



INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH ALERT LOGIC

1. This DPA consists of distinct parts: this body and its set of definitions and provisions, Annex 1 (the Standard Contractual Clauses), and Appendices 1-3.
2. This DPA has been pre-signed on behalf of Alert Logic, Inc., as the data importer or processor.
3. To complete this DPA, Customer must: (a) Complete the information in the signature box and sign on Page 9, (b) Complete the information as the data exporter on Page 10, (c) Complete the information in the signature box and sign on Annex 1 and Appendices 1-3.
4. Customer must send the completed and signed DPA to Alert Logic by email to DPA@alertlogic.com. Upon receipt of the validly-completed DPA by Alert Logic at this email address, this DPA shall come into effect and legally bind the parties.

ALERT LOGIC, INC. DATA PROTECTION AGREEMENT

This Data Protection Agreement (hereinafter referred to as the "DPA") forms part of the Master Terms and Conditions (or Master Services Agreement, as applicable) (either, the "Agreement") between Alert Logic, Inc., a Delaware corporation with the address of 1776 Yorktown, Suite 150, Houston, Texas, 77056 ("Alert Logic") and Customer for the purchase of Services (as defined in the Agreement) from Alert Logic. This DPA reflects the parties' agreement with regard to the processing of personal data. Customer enters into this DPA on behalf of itself and in the name and on behalf of its Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. PURPOSE

This DPA establishes the terms and conditions that govern the transfer of personal data between controller and processor.

2. DPA DEFINITIONS

"controller", "processor", "process/processing", "data subject", "personal data", "personal information", "personal data breach", "subprocessor", and "supervisory authority" shall all have the same meanings as given them in GDPR, or, if applicable, other Applicable Law.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Alert Logic" means the Alert Logic entity which is a party to this DPA, or if not otherwise specified, Alert Logic, Inc., a company incorporated in Delaware and its primary address as 1776 Yorktown, Suite 150, Houston, Texas, 77056, USA, or an Affiliate of Alert Logic, Inc., as applicable.

"Alert Logic Group" means Alert Logic, Inc. and its Affiliates engaged in the processing of personal data.

"Applicable Law" means all applicable laws (including those arising under common law), statutes, cases, ordinances, constitutions, regulations, treaties, rules, codes, and other pronouncements having the effect of law of the European Union, United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority and specifically including those laws relating to the privacy, confidentiality, retention and security of personal data, including but not limited to the GDPR. References to "Applicable Law" mean Applicable Law as may be amended or supplemented.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data

protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Service pursuant to the Agreement between Customer and Alert Logic, but has not signed its own Order Form with Alert Logic and is not a "Customer" as defined under the Agreement.

“Clauses” means the Standard Contractual Clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council adopted by the Commission Decision of 5 February 2010 on standard contractual clauses – C(2010) 593, or the equivalent as revised or under other Applicable Law.

“Customer Data” means all electronic data submitted by or on behalf of Customer, or an Authorized Affiliate, to the Service.

“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), as amended.

“Order Form” means a written ordering document executed between Alert Logic and Customer for the provision of Services, and which shall, at a minimum, include a description and term of the Services and fees to be paid by Customer to Alert Logic for those Services.

“Trust & Compliance Documentation” means the Documentation applicable to the specific Services purchased by Customer, as may be updated periodically, as made reasonably available by Alert Logic.

“Standard Contractual Clauses” means the Clauses.

“User” means a Customer employee who is authorized by Customer to access the Service and for whose actions and omissions Customer accepts all liability and responsibility.

3. DPA TERMS

Alert Logic and the signatory below at the address below (“Customer”) hereby enter into this DPA effective as of the last signature date below. This DPA is incorporated into and forms part of the Agreement.

