited capacity but no reasonable workaround exists; and (c) one of the following is true:
    - Data ingest is significantly delayed or has stopped for a portion of data.
    - Search is operational but there is a significant performance degradation or exceptions are seen across a large number of searches.
    - Errors that result in the inability to register (or otherwise set up) any new Collectors.
- Priority 3 – Normal ("**P3**") means an Error that (a) is impacting a minority of Customer users; (b) users are able to perform their job responsibilities with minimal impact and short-term workarounds are available; and (c) one of the following is true:
    - Service is up but a critical documented feature is marginally impacted.
    - Search is operational but there is a minor performance degradation; some specific search queries result in exceptions.

    - Errors that result in the inability to update configurations to existing Collectors or Sources.
    - Collector is registering as down but is actually collecting and sending data.
- Priority 4 – Low ("**P4**") means an Error that is (a) anything else; (b) any general product or how-to questions, such as query writing or account configuration questions; (c) scheduled downtime questions; or (d) issues in help and/or support documentation.

3. SUPPORT COVERAGE AND RESPONSE TIME TARGETS.

3.1 SUPPORT COVERAGE. Support consists of (a) response to Error reports provided to a Certified Support Contact concerning the use of the Sumo Logic Technology; (b) E-mail Support; (c) Online Support; and (d) Sumo Logic Technology updates that Sumo Logic in its discretion makes generally available to its Support customers without additional charge. All Support will be provided in the English language. Each Support Level permits up to 5 Certified Support Contacts.

Permitted number of Certified Support Contacts: 5.

3.2 SUPPORT HOURS.

Priority	**Standard**	**Enterprise**	**Premium**
P1	Business Hours	24x7	24x7
P2	Business Hours	Business Hours	24x7
P3	Business Hours	Business Hours	Business Hours
P4	Business Hours	Business Hours	Business Hours

3.3 RESPONSE TIME TARGETS. Sumo Logic shall exercise commercially reasonable efforts to provide the Initial Response Time to Errors reported by Customers in accordance with the priority level.

Priority	**Standard**	**Enterprise**	**Premium**
P1	1 Hour	1 Hour	0.5 Hour
P2	4 Hours	4 Hours	2 Hours
P3	1 Day	1 Day	6 Hours
P4	2 Days	2 Days	1 Day

3.4 CUSTOMER OBLIGATIONS. Error reports will, if applicable, include the following: (a) Customer's identification number, if a case has already been created; (b) a reproducible test case with instructions that allow Sumo Logic to reproduce the Error; (c) the exact wording (or screenshots) of related error messages; (d) a description of the Error and expected results; and (e) any additional or unique circumstances surrounding the discovery of the Error. Customer is solely responsible for determining which information it decides to share with Sumo Logic for the identification and remediation of any Errors. To aid in identified and remediation, if applicable, Customer will collaborate with Sumo Logic to address the reported Error.

Sumo Logic may share such information regarding Errors and remediations with its contractors, vendors and partners to support Sumo Logic's provision of the Support.

3.5 TERM. This Support Addendum will be effective for the Subscription Period provided on the applicable Order Form for Support. Notwithstanding anything to the contrary, this Support Addendum will terminate upon expiration or termination of the Master Agreement. During the initial Subscription Term (and any elected renewals) for Support, Customer will purchase and maintain the Support Level for all its users. For clarity, Customer may not elect to purchase (or renew) Support for just a portion of its Services or of its users.

4. PREMIUM SUPPORT TECHNICAL ACCOUNT MANAGER ("TAM").

As part of the Premium Support plan, Customer Certified Support Contacts have access to a named TAM during the TAM's standard Business Hours in the TAM's local time zone. Customer and TAM will make reasonable efforts to find mutually agreeable times for meetings and assistance. TAMs are not dedicated to a single Customer. For clarity, the Initial Response Time does not apply to TAM correspondence.

TAMs participate in a variety of Customer success activities in collaboration with Customer over the Subscription Term that are on a use-it-or-lose-it basis that do not accumulate if not used, and are as follows:

- Recurring Status Calls - TAM may participate in up to 2 recurring status calls per month to review account status, open issues and guidance.
- Customer Success Plan - Parties may work together to create a Customer Success Plan (defining actions, owners and target dates in order to optimize Customer's Sumo Logic environment and achieve maximum value) that Customer can choose to leverage for their internal use and implementation.
- Onsite Training – TAM may deliver 1 day of onsite or online training per subscription year, as reasonably agreed upon between Sumo Logic and Customer, where additional Fees may be required and will be agreed upon in advance. Training follows a standard agenda, but TAM may work with Customer to tailor the agenda to the applicable audience.
- Data Ingest Strategy - Parties may work together to establish a data ingest strategy defining data sources, collection options, and meta data design.
- Technical Health Check - TAM may review Customer's account usage and provide feedback on optimization opportunities, feature usage, adoption and best practices.
- Lunch and Learn Sessions - TAM may deliver an abbreviated virtual product overview training to Customer's users followed by a question & answer session. Training agenda may be customized if mutually agreed by the parties. This is not to exceed one Lunch and Learn Session per quarter.
- Product Feedback Loop - TAM may work with Customer to gather product requests/feedback and present them to Sumo Logic product management, where Customer acknowledges that Sumo Logic determines the product roadmap.
- Onsite Visits - TAM may visit Customer on-site for business review, strategic planning sessions and other activities mutually agreed by the parties in writing, where additional Fees may be required and will be agreed upon in advance. Not to exceed 1 business day per visit and 2 visits per year. Additional onsite time is available at the then-current consulting rates.
- Data Onboarding - TAM may assist Customer with basic set-up such as adding additional data sources via standard documented collection methods. TAM may also create an example content (dashboard or scheduled search) to demonstrate the value of the data source.

5. EXCLUSIONS.

1. Support does not include:
   i. Support for users other than Certified Support Contacts;
   ii. Support for instances of Services without a valid support agreement;
   iii. Training Services, unless expressly identified in this Support Addendum (separately available through Order Forms);
   iv. Support for 3rd party add-ons;
   v. End of life offerings;
   vi. Betas (public or private Betas);
   vii. Open-Source Software;
   viii. Feature requests, or additional commitments from the product or development teams; and
   ix. Remote administration

2. Further, Sumo Logic shall have no obligation to Support with respect to or in the case of: (i) altered or damaged Software; (ii) problems with the Sumo Logic Technology caused by Customer's negligence, abuse or misapplication, or unauthorized use of Sumo Logic Technology other than as specified in the Sumo Logic's documentation or other causes beyond the control of Sumo Logic; or (c) use of the Services that is not in compliance with the Master Agreement.

