LOGICMONITOR DATA PROCESSING ADDENDUM
(Global - Containing EU Processor Standard Contractual Clauses)

This Data Processing Addendum (this “Addendum” or “DPA”) supplements the Service Agreement (the “Agreement”) entered into by and between the **Customer** named in the LogicMonitor Order Form (“Customer” or “Controller”) and **LogicMonitor, Inc.** (“LogicMonitor” or “Processor”) (each a “party” and collectively the “parties”), under which Customer obtains SaaS Services (“Services,” the “Service” or “SaaS Services”) from LogicMonitor. ***This Addendum applies solely to the extent that Customer is deemed a Data Controller and LogicMonitor is deemed a Data Processor as defined below and under applicable laws and regulations.***

Introduction and Background

a. The parties understand that the purpose and focus of the SaaS Service is IT systems status and performance monitoring and not to function as a receptacle, conduit or service to store, manipulate, transmit, retrieve or process Personal Data.

b. Nonetheless, the parties acknowledge that the incidental capturing of nominal Personal Data (as defined herein) in connection with the Service will occur in the ordinary course (for example, credentials (login) information for authorized users and information in log files with transactional monitoring, and names and contact information of employees of each party as needed to conduct the SaaS Services and business relationship).

c. The purpose of this Addendum is to provide that the parties shall manage their operations and activities with respect to Personal Data in a confidential and secure manner and in accordance with all applicable laws and regulations.

Therefore, Customer and LogicMonitor agree as follows:

1. Definitions

a) *“**Affiliate(s)**”* has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any entity that directly or indirectly controls, is controlled by, or is under common control or ownership with a party, where “control,” “controlled by” and “under common control with” means the possession of the power to direct, cause or significantly influence the direction of the entity, whether through the ownership of voting securities, by contract, or otherwise;

b) “**California Data Protection Laws**” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq., and all regulations issued pursuant to it.

c) "***Contracted Processor***" means LogicMonitor or LogicMonitor Affiliate and/or a Subprocessor, as the context requires;

d) “***Controller to Processor SCCs***" means the Module 2 of the EU Standard Contractual Clauses set out in the 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, as set out in Appendix 4 to this Addendum; as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws;

e) "***Data Protection Laws***" and *“**Applicable Law**”* means the California Data Protection Laws, EU Data Protection Legislation, Swiss Data Protection Law, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

f) “***Data Subject***” (whether or not capitalized) means an identified or identifiable natural person as defined in the GDPR;

g) "***Data Controller***" or ***“Controller”*** means the entity which determines the purposes and means of Processing Personal Data (in this case, Customer) as defined in the GDPR, and shall include a “business” as that term is defined in the California Data Protection Laws;

h) "***Data Processor***" or ***“Processor” means*** the entity which Processes Personal Data on behalf of the Data Controller (in this case, LogicMonitor) as defined in the GDPR, and shall include a “service provider” as that term is defined in the California Data Protection Laws**;**

i) *"**EEA**"* means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein;

j) *"**EU Data Protection Legislation**"* means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, including any applicable national implementations thereof, (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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***" or "***GDPR***"), including any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR, and (iii) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time;

k) "***EU Restricted Transfer***" means a transfer of Personal Data by Customer or any Customer Affiliate to LogicMonitor or any LogicMonitor Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by EU Data Protection Legislation in the absence of the protection for the transferred Personal Data provided by the EU Standard Contractual Clauses;

l) "***EU Standard Contractual Clauses***" means the standard contractual clauses set out in the 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, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws;

m) "***Member State***" means a member state of the EU;

n) *“**Personal Data**”* means any data, information or record that directly or indirectly identifies a natural person (data subject) or relates to an identifiable natural person, including but not limited to, name, address, telephone number, email address, payment card data, identification number such as social security or tax ID number, date of birth, driver’s license number, medical and health-related information, and any other personally identifiable information that LogicMonitor or any third party acting on LogicMonitor’s behalf Processes in connection with this Agreement, and includes “personal data” as is defined in the GDPR and “personal information” as is defined in the California Data Protection Laws;