- a. **Provision of the Service.** Alert Logic provides the Services to Customer under the Agreement. In connection with the Services, the parties anticipate that Alert Logic may process Customer Data that contains personal data relating to data subjects.
- b. **The Parties’ Roles.** The parties agree that with regard to the processing of personal data, Customer is a controller, Alert Logic is a processor, and that Alert Logic or members of the Alert Logic Group will engage subprocessors pursuant to the requirements of this DPA.
- c. **Customer Responsibilities.** Customer shall, in its use of the Service, process personal data

in accordance with the requirements of Applicable Law. For the avoidance of doubt, Customer's instructions for the processing of personal data shall comply with Applicable Law. Customer shall have sole responsibility for the accuracy, quality, required consents, and legality of the personal data and the means by which Customer acquired and may processes or transfer such personal data.

- d. **Processing Purposes.** Alert Logic shall keep personal data confidential and shall only process personal data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) processing in accordance with the Agreement and applicable Order Form(s); (ii) processing initiated and consented to by Customer or Users in their use of the Service; and (iii) processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. Alert Logic shall not be required to comply with or observe Customer's instructions if such instructions would violate the Applicable Law or the request of a data subject.
- e. **Scope.** The scope of the processing of personal data by Alert Logic is limited to the performance of the Service pursuant to the Agreement.
- f. **Purpose.** The subject matter and duration of the processing, nature and purpose of the processing, and types of personal data and categories of data subjects under this DPA are detailed in this DPA and further in Appendix 1.
- g. **Data Subject Requests.** Alert Logic will comply with reasonable requests by Customer to support Customer's obligations in relation to data subject's rights under Applicable Law. To the extent legally permitted, Alert Logic shall promptly notify Customer if Alert Logic receives a request from a data subject to exercise the right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, object to the processing, or a right not to be subject to an automated individual decision making ("Data Subject Request"). In addition, to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Alert Logic shall, upon Customer's request, provide commercially-reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Alert Logic is legally authorized to do so, and the response to such Data Subject Request is required under Applicable Law. To the extent legally permitted, Customer shall be responsible for any costs arising from Alert Logic's provision of such assistance.
- h. **Alert Logic Personnel.** Alert Logic shall ensure that its personnel engaged in the processing of personal data are informed of the confidential nature of the personal data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements at least as protective as this DPA. Alert Logic shall take commercially-reasonable steps to ensure the reliability of any Alert Logic personnel engaged in the processing of personal data. Alert Logic shall ensure that Alert Logic's access to personal data is limited to those personnel assisting in the provision of the Service in accordance with the Agreement.

- i. **Data Protection Officer.** Alert Logic shall has appointed a data protection officer, or the equivalent, in any jurisdiction in which such appointment is required by Applicable Law. The DPO may be reached at privacy@alertlogic.com.
- j. **Subprocessors.** Customer has instructed or authorized the use of subprocessors to assist Alert Logic with respect to the performance of Alert Logic's obligations under the Agreement and Alert Logic agrees to be responsible for the acts or omissions of such subprocessors to the same extent as if Alert Logic was performing the services directly. Upon written request of the Customer, Alert Logic will provide to Customer a list of its then-current subprocessors. Customer acknowledges and agrees that (a) Alert Logic's Affiliates may be retained as subprocessors; and (b) Alert Logic and Alert Logic's Affiliates respectively may engage third-party subprocessors in connection with the provision of the Service. Customer may request to be notified of new subprocessors for each applicable Service to which Customer uses and if so requested, Alert Logic shall provide notification of a new subprocessor(s) before authorizing any new subprocessor(s) to process personal data in connection with the provision of the applicable Service. In order to exercise its right to object to Alert Logic's use of a new subprocessor, Customer shall notify Alert Logic promptly in writing within ten (10) business days after receipt of Alert Logic's notice in accordance with the mechanism set out above. In the event Customer objects to a new subprocessor, and that objection is not unreasonable, Alert Logic will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially-reasonable change to Customer's configuration or use of the Service to avoid processing of personal data by the objected-to new subprocessor without unreasonably burdening the Customer. If Alert Logic is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Service which cannot be provided by Alert Logic without the use of the objected-to new subprocessor by providing written notice to Alert Logic.
- k. **Subprocessor Agreements.** Alert Logic will require all approved subprocessors to provide sufficient guarantees in writing with respect to technical and organizational measures governing the processing of personal data in the form of the Clauses, as the same may be amended. Alert Logic further agrees to take reasonable steps to ensure all subcontractors comply with this DPA and the required measures set out under the Clauses. The parties agree that the copies of the subprocessor agreements that must be provided by Alert Logic to Customer pursuant to Clause 5(j) of the Clauses may have all commercial information, or clauses unrelated to the Clauses or their equivalent, removed by Alert Logic beforehand; and, that such copies will be provided by Alert Logic, in a manner to be determined in its discretion, only upon request by Customer.
- l. **Security Measures.** Alert Logic shall maintain appropriate organizational and technical measures for protection of the security to secure personal data from unauthorized access, use, disclosure, destruction, or loss, and against unlawful, accidental, or unauthorized destruction, alteration, damage, loss, disclosure, or access. Alert Logic regularly monitors compliance with the measures set forth in the applicable Security & Compliance Documentation. Alert Logic will not materially decrease the overall security of the Service during Customer's and/or Authorized Affiliates' subscription term.