3. If Sumo Logic believes that a problem reported by Customer may not be due to an Error in the Sumo Logic Technology, Sumo Logic will so notify Customer. At that time, Customer may (1) instruct Sumo Logic to proceed with problem determination at its possible expense as set forth below, or (2) instruct Sumo Logic that Customer does not wish the problem pursued at its possible expense. If Customer requests that Sumo Logic proceed with problem determination at its possible expense and Sumo Logic determines that the error was not due to an Error, Customer shall pay Sumo Logic, at Sumo Logic's then-current consulting rates, for all work performed in connection with such determination, plus reasonable related expenses incurred therewith.

   If Customer instructs Sumo Logic that it does not wish the problem pursued at its possible expense or if such determination requires effort in excess of Customer's instructions, Sumo Logic may, at its sole discretion, elect not to investigate the Error with no liability therefor.

   For clarity, Sumo Logic may offer Training Services to help resolve issues that fall outside the scope of Support. Any engagement of Training Services will be provided under a separate agreement and will be subject to the Master Agreement.
4. Sumo Logic shall have no liability for any changes in Customer's hardware or software systems that may be necessary to use the Sumo Logic Technology due to a Workaround or maintenance.

6. REVISED TERMS AND CONDITIONS. Sumo Logic may non-materially revise this Support Addendum at any time and will notify Customer of any such revision. Notification may occur via email and/or be posted on the Customer account. If Customer does not accept said non-material revisions, then Customer must notify Sumo Logic in writing within 30 days of the date of Sumo Logic's notification of the proposed changes. If Customers does notify Sumo Logic, then the Support will continue to be governed by the last Support Addendum that Customer accepted until the end of Customer's then current Subscription Term,. Notwithstanding anything to the contrary, in the event Sumo Logic revises this Support Addendum, Customer will not be entitled to any additional benefits or services offered thereunder absent the payment to Sumo Logic or resellers of the appropriate Fee related to said revision, if any.

7. MISCELLANEOUS. Notwithstanding anything to the contrary, scheduled downtime shall not be deemed an Error. The terms of this Support Addendum will control to the extent there is any conflict between terms of this Support Addendum and the terms of the Master Agreement. Except as specifically amended and modified by this Support Addendum, the terms and provisions of the Master Agreement remain unchanged and in full force and effect. Except as otherwise expressly provided herein, no supplement, modification or amendment of this Support Addendum will be binding, unless executed in writing by a duly authorized representative of each party to this Support Addendum. You acknowledge and agree that Sumo logic may add to or change the terms of this Support Agreement or the Support Benefits Terms from time to time, provided that, Sumo Logic will provide at least 30 days' notice of the additions or changes before the additions or changes are effective as to Customer.

Note: Key update from prior version (September 16, 2019): the Support Plan naming convention for Professional Support changed to Standard Support. All prior references to Professional Support are now replaced with Standard Support.

Exhibit B
Acceptable Use Policy

Customer will promptly notify Sumo Logic in writing of any unauthorized use of the services under this AUP (in each case that comes to customer's attention) and promptly take all reasonable steps necessary to terminate such unauthorized use, including collaborating with Sumo Logic to remediate.

Customer will not, and will not encourage, permit or assist any third party to:

- Circumvent any usage or access limits on the use of the services.
- Create multiple accounts, including online or otherwise, to access the services in a manner intended to void incurring fees.
- Intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other item of a destructive or deceptive nature.
- Make the services available to any third party (via a services arrangement, service bureau, lease, sale, resale, or otherwise) or use such for any purpose other than its own internal business purposes.
- Damage, disable, overburden, impair, or disrupt the services or attempt to gain unauthorized access to any systems or networks that connect thereto or otherwise interfere with the operation of the services or in any way with the use or enjoyment of the services by others.
- Perform or disclose network discovery, port and service identification, vulnerability scanning, password cracking, or penetration testing of the services (without first obtaining Sumo Logic's written consent).
- Use the services other than in accordance with the Agreement and in compliance with all applicable laws and regulations (including but not limited to any European or local privacy laws to the extent applicable to customer).
- Use the services in a manner that violates any third-party rights (including, without limitation, intellectual property and privacy rights).
- Promote, facilitate, or encourage illegal activity.
- Access or use the services in order to create a product or service competitive with the services.
- Copy any features, functionality, or graphics of the services.
- Remove any copyright, trademark, or other proprietary rights notices contained in or on the services or reformat (or frame) any portion of the web pages that are part of the service's administration display.
- Use the services in connection with any real-time control system (including any aviation, mass transit, medical or nuclear application) or any other application that could result in death, personal injury, catastrophic damage or mass destruction.
- Use any services in any manner that would disparage Sumo Logic.
- To the extent the following restriction is permitted by applicable law, access or use the services for purposes of evaluating the availability, performance or functionality of the services, or for any other benchmarking or competitive purposes.
- Create, train or improve (directly or indirectly) a substantially similar product or service, including machine learning engine.
- Reverse engineer (except to the extent statutory law expressly prohibits or limits restrictions on reverse engineering and, in which instance, customer will provide notice to Sumo Logic so that Sumo Logic can respond and assist with such request), decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the services, documentation or data related to the services.
- Modify, translate, or create derivative works based on the services.