o) *“**Process**,” “**Processes**,” “**Processing**”* or *“**Processed**”* means, as is defined in the GDPR, any operation or set of operations which is performed on any data, information, material, work, expression or other content, whether or not by automated means, such as collection, recording, downloading, uploading, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

p) ***“Security Incident”*** means, as is defined in the GDPR, any suspected or actual loss, unauthorized or unlawful processing, destruction, damage, or alteration, or unauthorized disclosure of, or access to the Personal Data;

q) "***Supervisory Authority***" means (a) an independent public authority which is established by an EU member state pursuant to EU Data Protection Legislation, and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

r) “**Swiss Data Protection Law**” means the Swiss Federal Act on Data Protection.

s) “**Swiss Restricted Transfer**” means a transfer of Personal Data by Customer or any Customer Affiliate to LogicMonitor (or any onward transfer), in each case, where such transfer would be prohibited by Swiss Data Protection Law in the absence of the protection for the transferred Personal Data provided by the EU Standard Contractual Clauses, subject to Switzerland-specific modifications as set out in clause 11.2;

t) "***UK Data Protection Laws"*** means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and other data protection or privacy legislation in force from time to time in the United Kingdom;

u) "***UK Restricted Transfer***” means a transfer of Personal Data by Customer or any Customer Affiliate to LogicMonitor (or any onward transfer), in each case, where such transfer would be prohibited by UK Data Protection Laws in the absence of the protection for the transferred Personal Data provided by the UK IDTA; and

v) "***UK IDTA***" means, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, effective March 21, 2022; as set out in Appendix 5 to this Addendum or as otherwise amended or replaced from time to time, pursuant to Article 46 of the UK GDPR.

2. Applicability. This Addendum shall apply only to the extent Customer is established within the EEA or Switzerland and/or to the extent LogicMonitor Processes Personal Data of data subjects located in the EEA or Switzerland on behalf of Customer or a Customer Affiliate.

3. Processing of Personal Data

3.1 Purpose Limitation. LogicMonitor will only Process the types of Personal Data, and only in respect of the categories of Data Subjects, and only for the nature and purposes of processing and duration, as is set out in Appendix 1, and on behalf of and in accordance with Customer’s written instructions.

3.2 Business Purpose. LogicMonitor shall only Process Personal Data for “business purposes,” as such term is defined under the California Data Protection Laws, including: (i) providing the Services to Customer; (ii) helping to ensure the security and integrity of Personal Data; (iii) debugging to identify and repair errors that impair existing intended functionality; and (iv) undertaking activities to verify or maintain the quality or safety of the Services.

3.3 Prohibited Actions. LogicMonitor is prohibited from “selling” or “sharing” Personal Data, as such terms are defined under the California Data Protection Laws.

4. Roles and Responsibilities

4.1 Responsibilities and Appointment. Customer (as Controller) appoints LogicMonitor as a Processor to process the Personal Data on Customer's behalf. However, where Customer may be a Processor, it appoints LogicMonitor as Customer's Sub-processor.

4.2 Compliance.

a) LogicMonitor, as Processor, will comply with all applicable Data Protection Laws.

b) To the extent that Customer is deemed a Controller under Applicable Law, Customer, as Controller, shall: (i) comply with all applicable Data Protection Laws; (ii) ensure that any instructions that it issues to LogicMonitor shall comply with Data Protection Laws; (iii) have sole responsibility for the accuracy, quality and legality of the Personal Data provided to LogicMonitor; (iv) have established the legal basis for processing under Data Protection Laws; (v) have provided all notices and obtained all consents as may be required under Data Protection Laws and (vi) ensure that it has and will continue to have, the right to provide access to the Personal Data to LogicMonitor in accordance with the terms of the Agreement and this Addendum.

c) If LogicMonitor believes that any instruction from Customer is in violation of, or would result in Processing in violation of Applicable Law, then LogicMonitor will promptly notify Customer, and if Customer believes LogicMonitor is or may be in violation of Applicable Law it will promptly notify LogicMonitor. Similarly, if Applicable Law requires LogicMonitor (or, for avoidance of doubt, any Sub-processor) to conduct Processing that is or LogicMonitor believes could reasonably be construed as inconsistent with Customer's instructions, LogicMonitor will notify Customer promptly prior to commencing the Processing, unless this notification is prohibited by law on important grounds of public interest.