- m. **Third-Party Certifications and Audit Results.** Alert Logic has attained the third-party certifications and audit results set forth in the Security & Compliance Documentation. Upon Customer's written request at reasonable intervals of not more than once annually, and subject to the confidentiality obligations set forth in the Agreement, Alert Logic shall make available to Customer a copy of Alert Logic's then most recent summary reports for such third-party certifications or audit results, as applicable.
- n. **Notifications Regarding Customer Data.** Alert Logic has in place reasonable and appropriate security incident management policies and procedures, and shall notify Customer without undue delay after becoming aware of the unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data, including personal data, transmitted, stored or otherwise processed by Alert Logic or its subprocessors of which Alert Logic becomes aware (hereinafter, a "Customer Data Incident"), as required to assist the Customer in ensuring compliance with its obligations to notify the Supervisory Authority in the event of personal data breach. Alert Logic shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Alert Logic deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident, to the extent that the remediation is within Alert Logic's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Users.
- o. **Return of Customer Data.** Alert Logic shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and time periods specified in the Security & Compliance Documentation, unless the retention of the data is requested from Alert Logic according to mandatory statutory laws.

4. APPLICATION OF THIS DPA.

- a. **Authorized Affiliates.** The parties agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Alert Logic and each such Authorized Affiliate. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. Any violation by an Authorized Affiliate shall be deemed a violation by Customer.
- b. **Customer Entities.** If the Customer entity signing this DPA:
 - i. is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Alert Logic entity (i.e., either Alert Logic, Inc. or a subsidiary of Alert Logic, Inc.) that is party to the Agreement is party to this DPA.
 - ii. has executed an Order Form with Alert Logic or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Alert Logic entity that is a party to such Order Form is a party to this DPA.
 - iii. is neither a party to an Order Form nor the Master Terms and Conditions, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement or an Order Form executes this DPA.

- c. **Exercise of Rights.** Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under Applicable Law be entitled to exercise the rights and seek remedies under this DPA. If, however, Applicable Law requires the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Alert Logic through the Customer then (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.
- d. **Liability.** Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Alert Logic, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Alert Logic's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including its Appendices.
- e. **Communications.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Alert Logic under this DPA and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

5. MISCELLANEOUS.

- a. **Regulatory References.** A reference in this Addendum to a section in any of the Applicable Law(s) means the section as in effect or as amended, and for which Alert Logic (if and to the extent applicable) and Customer's compliance is required.
- b. **GDPR.** Alert Logic will process personal data in accordance with the GDPR requirements directly applicable to Alert Logic's provision of the Service.
- c. **California Consumer Privacy Act Compliance.** Alert Logic acknowledges that personal information may include information about individuals protected under the California Consumer Privacy Act of 2018 ("CCPA"). Accordingly, Service Provider certifies that it: (i) understands the restrictions set forth in the CCPA and that it will comply with the same; (ii) it will not retain, use, or disclose any personal information for any purpose other than the specific purpose of performing the Services specified in the Agreement, including retaining, using or disclosing such personal information for a commercial purpose other than providing the Services specified in the Agreement; and (iii) it will not "sell" any personal information, as such term is defined in the CCPA. Alert Logic will obtain from any affiliate or subcontractor with whom it shares any personal information a certification substantially similar to the one set forth in subsection (i), above. Upon request from Customer, Alert Logic will provide