Exhibit C
Security Exhibit

1. **Purpose.** This Security Exhibit sets forth the information security program and infrastructure policies that Sumo Logic will meet and maintain in order to protect Customer Data from unauthorized use, access or disclosure, during the term of the Agreement.
2. **Information Security Management Program.** Sumo Logic will maintain throughout the Term of the Agreement an information security management program (the "**ISMP**") designed to protect and secure Customer Data from unauthorized access or use. The ISMP will be documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices and industry standards.
3. **Standards.** Sumo Logic incorporates commercially reasonable and appropriate methods and safeguards to protect the security, confidentiality, and availability of Customer Data. Sumo Logic will, at a minimum, adhere to applicable information security practices as identified in International Organization for Standardization 27001 (ISO/IEC 27001) (or a substantially equivalent or replacement standard) or other authoritative sources (e.g. SOC2).
4. **Independent Assessments.** On an annual basis, Sumo Logic has an independent third-party organization conduct an independent assessment consisting of a Report on Controls at a Service Organization Relevant to Security, Availability, Processing, Integrity, Confidentiality and/or Privacy (SOC2 Type II) or such other assessment at its sole discretion (e.g. ISO 27001 Certificate). Additionally, Sumo Logic undergoes regular penetration testing from independent third parties at least on an annual basis.
5. **Information Security Policies.** Sumo Logic will implement, maintain, and adhere to its internal information security and privacy policies that address the roles and responsibilities of Sumo Logic's personnel, including both technical and non-technical personnel, who have direct or indirect access to Customer Data in connection with providing the Services. All Sumo Logic personnel with access to Customer Data will receive annual training on Sumo Logic's ISMP.
6. **Information Security Infrastructure.**
    1. **Access Controls**. Sumo Logic will ensure appropriate access controls are in place to protect Customer Data. Sumo Logic agrees that it shall maintain, throughout the Term of the Agreement and at all times while Sumo Logic has access to or possession of Customer Data, appropriate access controls (physical, technical, and administrative) and shall maintain such access controls in accordance with Sumo Logic's policies and procedures.
    2. **Encryption**. Sumo Logic will encrypt Customer Data at rest within the Services. Sumo Logic will use at a minimum AES algorithm for encryption of Customer Data at rest with a default value of 256-bit strength. Customer Data processed in transit within the Services will be protected using TLS 1.2 encryption or stronger.
    3. **Network and Host Security**. Sumo Logic has network intrusion detection and firewalls in place. Sumo Logic uses reasonable efforts to ensure that the Services' operating systems and applications that are associated with Customer Data are patched or secured to mitigate the impact of security vulnerabilities in accordance with Sumo Logic's patch management processes.
    4. **Data Management.** Sumo Logic has adequate information security infrastructure controls in place for Customer Data obtained, transported, and retained by Sumo Logic for the provision of the Services.
7. **Business Continuity.** Sumo Logic will maintain a business continuity plan, which is designed to ensure Sumo Logic will be able to continue to provide the Services in accordance with the Agreement in the event of a disaster or other significant event that might otherwise impact Sumo Logic's operations.

Notwithstanding the foregoing, You understand and acknowledge that You will be solely responsible for implementing and maintaining access and security controls on its own systems.

Sumo Logic Data Processing Addendum

Updated: May 9, 2025

This Data Processing Addendum ("**DPA**") is entered into by and between Sumo Logic, Inc. ("**Sumo Logic**") and Customer. This DPA amends the terms and forms part of the Master Service Agreement or other agreement between Customer and Sumo Logic governing the access to and use of Services (collectively, the "**Master Agreement**").

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. DEFINITIONS AND BACKGROUND

1.1 Definitions. Capitalized terms used but not defined below or in Attachment 1 (Definitions) to this DPA shall have the meanings set forth in the Master Agreement.

1.2 Background. Customer and Sumo Logic (each, a "**Party**" and collectively, the "**Parties**") acknowledge that Customer may be using the Services to Process Personal Data on behalf of itself, in which case Sumo Logic shall be a processor and Customer shall be a controller under this DPA, or Customer may be using the Services to Process Personal Data as a processor on behalf of its customers, in which case Sumo Logic shall be a sub-processor to Customer (and such customers shall remain the controller).

1.3 Effectiveness. This DPA shall be effective as of the effective date of the Master Agreement. If the Customer makes any deletions or revisions to this DPA, then this DPA is null and void. This DPA shall terminate automatically upon termination of the Master Agreement or as earlier terminated pursuant to the terms of this DPA. Notwithstanding the foregoing, Sumo Logic shall continue to secure Personal Data in accordance with the terms in this DPA for so long as Sumo Logic has access to such Personal Data.

2. DATA PROCESSING AND PROTECTION

2.1 Limitations on Use. Sumo Logic shall Process Personal Data only: (a) in a manner consistent with documented instructions as specified under Section 2.2 (Instructions), including with regard to transfers of Personal Data to a third country; and (b) as required by Data Protection Law, provided that Sumo Logic shall inform Customer (unless prohibited by such Data Protection Law) of the applicable legal requirement before Processing pursuant to such Data Protection Law (as further detailed in Section 2.3 (Confidentiality)).

2.2 Instructions. Customer instructs Sumo Logic to Process Personal Data to provide the Services and as otherwise authorized or permitted under the Master Agreement, including as specified in Attachment 2 (Scope of Processing). This DPA and the Master Agreement (including the instructions via configuration tools such as the Sumo Logic portal made available by Sumo Logic for the Services) constitute Customer's documented instructions regarding Sumo Logic's Processing of Personal Data. Additional instructions provided by Customer (if any) require prior written agreement by Customer and Sumo Logic, including agreement on any additional fees to carry out such instructions. Customer shall not instruct Sumo Logic to perform any Processing of Personal Data that violates any Data Protection Law. Sumo Logic may suspend Processing based upon any Customer instructions that Sumo Logic reasonably suspects violate Data Protection Law. Sumo Logic shall promptly inform Customer if, in Sumo Logic's opinion, an instruction infringes Data Protection Law. Without limiting the instructions under this Section 2.2, Sumo Logic shall not retain, use, or disclose the Personal Data provided under the Master Agreement for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Services, and shall not sell the Personal Data. Please refer to *Attachment 4* for US state law additions.

2.3 Confidentiality. Sumo Logic shall ensure that persons authorized by Sumo Logic to Process any Personal Data are subject to appropriate confidentiality obligations.

2.4 Security. Sumo Logic shall implement and maintain appropriate technical and organizational measures designed to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, theft, alteration or disclosure in accordance with Attachment 3 (Data Security Exhibit). Sumo Logic may amend the technical and organizational measures, provided the new measures do not fall short of the level of security provided by the specified measures.

2.5 Disposal. At the choice of Customer, Sumo Logic shall (or shall enable Customer via the Services to) delete (and shall delete existing copies of) all Personal Data after the end of the provision of Services (unless Data Protection Law requires the storage of such Personal Data by Sumo Logic).

2.6 Customer Controls. Customer shall delete Personal Data not required for its use of the Services before ingestion via the Services. The Services provide Customer with a number of controls that Customer may exercise with respect to its Personal Data. Customer shall use these controls as technical and organisational measures to assist it in connection with obligations under Data Protection Law.