d) If LogicMonitor determines it can no longer meet its obligations under Applicable Law, it must promptly notify Customer and suspend all Processing of Personal Data until appropriate remedial actions are taken.

e) Each party shall maintain records of all processing operations under its responsibility that contain at least the minimum information required by Data Protection Laws, and shall make such information available to any Supervisory Authority on request.

5. Confidentiality and Security.

5.1 Security Program. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, LogicMonitor will maintain or cause to be maintained a reasonable and commercially feasible information security program that complies with all Applicable Laws and is designed to reasonably ensure the security and confidentiality of all Personal Data.

5.2 Security Measures. LogicMonitor will take all appropriate and commercially reasonable measures, including, without limitation, administrative, physical, technical (including electronic), and procedural safeguards to protect Personal Data against the risks of a Security Incident. LogicMonitor will take commercially reasonable measures to ensure that Personal Data are only available to LogicMonitor personnel and its agents and Affiliates who have a legitimate business need to access Personal Data, who are bound by legally enforceable confidentiality obligations, who have received training on applicable data protection policies and procedures, and who will only process the Personal Data in line with Customer's instructions.

5.3 Confidentiality of Processing. LogicMonitor shall ensure that any person that it authorizes to Process Personal Data (including its staff, agents, subcontractors and Sub-processors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

5.4 Security Incident Response and Notification.

a) With respect to any Security Incident regarding Personal Data of which LogicMonitor becomes aware, in addition to its obligations set forth in other sections of this Agreement, LogicMonitor will promptly and without undue delay, notify Customer and provide such timely information as Customer may reasonably require to enable Customer to fulfill any data breach reporting obligations under Data Protection Laws. The notice will summarize in reasonable detail the nature of the Security Incident; whether the suspected data is lost, stolen or compromised, if known; LogicMonitor's appraisal of the consequences of the Security Incident; the corrective action taken or to be taken by LogicMonitor; and any internal point(s) of contact responsible for managing or responding to the Incident, including the contact information LogicMonitor's data protection director or officer. LogicMonitor will promptly take all reasonably necessary and advisable corrective actions and will cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate, or rectify such Security Incident.

b) In the event of a Security Incident, if either party determines that any Security Incident must be disclosed or reported to a third party, including individuals or governmental authorities (including any Supervisory Authority), each party will fully cooperate with and assist the other party in fulfilling such reporting and disclosure obligations. Unless required by Applicable Law, LogicMonitor shall not make any notifications to a Supervisory Authority or any data subjects about the Security Incident without the

Customer’s prior written consent (not to be unreasonably withheld or delayed).

6. Sub-processors

6.1 Appointment of Sub-Processors. Customer agrees that LogicMonitor may engage LogicMonitor Affiliates and third party sub-processors (collectively, "***Sub-processors***") to Process the Personal Data on LogicMonitor's behalf. Whenever LogicMonitor engages the services of sub-processors, LogicMonitor agrees that such sub-processors are capable of maintaining appropriate safeguards for Customer's Personal Data and that LogicMonitor has contractually obligated such Sub-processors to maintain appropriate safeguards designed to comply with Applicable Law and to protect the Personal Data to the same standard provided for by this Addendum. A list of current Sub-processors is maintained in LogicMonitor’s Data Handling Supplement, available at available at https://www.logicmonitor.com/data-handling-supplement (which location may be updated by LogicMonitor from time-to-time and Customer will be notified of such new location) (the “Listing”). If LogicMonitor engages a new Sub-processor ("New Sub-processor"), LogicMonitor shall update the Listing and send a notification by email to Customer at its primary business e-mail contact. Customer may object to the engagement of such New Sub-processor by notifying LogicMonitor within 10 days of LogicMonitor’s notification, provided that such objection must be on reasonable, substantial grounds, directly related to such New Sub-processor's ability to comply with substantially similar obligations to those set out in this Addendum (an “Objection”). LogicMonitor shall have the right to cure any Objection, provided, that if it determines the same is not curable, it will notify Customer and if the parties are not able to reach a reasonable resolution, either party may terminate the Agreement upon thirty (30) days’ notice. If the Customer does not so object, the engagement of the New Sub-processor shall be deemed accepted by the Customer.