reasonable assistance in responding to requests to exercise an individual's rights under CCPA. Furthermore, Alert Logic agrees to execute any other documents that may be reasonably requested by Customer for purposes of Customer's efforts to comply with CCPA. To the extent legally permitted, Customer shall be responsible for any costs arising from Alert Logic's provision of such assistance.

- d. **Data Protection Impact Assessment.** Upon Customer's reasonable request, but not more than annually, Alert Logic shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Applicable Law to carry out a data protection impact assessment or its equivalent related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Alert Logic. Alert Logic shall provide reasonable assistance to Customer in the cooperation or prior consultation with the any requirements or obligations imposed on Customer by a Supervisory Authority having appropriate jurisdiction over the Customer and the Services provided to it by Alert Logic under the Agreement.
- e. **Customer's Processing Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to Alert Logic for the processing of personal data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Clauses, the following is deemed an instruction by the Customer to process personal data: (a) in accordance with the Agreement and applicable Order Form(s); (b) as initiated by Customer or Users in their use of the Service and (c) to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.
- f. **Audits.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Clauses shall be carried out in accordance with the following specifications: Alert Logic agrees that Customer may audit Alert Logic's overall compliance with the terms of this DPA and the technical and organizational security measures implemented by Alert Logic (as documented in Appendix 2 to the Clauses) at any time by reviewing independent third-party audit report summaries obtained and provided by Alert Logic. Such audit may be carried out by Customer or its mutually agreed upon internal or external auditors only through their review of independent third-party audit reports summaries obtained and provided by Alert Logic. Such audits shall be carried out remotely to the extent feasible, during normal business hours, upon reasonable notice of not less than thirty (30) days, without disruption to the business of Alert Logic and without Customer or the auditors obtaining access to Alert Logic's premises, network, or otherwise breaching or putting at risk Alert Logic's obligations of confidentiality regarding data which is not the property of Customer.

Alert Logic will conduct regular internal audits with respect to the technical and organizational security measures specified in Appendix 2 to the Clauses and will submit the summary audit reports to Customer following Customer's written request, and subject to the confidentiality obligations set forth in the Agreement.

- g. **Data Deletion.** The parties agree that the certification of deletion of personal data that is described in Clause 12(1) of the Clauses shall be provided by Alert Logic to Customer only upon Customer's request.

- h. **Order of Precedence.** This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Clauses, the Clauses will prevail.
- i. **Interpretation.** Any ambiguity in this DPA shall be resolved in favor of a meaning that permits compliance with Applicable Law. The titles and headings set forth at the beginning of each Section hereof are inserted for convenience of reference only and shall in no way be construed as a part of this DPA or as a limitation on the scope of the particular provision to which it refers.
- j. **Invalid or Unenforceable Provision.** The provisions of this DPA shall be severable. The invalidity or unenforceability of any particular provision of this DPA shall be construed, in all respects, as if such invalid or unenforceable provision had been omitted and shall not affect the validity and enforceability of the other provisions hereof.
- k. **Counterparts; Electronically Transmitted Documents and Signatures.** This DPA may be executed in one or more counterparts, each of which are deemed an original and all of which together constitute one and the same instrument, it being understood that the parties need not sign the same counterpart. A manual signature on this DPA, which image is transmitted electronically, will constitute an original signature for all purposes. The delivery of this DPA, including signature pages, by any electronic means intended to preserve the original graphic and pictorial appearance of a document, including sending in portable document format (“PDF”), will have the same effect as physical delivery of the paper document bearing the original signature. Further, the parties agree that this DPA may be signed by means of an electronic signature, provided that such signature and any related signing process comply fully with all applicable.