3. DATA PROCESSING ASSISTANCE

3.1 Data Subject Rights Assistance. Sumo Logic shall, to the extent permitted by Data Protection Law, notify Customer without undue delay if Sumo Logic receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, its right not to be subject to an automated individual decision making or other Data Subject rights under Data Protection Law, each such request being a "**Data Subject Request**". To the extent Customer, in its use of the Services, does not have the ability to address the Data Subject Request without further assistance, Sumo Logic shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent the response to such Data Subject Request is required under Data Protection Law.

3.2 Security Assistance. Taking into account the nature of Processing and the information available to Sumo Logic, Sumo Logic shall provide commercially reasonable efforts to assist Customer in ensuring compliance with the obligations pursuant to Article 32 of the GDPR by providing the information and assistance described in Section 4 (Audits).

3.3 Security Incident Notice and Assistance. Sumo Logic shall notify Customer without undue delay after confirming a Security Incident. Sumo Logic shall further take commercially reasonable steps to mitigate the effects and minimize any impact from the Security Incident. Taking into account the nature of Processing and the information available to Sumo Logic, Sumo Logic shall assist Customer in ensuring compliance with the applicable controller's notification obligations imposed under Data Protection Law in connection with any Security Incident, including assistance necessary to facilitate the applicable controller's compliance with Articles 33 and 34 of the GDPR. Customer acknowledges that an unsuccessful Security Incident shall not be subject to this Section 3.3 (Security Incident Notice and Assistance). An unsuccessful Security Incident is one that results in no unauthorized access to Personal Data and may include, without limitation, pings and other broadcast attacks on firewalls or edge networks, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents. Notifications of Security Incidents shall be delivered to one or more of Customer's administrators. It is the Customer's sole responsibility to maintain accurate contact information on the Sumo Logic portal and to use secure transmission at all times.

3.4 Data Processing Impact Assessment ("DPIA") Assistance. Taking into account the nature of Processing and the information available to Sumo Logic, Sumo Logic shall provide commercially reasonable efforts to assist Customer in ensuring compliance with its obligations relating to DPIAs under Data Protection Laws, including pursuant to Articles 35 and 36 of the GDPR.

4. AUDITS

4.1 General Assistance. Subject to Section 4.3 (Customer Audits), Sumo Logic shall make available to Customer information necessary to demonstrate compliance with its obligations in this DPA. Any such information or results of audits shall be deemed the confidential information of Sumo Logic under the Master Agreement.

4.2 Sumo Logic Reports. Sumo Logic procures independent audits by third parties to assess Sumo Logic's adherence to the following standards or requirements: (a) SOC 2 Type II (or reports or other documentation describing the controls implemented by Sumo Logic that replace or are substantially equivalent to SOC 2 Type II); (b) ISO 27001 (or certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001); and (c) PCI DSS Service Provider Level 1 (or certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to PCI DSS) (collectively, "**Reports**"). Subject to the confidentiality obligations set forth in the Master Agreement, Sumo Logic shall provide Customer with a copy of Sumo Logic's then-current summary of such audit reports or certifications as reasonably requested. If the Master Agreement does not include a provision protecting Sumo Logic's confidential information, then the Reports shall be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Reports.

4.3 Customer Audits. Customer shall only request additional information or an on-site audit of Sumo Logic to the extent information provided by Sumo Logic (including under Section 4.2 (Sumo Logic Reports)) is not reasonably sufficient to enable Customer to evaluate Sumo Logic's compliance with this DPA. Customer can exercise any right it may have to conduct an audit by instructing Sumo Logic to carry out the audit described in Section 4.2 (Sumo Logic Reports). If Customer wishes to modify this instruction regarding the audit, then Customer has the right to request a modification by sending Sumo Logic written notice. Customer shall provide written communication of any audit findings to Sumo Logic. The scope of the audit shall not require Sumo Logic to disclose to Customer (or its authorized representatives): (i) any data or information of any other Sumo Logic customer; (ii) any Sumo Logic internal accounting or financial information; (iii) any Sumo Logic trade secret; (iv) any information that, in Sumo Logic's reasonable opinion, could compromise the security of the systems or premises; or cause Sumo Logic to breach its obligations under Data Protection Law or security, confidentiality, or privacy obligations to another customer or other third party; or (v) any information that Customer seeks to access for any reason other than the good faith fulfillment of Customer obligations under the Data Protection Law and Sumo Logic's compliance with the terms of this DPA. Sumo Logic reserves the right to suspend or terminate an audit in the event of a breach of this Section 4.3 (Customer Audits).

5. SUBPROCESSORS

5.1 Appointment of Subprocessors. Customer authorizes Sumo Logic to use subcontractors to Process Personal Data in connection with the provision of Services (each, a "**Subprocessor**"). Customer specifically consents to Sumo Logic's appointment of the Sumo Logic applicable affiliates and third party Subprocessors listed at: https://www.sumologic.com/solutions/security/subprocessors (or its successor site).

5.2 Objection Right for New Subprocessors.

a. Sumo Logic may update the list of approved Subprocessors, at which point Customer may object to Sumo Logic's use of a new Subprocessor within 10 days of receiving such notice if Customer reasonably determines that such Subprocessor is unable to Process Personal Data in accordance with the terms of this DPA ("**Objection Notice**"), by sending an e-mail to privacy@sumologic.com clearly indicating its desire to object to any such change. To receive additional information about updates to the list of Subprocessors, Customer may subscribe via the update mechanism on the public Subprocessor page linked in Sec. 5.1.

b. If Customer objects to the change in Subprocessors, Sumo Logic and Customer shall cooperate in good faith to consider whether any accommodation may be available and whether any such accommodation may require payment of additional fees or expenses. If the parties do not agree on any proposed accommodation within 30 days of Sumo Logic's receipt of Customer's objection ("**Accommodation Deadline**"), then Customer may terminate the applicable Order Form(s) only with respect to those Services that Sumo Logic indicates cannot be provided without such change. Customer must exercise this right of termination within 14 days of the Accommodation Deadline or it shall waive such right of termination and shall be deemed to have rescinded its objection to such change. If Customer exercises its termination rights, then, as Customer's sole and exclusive remedy, Sumo Logic shall refund Customer on a prorated basis any unused prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination.

5.3 Liability. Sumo Logic shall impose data protection obligations upon any Subprocessor that are no less protective than those included in this DPA. Sumo Logic shall remain liable for any breach of such obligations by its Subprocessors.