6.2 Liability. LogicMonitor will be liable for the acts and omissions of its Sub-processors to the same extent that LogicMonitor would be liable if performing the services of each Sub-processor directly. Upon request, LogicMonitor will make available to Customer a current list of Sub-processors that Process Personal Data in connection with this Agreement.

7. Access Requests

7.1 Notice of Access Requests. LogicMonitor will promptly notify Customer of any request for access to any Personal Data from any regulatory body, government official or other third person.

7.2 Responding to Access Requests. LogicMonitor will cooperate with Customer if Customer, its regulators or a data subject requests access to Personal Data for any reason, provided that the Customer shall be responsible for LogicMonitor’s reasonable costs and expenses arising from such cooperation.

8. Retention and Destruction of Personal Data

8.1 Subject to clause 8.2, LogicMonitor will not retain Personal Data any longer than is reasonably necessary to accomplish the intended purposes for which the data was Processed pursuant to this Agreement, and except as required under Applicable Law or in order to defend any actual or possible legal claims as the Customer so directs, LogicMonitor shall take reasonable steps to return or irretrievably delete all Personal Data in its control or possession when it no longer requires such Personal Data to exercise or perform its rights or obligations under this Agreement, and in any event on expiry or termination of this Agreement.

8.2 To the extent that LogicMonitor is required by Applicable Law to retain all or part of the Personal Data (the "**Retained Data**"), LogicMonitor shall:

a) cease all processing of the Retained Data other than as required by the Applicable Law;
b) keep confidential all such Retained Data in accordance with Section 5 (Confidentiality and Security); and
c) continue to comply with the provisions of this Agreement in respect of such Retained Data.

9. Security Reports and Audit

9.1 Audits. To the extent that LogicMonitor is engaged in Processing Personal Data for Customer under the Agreement, Customer will have the right to verify compliance by LogicMonitor and any Sub-processor with the terms of this Agreement or to appoint a third party under reasonable covenants of confidentiality acceptable to the parties to verify the same on Customer's behalf. LogicMonitor will grant Customer or its agents access at mutually acceptable times, and no more than once annually, to the extent necessary to accomplish the inspection and review of the procedures relevant to the protection and Processing of Personal Data. LogicMonitor and Customer will consult and agree on the reasonable start date, scope and duration and security and applicable confidentiality controls for the audit. LogicMonitor agrees to provide reasonable assistance to Customer in facilitating this inspection function. Customer shall provide LogicMonitor with any audit reports generated in connection with any audit at no charge unless prohibited by applicable law, the audit reports shall be confidential and Customer may use the audit reports only for the purposes of meeting its audit requirements under applicable law and confirming compliance with the requirements of this Addendum. Nothing in this Section shall require LogicMonitor to breach any duties of confidentiality owed to any of its clients, employees or third party providers, and all audits shall be at Customer’s sole cost and expense.

9.2 Security Reports. Any provision of security attestation or audit reports (such as SOC 2, Type II or equivalent) shall take place in accordance with Customer's rights under the Agreement. If the Agreement does not include a provision regarding security attestation reports or audit rights, LogicMonitor shall provide a copy of its most current security report upon Customer's written request and subject to the confidentiality provisions of the Agreement.

10. Rights of Data Subjects

LogicMonitor will assist Customer as requested with responding to data subjects’ requests to exercise their rights under Applicable Law and regulations, which may include, without limitation, rights of access, correction, amendment, blocking and deletion. LogicMonitor will notify Customer promptly if it receives any such request or claim from a data subject relating to Personal Data or LogicMonitor’s Processing thereof. For the avoidance of doubt, Customer is responsible for responding to data subject requests for access, correction, restriction, objection, erasure or data portability involving that data subject's Personal Data.