List of Schedules:

Annex 1: Standard Contractual Clauses – Required Information

Appendix 1: Details of the Processing

Appendix 2: Technical Standards

Appendix 3: Sub-processors as of DPA Execution

[The Next Page is the Signature Page

The Remainder of This Page is Intentionally Blank]



IN WITNESS WHEREOF, the parties have caused this Data Protection Agreement to be executed on their behalves on the date first written above.

CUSTOMER

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

ALERT LOGIC, INC.

Signature: ^{DocuSigned by:} Sheila Flaherty
F331A08A50FD463...

Print Name: Sheila M. Flaherty

Title: Chief Legal & Administrative Officer

Date: 3/26/2020

ALERT LOGIC UK LTD

Signature: ^{DocuSigned by:} Sheila Flaherty
F331A08A50FD463...

Print Name: Sheila M. Flaherty

Title: Director

Date: 3/26/2020



ANNEX 1

**Commission Decision C(2010)593, or the equivalent as revised
Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, the Clauses as detailed [here](#).

If the Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

Name of the data exporting organisation:.....

Address:

Tel.:; fax: ; e-mail:.....

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: Alert Logic, Inc.

Address: 1776 Yorktown, Suite 150, Houston, Texas 77056

Tel.: 1.877.484.8383 ; fax: 1.713.660.7988 ; e-mail: dpa@alertlogic.com

Other information needed to identify the organisation:

.....
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the Clauses as set out [here](#) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)


On behalf of the data importer: Alert Logic, Inc.

Name (written out in full): Sheila M. Flaherty

Position: Chief Legal & Administrative Officer

Address: 1776 Yorktown, Suite 150, Houston, Texas 77056

Other information necessary in order for the contract to be binding (if any):

Signature .....
F331A08A50FD463...

(stamp of organisation)



APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the legal entity that has executed the Data Processing Agreement based on the Standard Contractual Clauses as a Data Exporter established within the European Economic area and Switzerland that have purchased the Service on the basis of one or more Order Form(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data importer, Alert Logic, Inc., is a cyber security service provider which processes personal data upon the instruction of the data exporter in accordance with an agreement for services and solely in accordance with the terms of such agreement and the applicable Data Processing Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit personal data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects:

- Customers, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customers, business partners, and vendors
- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit personal data, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- First and last name
- Business contact information (company, email, phone, physical business address)
- Personal contact information (email, cell phone)
- Title
- Position
- Employer
- ID data
- Professional life data
- Personal life data (in the form of security questions and answers)
- Connection data
- Localization data

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Not Applicable

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing of personal data by the data importer is solely pursuant to the performance of the Service under the applicable agreement for services and at the instruction of the Data Exporter.


DATA EXPORTER

Name:.....

Authorised Signature

DATA IMPORTER: ALERT LOGIC, INC.

Name: Sheila M. Flaherty, Chief Legal & Administrative Officer

Authorised Signature: 

F331A08A50FD463...



APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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):

1. Physical access monitoring

Measures to prevent unauthorised persons from gaining physical access to data processing facilities where Personal Data are processed and used:

Alert Logic corporate offices include all the departments necessary to sustain our business and include our Operations, Research & Development, Security Operations, and Support functions. Alert Logic maintains a digital closed circuit television surveillance system to monitor access to Alert Logic facilities and Security Operations Center. Surveillance cameras are located at numerous ingress and egress points.

Visitors to our corporate offices are required to wear visitor badges and have an employee escort. Employees and contractors are required to use a combination of card keys and numeric keypad readers. These security mechanisms control access to the building during business and non-business hours and restrict resources to appropriate personnel.

Our Data Centers are in highly secure co-location facilities. These facilities are protected with various physical and environmental access controls that would be difficult and costly to duplicate in our corporate offices.

The buildings are reinforced physical structures that feature elements such as concrete bollards around the perimeters, steel lined walls, bulletproof glass, and barbed wire perimeters. The facilities are protected by onsite security officers and state of the art digital recording systems 24x7x365.