6. DATA TRANSFERS

The transfer of EEA, UK, and Swiss residents' Personal Data outside of the respective jurisdiction to a country not deemed adequate by the applicable data protection authority ("**Data Transfer**") shall be subject to a data protection regime pursuant to Chapter V GDPR: For transfers from these three participating jurisdictions to the United States, the **Data Protection Framework ("DFP")** as certified by Sumo Logic shall apply (https://www.dataprivacyframework.gov/list). For transfers to other jurisdictions, or in the case of any challenge to the DPF, Logic utilizes Standard Contractual Clauses.

6.1 Standard Contractual Clauses. Where EEA or Swiss residents' Personal Data is transferred, Customer shall notify Sumo Logic and any such transfer shall be conducted pursuant to the Standard Contractual Clauses attached as Attachment 4 and such clauses shall be deemed executed by the Parties as of the effective date of this DPA. Where Customer is processing Customer Data as a controller, Module Two of those clauses shall apply. Where Customer is processing Customer Data as a processor, Module Three of those clauses shall apply. Any audits required under those clauses shall be conducted pursuant to Section 4.3 (Customer Audits) of this DPA.

6.2 Transfers Subject to Swiss Data Protection Law. If any Personal Data subject to the Federal Act on Data Protection of 19 June 1992 (the "**FADP**") is transferred out of Switzerland, the parties shall conduct such transfer pursuant to Section 6.1. The Standard Contractual Clauses for such transfers shall include the following provisions:

a. The competent supervisory authority in Annex I.C under Clause 13 shall be the Federal Data Protection and Information Commissioner;

b. References to a "Member State" and "EU Member State" shall not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) and references to GDPR shall be understood as references to the FADP; and

c. Until the revised FADP enters into force, the Standard Contractual Clauses shall also protect the data of legal entities in Switzerland.

6.3 Transfers Subject to the UK GDPR. Any Data Transfer of Personal Data subject to the UK GDPR shall be pursuant to the Standard Contractual Clauses subject to the UK Addendum (which shall be deemed executed by the Parties as of the effective date of this DPA), incorporated herein by reference. If a competent governmental authority requires additional documentation to effectuate such transfers from the UK, then the parties shall work together in good faith to execute such other documentation. For transfers subject to the UK Addendum the following conditions shall apply: (a) the information required for Table 1 is contained in Part A of Annex I of Attachment 5 of this DPA; (b) in relation to Table 2, the version of the Standard Contractual Clauses to which the UK Addendum applies is Module Two for Controller to Processor and, where Customer acts as processor, Module Three for Processor to Processor transfers; (c) in relation to Table 3, the list of parties and description of the transfer are as set out in Attachment 2 of this DPA, Sumo Logic's technical and organisational measures are set in Attachment 3 of this DPA, and the list of Sumo Logic's sub-processors are as referenced in section 5.1 of this DPA; (d) in relation to Table 4, neither party shall be entitled to terminate the UK Addendum in accordance with clause 19 of the Mandatory Clauses of the UK Addendum; and (e) any audits required under the Standard Contractual Clauses subject to the UK Addendum shall be conducted pursuant to Section 4.3 (Customer Audits) of this DPA.

6.4 Supplementary Measures. The following additional safeguards shall be added as a new supplementary annex of the Standard Contractual Clauses where they apply:

a. Data Exporter represents and warrants that, to the best of its knowledge, the Personal Data it transfers under the Standard Contractual Clauses does not include any data that would be subject to access requests under Section 702 of the U.S. Foreign Intelligence Surveillance;

b. Data Importer shall use reasonable measures to encrypt Personal Data transferred to it pursuant to the Standard Contractual Clauses during transmission via the Services; and

c. If Data Importer receives a request for any such Personal Data from any government or law enforcement authority, it shall make commercially reasonable efforts to assert available defenses against making the disclosure and shall minimize the scope of any legally required disclosure to only that which is reasonably necessary to meet the disclosure obligation.

7. AUTHORIZED AFFILIATES

By executing this DPA, Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Sumo Logic and each such Authorized Affiliate subject to the provisions of the Master Agreement and this Section 7 (Authorized Affiliates) and Section 8 (Limitation of Liability). Customer represents to Sumo Logic that it has and shall maintain such contracting authority. Each Authorized Affiliate shall be bound by the obligations under this DPA and, to the extent applicable, the Master Agreement. For clarity, an Authorized Affiliate is not and does not become a party to the Master Agreement, and is only a party to the DPA. All access to and use of the Services and Customer Data by Authorized Affiliates must comply with the terms and conditions of the Master Agreement, and any violation of the terms and conditions of the Master Agreement by an Authorized Affiliate shall be deemed a violation by Customer. Customer shall remain liable to Sumo Logic for the performance of its Authorized Affiliates

The Customer that is the contracting party to the Master Agreement shall remain responsible for coordinating all communications with Sumo Logic under this DPA, and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

Where an Authorized Affiliate becomes a party to the DPA with Sumo Logic, it shall to the extent required under Data Protection Laws be entitled to exercise its rights and seek remedies under this DPA, subject to the following:

a. Except where Data Protection Law requires the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Sumo Logic directly by itself, (i) solely the Customer that is the contracting party to the Master Agreement shall exercise any right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Master Agreement shall exercise any such rights under this DPA (not separately for each Authorized Affiliate individually but) in a combined matter for itself and all of its Authorized Affiliates together.

b. For example, the Customer that is the contracting party to the Master Agreement shall, when requesting an audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit impact on Sumo Logic and its Subprocessors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates into one single audit.

8. LIMITATION OF LIABILITY

Each party's and all of its Authorized Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Sumo Logic, whether in contract, tort, or under any other theory of liability, is subject to the "Limitation of Liability" section of the Master Agreement and other relevant provisions, and any reference to such section to the liability of a party means the aggregate liability of that party and all of its affiliates (including Authorized Affiliates) under the Master Agreement and all DPAs together. Nothing in this Section 8 is intended to restrict the rights of data subjects under Data Protection Law.