11. Restricted Transfers

11.1 In respect of any EU Restricted Transfer, Customer and each Customer Affiliate (each as "data exporter") and LogicMonitor and each LogicMonitor Affiliate (each as "data importer") with effect from the commencement of the relevant transfer hereby enter into the Controller to Processor SCCs. Annex 1 to the Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of Appendix 1 to this Addendum and the processing operations are deemed to be those described in the Agreement. Annex 2 to the Controller to Processor SCCs shall be deemed to be pre-populated with the relevant sections of Appendix 2 (Technical and Organisational Measures) to this Agreement.

11.2 In respect of any Swiss Restricted Transfer, Customer and each Customer Affiliate (each as "data exporter") and LogicMonitor and each LogicMonitor Affiliate (each as "data importer") with effect from the commencement of the relevant transfer hereby enter into the Controller to Processor SCCs to be completed as set out in clause 11.1, subject to the following modifications:

a) For purposes of Annex I.C and Clause 13 of the Controller to Processor SCCs, insofar as the data transfer is governed by the Swiss Data Protection Law, the Supervisory Authority shall be Switzerland’s Federal Data Protection and Information Commissioner (FDPIC);
b) The term “member state” must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in Switzerland in accordance with Clause 18(c) of the Controller to Processor SCCs.
c) The Controller to Processor SCCs shall protect the data of Switzerland legal entities until the entry into force of the 25 September 2020 revised version of the Swiss Federal Act on Data Protection.
d) Any reference in the Controller to Processor SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” shall be interpreted as references to the Swiss Data Protection Law.

11.3 In respect of any UK Restricted Transfer, Customer acting on its own behalf and as agent for each Customer Affiliate (each as "data exporter") and LogicMonitor acting on its own behalf and as agent for each Contracted Processor (each as "data importer") with effect from the commencement of the relevant transfer hereby enter into the UK IDTA. If at any time the UK Government approves the Controller to Processor SCCs for use under the UK Data Protection Laws, the provisions of clause 11.1 shall apply in place of this clause 11.3 in respect of UK Restricted Transfers, subject to any modifications to the Controller to Processor SCCs required by the UK Data Protection Laws (and subject to the governing law of the Controller to Processor SCCs being English law and the supervisory authority being the Information Commissioner's Office).

11.4 The Controller to Processor SCCs made under clauses 11.1 and 11.2, and the UK IDTA made under clause 11.3, of this Agreement, as applicable, come into effect on the later of:

a) the data exporter becoming a Party to this Agreement;
b) the data importer becoming a Party to this Agreement; and
c) the commencement of the EU Restricted Transfer or UK Restricted transfer (as applicable) to which the Controller to Processor SCCs or the UK IDTA relate.

11.5 If, at any time, a Supervisory Authority or a court with competent jurisdiction over a Party mandates that transfers from Controllers in the EEA or the UK to Processors established outside the EEA or the UK must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted with the benefit of such additional safeguards.

12. Miscellaneous

12.1 Standard of Protection. Subject to Section 2 (Applicability) above, this Addendum supersedes any other provision of the Agreement to the extent such provision relates to the privacy, confidentiality or security of Personal Data; provided, however, in the event of any conflict between the provisions of this Addendum and the other portions of the Agreement, the parties will comply with the obligations that provide the most protection for Personal Data.

12.2 General. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control. Any claims brought under this Addendum shall be subject to the terms and conditions, including but not limited to the exclusions and limitations set forth in the Agreement.

12.3 Limitation of Liability. The total liability of each Customer and LogicMonitor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement, except to the extent that such limitation is invalid under Applicable Law.

12.4 Governing Law. This Addendum will be governed by and construed in accordance with the law stated in the Agreement, except to the extent that applicable data protection laws require otherwise, in which event this Addendum will be governed in accordance with applicable data protection laws and, if applicable, be subject to the jurisdiction of the relevant data exporter that exported the Personal Data from the EEA.