Our personnel are required to wear visitor badges and are escorted by data center provider personnel. Physical access is controlled through mechanisms such as the use of card key authentication and biometrics. Our provider maintains a list of personnel that are authorized to enter the server room and our cage. The cage restricts access to Alert Logic's hardware and can only be opened by the data center provider's personnel.

Fire protection systems include smoke detectors and suppression systems designed to provide early warning and containment of a fire. Air conditioning is used to control temperature and humidity to acceptable operating ranges. Raised floors and seismically rated equipment protect against water, hurricane or earthquake damage. The facilities include diesel powered electrical generators, back up battery systems and redundant external communication connections.

2. System access monitoring

Measures to prevent unauthorised persons from being able to use the data processing systems:

Employees are explicitly granted only the rights, privileges and access necessary to accomplish their assigned duties. Development, back office, and production systems are managed by separate IT groups.

Access to all systems requires management approval, a user ID and password. Users and administrators are uniquely assigned user IDs in order to be identified and authenticated to our systems. User IDs provide the mechanism by which we promote resource availability and protect our systems from unauthorized access, alteration, loss, and disclosure of information.

Local and remote authentication to all systems is protected via VPN and with standard password controls that include: complexity rules, maximum number of failed access attempts, minimum length and expiration. All employees are responsible for maintaining the confidentiality of their passwords.

Logical access to routers and firewalls is restricted to the infrastructure team. Administrator level access to the Threat, Log, and Web Security Manager databases and all configuration files is restricted to the Production Support Team.

Employee access to the remote customer appliances are accessed through establishing a VPN connection using multifactor authentication; separate authenticating through LDAP to a jumphost system; then initiating a SSH from our own internal network with unique credentials. Additionally, customer appliances are configured to only accept inbound SSH connections from a designated Alert Logic IP address range. This access is utilized to provide our customers with technical support for the appliances that are in the field.

3. Data access monitoring

Measures to ensure that the persons authorised to use a data processing system have access only to the data which they have the authority to access and that the Personal Data cannot be read, copied, altered or removed without authorisation during the processing, use or after the storage thereof:

Alert Logic logs, monitors, and reviews server and application event logs on a daily basis. Administrative users are required to log onto appliances and our servers as non-privileged users and then switch to privileged accounts. The act of switching accounts is logged by our systems. We do not allow remote root logins to our systems.

Alert Logic employees are granted only those privileges and accesses necessary to successfully accomplish their assigned duties. Back office IT resources and Alert Logic's customer production environment are managed by separate IT groups who assign all passwords for their respective networked systems. Password rules (i.e., password minimum length, password expiration, maximum unsuccessful log in attempts) are in place for each user and follow industry best practices. A request for a new user ID or changes in access levels on an existing user ID must be submitted

as a written request from management. Alert Logic enforces password complexity requirements and requires users to change their passwords within Active Directory. Remote and local access to the customer-facing production environment is authenticated through synchronized 2FA VPN and directory services to provide access to authorized personnel with a valid user ID and password.

4. Disclosure monitoring

Measures to ensure that the Personal Data are not read, copied, altered or removed without authorisation during the electronic transmission or transport or data carrier backup thereof and that it will be possible to review and determine which bodies have been envisaged as the recipient of a Personal Data transfer by way of data transmission facilities:

Customer appliances regularly communicate with the Alert Logic data center through encrypted Internet channels. The encryption technology utilized varies depending on the service. Threat Manager uses the Advanced Encryption Standard (AES) with 256-bit symmetric keys. Depending on the performance needs, Log Manager and Web Security Manager use Secure Sockets Layer (SSL) with 2,048 primes.

5. Input monitoring

Measures to ensure that it will be possible to review and determine after the fact whether and by whom Personal Data was entered into, modified in or removed from data processing systems:

Once received within Alert Logic's network, log data is stored within an Alert Logic defined container called a packet. Log messages are stored within a packet as a stream of compressed blocks and for each block we calculate a SHA-256 digest. These block digests are stored separately within the packet header, and are verified every time the log messages within a block are read. The packets are generated on the on-premise appliance soon after reception and prior to transport to the Alert Logic data center.