9. MISCELLANEOUS

Customer shall pay any fees and expenses authorized under this DPA in accordance with the payment terms of the Master Agreement. The terms of this DPA shall control to the extent there is any conflict between terms of this DPA and the terms of the Master Agreement. To the extent there is any conflict between the terms of this DPA and applicable Standard Contractual Clauses, the Standard Contractual Clauses shall control. Except as specifically amended and modified by this DPA, the terms and provisions of the Master Agreement remain unchanged and in full force and effect. Without limiting the foregoing, the governing law clause and forum selection clause of the Master Agreement shall apply to any disputes arising out of this DPA. Except as otherwise expressly provided herein, no supplement, modification or amendment of this DPA shall be binding, unless executed in writing by a duly authorized representative of each party to this DPA. This DPA may be executed in several counterparts (including delivery via facsimile or electronic mail), each of which shall be deemed to be an original but all of which together shall constitute one and the same instrument.

Attachment 1: Definitions

For purposes of this DPA, the following terms shall have the meaning ascribed below:

"Authorized Affiliate" means any direct or indirect, current or future subsidiary of a Customer that is controlled by Customer. The term "**control**" as used herein shall mean possession, directly or indirectly of at least fifty percent (50%) of the voting equity of another entity (or other comparable interest for an entity other than a corporation), or the power to direct or cause the direction of the management or policies of an entity whether through ownership of securities, by contract or otherwise.

"**Data Protection Law**" means data protection law applicable to Sumo Logic's Processing of Customer Data, including, as applicable, European Directives 2002/58/EC, GDPR, UK GDPR, U.S. state and federal privacy laws, including the California Consumer Privacy Act (as amended by the California Privacy Rights Act), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, and the Connecticut Data Privacy Act, in each case as amended, and any legislation or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates such legislation or regulation, as well as, internationally, applicable law.

"**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). For purposes of data relating to individuals in the UK, references to GDPR shall be interpreted to refer to the UK GDPR.

"**Standard Contractual Clauses**" means Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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 (Text with EEA relevance), as may be replaced or superseded by the European Commission.

"**Personal Data**" means any data that Sumo Logic Processes on behalf of Customer via the Services that is deemed "personal data," or "personal information" (or analogous variations of such terms) under GDPR or other Data Protection Law.

"**Security Incident**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, any unauthorized use or disclosure of, or access to, Personal Data.

"**Process**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated 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, extending further to such operation or operations under Data Protection Law.

"**Services**" means the services provided by Sumo Logic pursuant to the Master Agreement.

"**UK Addendum**" means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force as of 21 March 2022

"**UK GDPR**" means the incorporation of the GDPR into UK law by the Data Protection Act of 2018 and by the Data Protection Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (each as amended, superseded, or replaced).

Attachment 2 – Scope of Processing

Controller

Customer

Processor

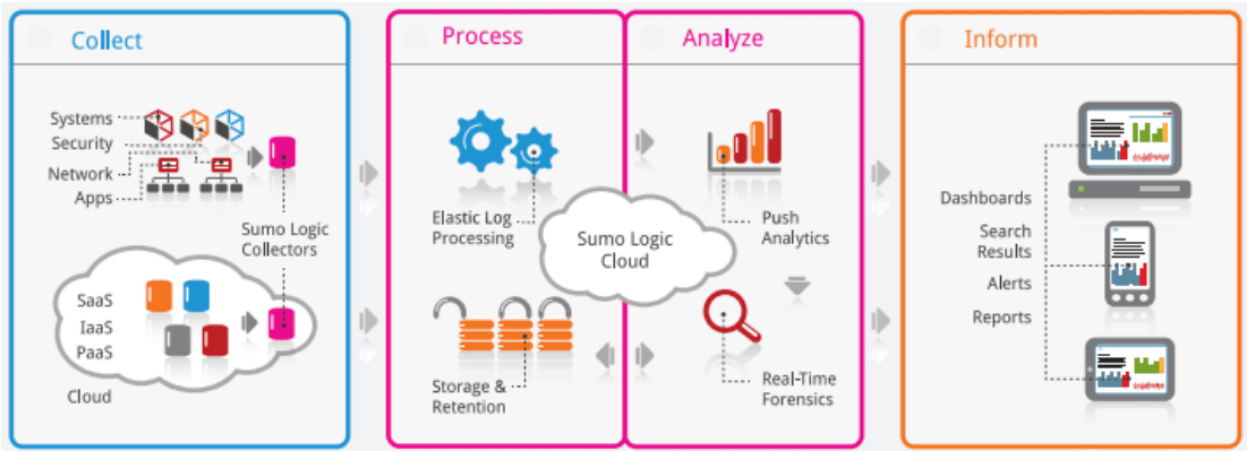
Sumo Logic

Subject-Matter and Duration of Processing

Sumo Logic Processes Personal Data if and when provided by Customer in the course of providing the Services in accordance with the Master Agreement and until the Master Agreement terminates or expires.

Nature and Purpose of Processing

Processing of Personal Data in connection with and for the purpose of Sumo Logic providing the Services to Customer pursuant to the Master Agreement. Specifically, the Personal Data shall, if and to the extent Customer provides it, be subject to the following baseline Processing activities



Types of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion. This may include, but is not limited to the following categories of data:

- Direct identifying information (e.g., name, email address, telephone)
- Indirect identifying information (e.g., gender, date of birth)
- Device identification data and traffic data (e.g., IP addresses, MAC addresses, web logs)
- Any other personal data supplied by users

Categories of Data Subjects

The data subjects shall include Customer's suppliers and end-users.

Special Categories of Data (as applicable)

The Services are not designed for special categories of Personal Data. Sumo Logic does not anticipate that Customer shall submit special categories to the Services. To the extent that such data is submitted to the Services, it is determined and controlled by Customer in its sole discretion.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c)

The technical and organizational security measures implemented by the data importer are as described in Attachment 3 of the DPA (Data Security Exhibit).

Attachment 3 – Data Security Exhibit

1. **Purpose.** This Data Security Exhibit sets forth the information security program and infrastructure policies that Sumo Logic shall meet and maintain in order to help protect Customer Data from unauthorized use, access or disclosure, during the term of the Master Agreement.

2. **Information Security Management Program.** Sumo Logic shall maintain throughout the Term of the Master Agreement an information security management program (the "**ISMP**") designed to protect and secure Customer Data from unauthorized access or use. The ISMP shall be documented and updated based on changes in applicable legal and regulatory requirements related to privacy and data security practices and industry standards. Sumo Logic incorporates commercially reasonable and appropriate methods and safeguards designed to protect the security, confidentiality, and availability of Customer Data. Sumo Logic shall, at a minimum, implement measures designed to adhere to applicable information security practices as identified in International Organization for Standardization 27001 (ISO/IEC 27001) (or a substantially equivalent or replacement standard) or other authoritative sources (e.g. SOC2).