[Signatures and Schedules Follow]

WHEREAS, the authorized representatives of the parties have accepted and agreed to this Addendum as of the date below:

Customer: ______________________
Legal Name of Customer

By:________________________________
Name:_____________________________
Title:______________________________
Email:_____________________________
Date: ____________________________

LogicMonitor, Inc.

By:________________________________
Name:_____________________________
Title:______________________________
Email:_____________________________
Date: ____________________________

APPENDIX 1 – DESCRIPTION OF THE PROCESSING

A. LIST OF PARTIES

Subject matter of processing	
Nature and purpose of processing	LogicMonitor may process Personal Data within normal operation of the service, typically for automated procedures such as notification delivery (email/SMS), audit logging and user support.
Frequency of the Processing	For the duration of the Agreement
Categories of Personal Data	Access (login) credentials, email addresses, mobile device numbers, workstation IP addresses.
Categories of Data Subjects	Employees, temporary workers and contractors assigned by Customer to use the SaaS Services.
Duration	For the duration of the Agreement.
Data Exporter(s)	Name: Address: Contact person's name, position and contact details: Activities relevant to the data transferred under these Clauses: Signature and date: Role (controller/processor): Controller
Data Importer	Name: LogicMonitor, Inc. Address: 820 State Street, 5th Floor, Santa Barbara, CA 93101 Contact person's name, position and contact details: Thomas Higham, DPO legal@logicmonitor.com Activities relevant to the data transferred under these Clauses: LogicMonitor primarily processes IT systems health, status and performance data

	from Customer’s information technology systems. Incidental Personal Data elements processed may include name, email address, mobile device number, and workstation IP address, upon the instruction of the Customer. Signature and date: Role (controller/processor): Processor
Competent Supervisory Authority	Applicable Supervisory Authority of the EU Member State in which Customer Primarily Resides

APPENDIX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (*or document/legislation attached*):

Entry control

Unauthorized persons are prevented from entering data processing facilities where personal data is processed and used.

Measures:
LogicMonitor's service platform is operated as a hybrid deployment across co-located datacenters and AWS resources. Both LogicMonitor's datacenter subservice provider and AWS maintain stringent controls around the physical and environmental security of each site. In our datacenter facilities a five-step process is required to gain physical access to LogicMonitor servers, including a 24x7x365 manned security check, electronic keycards, and successive biometric scanning at each point of access. High-resolution video surveillance is maintained throughout the facilities.

Data processing systems access control

Unauthorized persons are prevented from using data processing systems (“DP Systems”).

Measures:
Access to the networks that contain customer data require authentication via a centrally-managed Single Sign-On (SSO) service. LogicMonitor’s SSO system enforces the use of strong password policies, including password expiration, restrictions on password reuse, and minimum password strength. Two-factor authentication is enforced to further protect against unauthorized access. Following successful authentication and authorization based on role, tertiary authentication against a privileged access management system is required to access any systems containing customer data.

Data access control

Measures are to be taken to ensure that only persons authorized to use a DP System may only access the data for which they have been granted access, and, while processing and using personal data and after it has been saved, it is not possible for such data to be read, copied, edited or deleted.

Measures:
The LogicMonitor service has been designed with sophisticated role-based authorization features that allow our customers to limit access to any type of collected data based on the principle of least privilege. LogicMonitor provides a number of default roles out-of-the-box, but the customer is solely responsible for the access rights assigned to each role and the assignment of roles to individuals.

Data transfer control

Measures are to be taken to ensure that personal data cannot be read, copied, edited or deleted by unauthorized persons while such data is being electronically transferred or while it is being transported or recorded on data media, and that it is possible to check and establish where personal data is to be transferred by data transfer equipment.

Measures:
A number of data elements collected by LogicMonitor – including personal data – are classified as customer sensitive and handled with utmost care. Specific controls include encryption at rest using AES-256 and encryption in transit using TLS 1.1 or higher with no weak ciphers.

Input control

Measures are to be taken to ensure the possibility of verifiable checks and the determination whether personal data has been entered, edited or deleted in the DP Systems, and if so by whom.