Data integrity is monitored and validated as each data packet is received. A SHA-256 digest is calculated for the entire packet and verified when received and written to the static Alert Logic data-grid. This audit and data-store prevents the deletion or modification of individual records and allows organizations to count on the accuracy and the integrity of the log records. In order to ensure replications are successful, the status of the data replication and packet validation process is monitored by the Alert Logic Infrastructure Support team on a real-time basis. Integrity checks will alert if corruption were to occur, log the incident, and escalate to the Infrastructure Support team for repair.

Data Expiration (deletion) is based on the customer data retention policy specified within the sales contract. While log retention period options span from 90 days to multiple years, customers frequently license 1 year according to the PCI-DSS mandate. Alert Logic utilizes a first-in-first-out (FIFO) method of deleting data that exceeds the retention policy time period. A data volume that extends beyond the retention period is disconnected from the SAN storage; at which point the data volume is no longer accessible via the UI and can no longer accept new data. The storage vendor's delete functionality is utilized to completely delete the LUN from the SAN and then prepare the data block for re-use at a later date.

6. Job monitoring

Measures to ensure that Personal Data, which are processed under commission, can be processed only in accordance with the Controller's Instructions:

Alert Logic is processing customer system log files and data traffic (IP Traffic) in order to analyse for security threads such as suspicious user / admin activities, SQL spoofing, and other – sophisticated – hacker attacks. It also identifies activities caused by viruses, worms, and other malware. Alert Logic does not release this information to other sub-processors.

7. Availability monitoring

Measures to ensure Personal Data is protected against accidental destruction and loss:

Our production data centers are a dual processing pair to provide disaster recovery and business continuity in the event of a catastrophic failure. The production network's instances are duplicated at the backup site, and are configured to mirror all operational data. Full systems backups including user organization data are performed in real-time at the data center facility via the redundant architecture that is in place for data replication. Replication activities are monitored in real time and e-mail notifications alert the Infrastructure and Production Support groups of any data errors and events. Random data restoration of individual files is performed on an on-going basis as part of Alert Logic's daily operations.

Upon initial deployment, appliance configurations are centralized and stored in our data center environment. Changes to appliance configurations are captured and backed up via the replication process.

8. Separation monitoring

Measures to ensure that data collected for different purposes can be processed separately:

Each customer's data is stored in either a private table space or private database, and these are never shared across customers. In addition, customer specific data is stored in a namespace associated with that particular customer. All application users must first authenticate as a user in that namespace to gain access to the data.

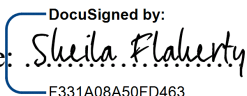
DATA EXPORTER:

Name:

Authorised Signature

DATA IMPORTER: ALERT LOGIC, INC.

Name: Sheila M. Flaherty, Chief Legal & Administrative Officer

Authorised Signature: 

DocuSigned by:
F331A08A50FD463...



APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

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

The list of subprocessors approved by the data importer as of the effective date of the DPA is as set forth below:

Entity Name	Corporate Location	Services provided
Amazon Web Services	Seattle, WA	Cloud hosting and storage services
Ntirety	Denver, CO	Co-location Data Center
Equinix	Redwood City, CA	Co-location Data Center
Next Generation Data	Newport, UK	Co-location Data Center
Zendesk	San Francisco, CA	Customer Support portal
MailChimp	Atlanta, GA	Automated Service and Incident notifications
Auth0	Bellevue, WA	Authentication Service provider
Alert Media	Austin, TX	Automated Service and Incident notifications
Whispir	Seattle, WA	Email delivery
Atlassian	Sydney, Australia	Status Page

DATA EXPORTER:

Name:.....

Authorised Signature

DATA IMPORTER: ALERT LOGIC, INC.

Name: Sheila M. Flaherty, Chief Legal & Administrative Officer

Authorised Signature 