3. **Independent Assessments.** On an annual basis, Sumo Logic has an independent third-party organization conduct an independent assessment consisting of a Report on Controls at a Service Organization Relevant to Security, Availability, Processing, Integrity, Confidentiality and/or Privacy (SOC2 Type II) or such other assessment at its sole discretion (e.g. ISO 27001 Certificate). Additionally, Sumo Logic undergoes regular penetration testing from independent third parties at least on an annual basis.

4. **Information Security Policies.** Sumo Logic shall implement information security and privacy policies that address the roles and responsibilities of Sumo Logic 's personnel who have access to Customer Data in connection with providing the Services. All Sumo Logic personnel with access to Customer Data shall receive annual training on Sumo Logic 's ISMP.

5. **Information Security Infrastructure.**

    a. **Access Controls**. Sumo Logic shall implement and maintain, throughout the Term and at all times while Sumo Logic has access to or possession of Customer Data, reasonable access controls (physical, technical, and administrative) that are designed to protect Customer Data.

    b. **Encryption**. Sumo Logic shall implement measures designed to encrypt Customer Data (i) at rest within the SaaS Services at a minimum AES algorithm with a default value of 256-bit strength; and (ii) in transit using TLS 1.2 encryption or stronger.

    c. **Network and Host Security**. Sumo Logic has implemented measures designed to address network intrusion detection and firewalls. Sumo Logic uses reasonable efforts designed to ensure that the SaaS Services' operating systems and applications that are associated with Customer Data are patched or secured to mitigate the impact of security vulnerabilities in accordance with Sumo Logic 's patch management processes.

    d. **Data Management.** Sumo Logic has reasonable information security infrastructure controls in place for Customer Data obtained, transported, and retained by Sumo Logic for the provision of the Services.

6. **Business Continuity.** Sumo Logic shall maintain a business continuity plan, which is designed to ensure Sumo Logic shall be able to continue to provide the SaaS Services in accordance with the Master Agreement in the event of a disaster or other significant event that may impact Sumo Logic's operations.

Notwithstanding the foregoing, Customer understands and acknowledges that Customer shall be solely responsible for implementing and maintaining access and security controls on its own systems.

Attachment 4: California Privacy Law Addendum

This California Privacy Law Addendum ("**California Addendum**") supplements, amends and forms part of the DPA.

1. Definitions

Capitalized terms used but not defined in this California Addendum shall have the meaning specified in the DPA. In addition, "**service provider**," "**sell**" and "**share**" shall have the meaning set forth under the California Consumer Privacy Act of 2018 [1798.100 – 1798.199], as amended, including by the California Privacy Rights Act of 2020, and all regulations adopted thereunder ("**CCPA**").

2. Sumo Logic Commitments

Sumo Logic shall not Process Personal Data subject to the CCPA ("**CCPA Data**") for any business purpose other than as necessary for the specific purpose of performing the Services, including not collecting, retaining, using, or disclosing the CCPA Data for a commercial purpose other than providing the Services to Customer. Without limiting the foregoing, Sumo Logic shall: (a) not sell or share the CCPA Data; (b) not retain, use, or disclose CCPA Data outside of the direct business relationship between Sumo Logic and Customer other than as permitted for service providers under the CCPA; (c) not combine the CCPA Data with any other personal information it collects or receives outside of its relationship with Customer other than as permitted for service providers under the CCPA; (d) in connection with its Processing of CCPA Data, comply with all applicable sections of the CCPA in its capacity as a service provider, including by providing the same level of privacy protection as required by the CCPA, for example, by providing assistance with respect to consumer requests as specified in Section 3.1 of the DPA and by implementing reasonable security procedures and practices as specified in Section 2.4 of the DPA; and (e) notify Customer if Sumo Logic makes a determination that it can no longer meet its obligations under the CCPA.

3. Customer Rights

Customer acknowledges that it has audit rights under Section 4 of the DPA pursuant to which Customer may take reasonable and appropriate steps to ensure that Sumo Logic uses the CCPA Data in a manner consistent with Customer's obligations under the CCPA. Sumo Logic grants Customer the additional right, upon notice to Sumo Logic, to stop and remediate Sumo Logic's unauthorized use of CCPA Data.

4. Customer Commitment.

Customer shall inform Sumo Logic of any consumer request made pursuant to the CCPA that Sumo Logic must comply with and provide the information necessary for Sumo Logic to comply with the request.

5. General

In the event of any conflict between the DPA and this California Addendum, the terms of this California Addendum shall control with respect to CCPA Data. Except as amended by this California Addendum, the DPA shall remain in full force and effective.

Attachment 5 – STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii. Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

   iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

   iv. Clause 12 – Modules Two and Three: Clause 12(a), (d) and (f);

   v. Clause 13;

   vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);

viii. Clause 18 – Modules Two and Three: Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties

shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it shall continue to ensure compliance with these Clauses and shall only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

a. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

b. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

c. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

d. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

a. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

d. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it shall continue to ensure compliance with these Clauses and shall only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

a. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

b. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

c. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

d. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

c. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

d. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

f. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

g. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

a. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

a. GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorized to do so by the controller.

b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject shall not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter

and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it shall continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). For Module Three: The data exporter shall forward the notification to the controller.

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, for Module Three, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by, for Module Three, the controller or in general the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

iii. For Module Three: The data exporter shall forward the notification to the controller.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). For Module Three: The data exporter shall forward the notification to the controller.

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial

authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. For Module Three: The data exporter shall make the assessment available to the controller.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   iv. In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. For Modules Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

   i. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it shall continue to ensure compliance with these Clauses and shall only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Italy.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of Italy.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s): [*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]*

1. Name: Customer identified in the Master Agreement

Address: Customer address identified in the Master Agreement

Contact person's name, position and contact details: Contact person identified in the Master Agreement

Activities relevant to the data transferred under these Clauses: Obtaining Cloud-Native Intelligence Services for Data Exporter's Operations, Business, or Security, as applicable.