Measures:

The only interface LogicMonitor provides for the collection of personal data is in the management of user authentication to the service. Any user management actions including creation, modification, and deletion are logged in the account audit log available to all account holders with sufficient access rights.

Order control

Measures are to be taken to ensure that personal data is processed by data importer only in accordance with instructions of the data exporter.

Measures:

LogicMonitor's use of personal data is limited to name, email address, and optionally mobile device number. These elements are used within our service only for account management and alert delivery purposes, and these use-cases are enforced by our application code.

Availability control

Measures are to be taken to ensure that personal data is protected against accidental destruction or loss.

Measures:

In addition to user interface controls protecting data from accidental deletion LogicMonitor maintains continual backups of customer data that form the basis of a rigorous disaster recovery program. Customer backups may be used to restore an environment to correct human error or as part of our disaster recovery processes deployed in case of a facility failure.

Separation control

Measures are to be taken to ensure that data collected for different purposes can be processed separately.

Measures:

LogicMonitor's use of Personal Data is constrained by our application such that it can be used only for account management and alert delivery purposes. All other data collected by LogicMonitor is targeted at monitoring the health and performance of IT systems. The controls that enforce this separation exist within the LogicMonitor codebase.

APPENDIX 3 - SUBPROCESSORS

A list of LogicMonitor's subprocessors is maintained at https://www.logicmonitor.com/data-handling-supplement

APPENDIX 4 – CONTROLLER TO PROCESSOR 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)[1] 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.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub- processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned.

(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 8.1(b),Clause 8.5 (e) 8.9(a), (b), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) 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 - Optional

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.

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 will continue to ensure compliance with these Clauses and will 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, unauthorised 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 authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. 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.

(c) 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[2] (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:

(i) 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;

(ii) 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;

(iii) 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

(iv) 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.

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.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of 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 noncompliance. 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.

Clause 9

Use of sub-processors

(a) 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 thirty (30) 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.[3] 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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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

(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 authorised 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.

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 authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(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 will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(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

(a) 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

(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[4];

(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.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 will 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).

(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. 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 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

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.

(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.).

(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.

(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.

<u>SECTION IV – FINAL PROVISIONS</u>

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.

In these cases, it shall inform the competent supervisory authority 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) 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. 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 will continue to ensure compliance with these Clauses and will 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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established (“Member State”). Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18

Choice of forum and jurisdiction

(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 the Member State.

(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.

ANNEX I – DESCRIPTION OF THE PROCESSING

NTD: This Annex I shall be deemed to be prepopulated with the information in Appendix I- Description of Processing.

A. LIST OF PARTIES

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: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses:

... Signature and date: ...

Role (controller/processor): Controller

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

1. Name:

... Address:

...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses:

... Signature and date: ...

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

....

Categories of personal data transferred

....

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.

....

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

....

Nature of the processing

....

Purpose(s) of the data transfer and further processing

....

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

C. COMPETENT SUPERVISORY AUTHORITY

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

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

See Appendix 2 above.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors set forth in Appendix 3 above.

APPENDIX 5 - UK INTERNATIONAL DATA TRANSFER ADDENDUM

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Effective Date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Appendix 1	Full legal name: LogicMonitor, Inc. Trading name (if different): n/a Main address (if a company registered address): 820 State St., 5th Floor, Santa Barbara, CA 93101 Official registration number (if any) (company number or similar identifier):
Key Contact	See Appendix 1	Full Name (optional): Thomas Higham Job Title: DPO Contact details including email: legal@logicmonitor.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date:

	Reference (if any):
	Other identifier (if any):
	Or
	☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	Included	Excluded	General Authorisation	30 days	No
3						
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: See Appendix 1 above

Annex 1B: Description of Transfer: See Appendix 1 above

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Appendix 2 above

Annex III: List of Sub processors (Modules 2 and 3 only): See Appendix 3 above

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

    l. In Clause 16(e), subsection (i) is replaced with:

        "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

    m. Clause 17 is replaced with:

        "These Clauses are governed by the laws of England and Wales.";

    n. Clause 18 is replaced with:

        "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.