Signature and date: Dated as of the effective date of the Master Agreement

Role (controller/processor): controller or processor, as applicable based on the Master Agreement or Order Form

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

1. Name: Sumo Logic, Inc.

Address: 855 Main Street, Suite #100, Redwood City, CA 94063

Contact person's name, position and contact details: Jennifer McCord, VP Finance & Chief Accounting Officer, jmccord@sumologic.com

Activities relevant to the data transferred under these Clauses: Delivering Cloud-Native Intelligence Services for Data Exporter's Operations, Business, or Security, as applicable

Signature and date: Dated as of the effective date of the Master Agreement

Role (processor/sub-processor): processor or sub-processor, as applicable based on the Master Agreement or Order Form

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Data exporter's end users, if applicable

Categories of personal data transferred

Information regarding data exporter's end users provided at the discretion of data exporter and without any insight or direction from data importer. Data exporter agrees that it shall not provide to data importer any personal data considered sensitive or a special category of data under applicable laws in an unencrypted format.

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.

If applicable based on the Master Agreement or Order Form: Information regarding data exporter's end users provided at the discretion of data exporter and without any insight or direction from data importer. Data exporter agrees that it shall not provide to data importer any personal data considered sensitive or a special category of data under applicable laws in an unencrypted format.

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

As indicated in the Master Agreement or Order Form.

Nature of the processing

Sumo Logic provides a cloud-based log, metrics and events management and analytics Software-as-a-Service (SaaS). A high-level depiction of the service is as follows: collect, process/analyze, inform. The service includes the following service components and features that may be chosen by Sumo Logic's Customer:

Elastic Processing – Sumo Logic's patented ELP engine scales each service component independently to meet each customer's compute, storage, and processing requirements on demand. ELP's absolute scalability supports a real-time indexing engine designed specifically for big data-scale volumes.

Managed Collection – Sumo Logic decouples the collection of log/metrics/events from data parsing and analysis, both of which are done inside the Sumo Logic service. Collectors and log sources are monitored by the service and collectors are automatically updated, eliminating the need for individual upgrades.

Managed Retention – Sumo Logic retains all log data in a highly secure, reliable repository to eliminate the need for data archiving, backups and restores, and redundancy strategies.

Real-Time Forensics – the Real-Time Forensics engine delivers search results from terabytes of log data uncovering actionable insights about new events occurring throughout the company's infrastructure.

Log Reduce – Sumo Logic's unique Log Reduce log reduction technology boils hundreds of thousands of log lines into a smaller number of digestible patterns that enable operations and security professionals to get to insights in seconds and find important system, application, and user behaviors that would otherwise remain buried under gigabytes of logs. Customers purchase hosted log storage in units of storage/day (e.g. terabyte-days). Log files are streamed from customer end-points to the hosted service via the transport layer security (TLS) encryption protocol. Customers then have the ability to view and analyze log data via the service portal

Security Orchestration Automated Response – Cloud SOAR connects disparate tools to fully automate incident response and leave time-consuming, manual tasks behind. Playbooks highlight appropriate courses of action, reducing the time needed to remediate incidents. Automate your incident response with our adaptive SOAR solution to boost the efficiency of the entire team. A heartbeat is sent periodically to a Sumo Logic service which has the installation ID, IP address and number of nodes in the system for licence enforcement.

OSS Observability – Agents as collectors of metrics and events data send them over a TLS encrypted connection to a backend which transforms the data for storage into any system selected by the customer. All data is transmitted using TLS encryption. The backend is owned and operated by the Customer on-premise. A heartbeat is sent periodically to a Tessen service which has the installation ID, IP address and number of nodes in the system for licence enforcement.

Security Information and Event Management – Cloud SIEM connects to various security relevant data sources to collect, normalize and detect security incidents in near real-time to reduce false positives and the amount of investigation required by a SOC Analyst. Data could be from a sensor deployed into a network, 3rd party security products via an API or any of a number of log sources. The detected incidents are presented as signals or Insights which are groupings of signals that together indicate a significant event that requires investigation. This aggregation of signals reduces the number of false positives and number of incidents that require manual investigation, thus boosting the efficiency of the SOC team.

Purpose(s) of the data transfer and further processing

To provide the Services under the Master Agreement.

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

For the duration of the Master Agreement and for any additional time as determined by data exporter or longer if required by applicable law.

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

Customer Data is transferred to sub-processors to provide the Services under the Master Agreement for the duration of the Master Agreement and for any additional time as determined by data exporter or longer if required by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

Garante per la protezione dei dati personali (Italian Data Protection Authority)

Piazza Venezia 11 – 00187 Roma (Italy)

+39 06.696771

protocollo@gpdp.it

protocollo@pec.gpdp.it

ANNEX II

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

For a description of the technical and organisational measures implemented by the data importer, see Attachment 3 – Data Security Exhibit of the Data Processing Addendum.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Amazon Web Services, Inc.

Salesforce, Inc.

Current list of Sumo Logic companies that are subprocessors is available at https://www.sumologic.com/security/subprocessors and Section 2.6.2.

2.6.2 Third-Party Subprocessors

Last Updated: 3/11/2026

Sumo Logic maintains a current list of subprocessors utilized in the processing of customer data for the provision of the Sumo Logic services, which may include personal data.

Third-Party Subprocessors

Third Party Service/Vendor	Purpose	Entity Country	Website
Amazon Web Services, Inc.	Data Hosting Generative AI features and functionalities optional through AWS Bedrock	United States, European Union, and other countries or jurisdictions as selected	https://aws.amazon.com/
Salesforce, Inc.	Customer Support Ticketing System	USA	https://www.salesforce.com/
Gainsight, Inc.	Customer Success Platform with genAI for communication utilizing their Staircase feature	USA	https://www.gainsight.com

Sumo Logic Group Subprocessors

Depending on the geographic location of Customer or its users, and the Services provided, Sumo Logic may engage one or more of its affiliates as Subprocessors to deliver some or all of the Services provided to Customer. Sumo Logic affiliates are as follows:

Sumo Logic Group Entity	**Entity Country**
Sumo Logic Australia Pty Ltd on behalf of itself and Sumo Logic Australia Pty Ltd, New Zealand Branch	Australia
Sumo Logic Canada Ltd.	Canada
Sumo Logic, Inc.	United States
Sumo Logic Japan KK	Japan
Sumologic Limited	United Kingdom
Sumo Logic Singapore Private Limited on behalf of itself and Sumo Logic Singapore Private Limited, Korean Branch	Singapore Korea
Sumologic Technologies Private Limited	India
Sumo Logic Costa Rica, SRL	Costa Rica