ALERT LOGIC DATA PROCESSING AGREEMENT

PARTIES

This Data Processing Agreement ("**DPA**") is entered into by the Customer and Alert Logic, as defined at Section 2 of this DPA.

INTERPRETATION

(i) This DPA, including **Annex 1 (*EU GDPR - Standard Contractual Clauses*)** and **Annex 2 (*UK GDPR - Standard Contractual Clauses)*** (and their respective Appendices), to the extent applicable, **Annex 3 (*Description of Technical and Organisational Measures*)** and **Annex 4 (*Description of Processing*)**, form part of and is incorporated by reference into the written or electronic services agreement according to which Alert Logic provides Services to Customer (the "**Agreement**").

(ii) Customer enters into this DPA on its own behalf, and if Alert Logic processes personal data on behalf of an Authorized Affiliate, and such Authorized Affiliate is a controller, also on the behalf of its Authorized Affiliates.

(iii) All capitalized terms not defined in this DPA have the same meanings as attributed to them in the Agreement.

(iv) This DPA is an addendum to and forms part of the Agreement. In the event of a conflict between the Agreement and this DPA as regards the Data Protection Legislation or the CCPA, this DPA shall take precedence.

AGREED

1. PURPOSE

This DPA applies to the processing of Customer Data for the purposes set forth in the Agreement and this DPA.

2. DPA DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer. "**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 that is a party to this DPA as follows: (i) if Customer is located in North America, Alert Logic, Inc., a company incorporated in the State of Delaware in the United States; or (ii) if Customer is located outside North America, Alert Logic UK Limited, a company incorporated under the laws of England and Wales with Company Number 08857442.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) that: (i) is subject to Data Protection Legislation; and (ii) 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.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code Section 1798.100 et seq., and its implementing regulations.

"**Commissioner**" means the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

"**Customer**" means the counterparty entering into an Order Form with Alert Logic.

"**Customer Data**" means all Personal Data transmitted by or on behalf of Customer or an Authorized Affiliate to Alert Logic

for the purposes of providing the Service(s).

"**Data Protection Legislation**" means: (i) to the extent the UK GDPR applies, all applicable data protection and privacy legislation in force from time to time in the UK including, without limitation, the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) ("**DPA 2018**"); and (ii) to the extent the EU GDPR applies, all applicable data protection and privacy legislation in force from time to time in the European Union and any member state of the European Union including, without limitation, the EU GDPR.

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

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679 of 27 April 2016.

"**Instructions**" means instructions from Customer regarding the processing of Customer Data as embodied in the Agreement, an Order Form, and this DPA, it being understood that these documents may be updated from time-to-time to reflect additional agreed upon instructions from Customer to Alert Logic.

"**Listing Site**" means the Alert Logic website which provides a list of appointed subprocessors (https://www.alertlogic.com/sub-processor-listing/, as updated or amended from time to time). The parties acknowledge that such subprocessors are "Service Providers" under the CCPA.

"**Order Form**" means a written or electronic ordering document effected by 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 to Alert Logic for those Services. For purposes of this DPA, an Order Form includes any master terms (e.g., an MSA or MTC) linked or referenced in such Order Form.

"**Personal Information**", "**Service Provider**", "**Sale**", and "**Sell**" shall all have the same meanings as in the California Consumer Privacy Act.

"**Regulator**" means: (i) to the extent the EU GDPR applies, a supervisory authority that has jurisdiction over Customer's processing of Customer Data; and (ii) to the extent the UK GDPR applies, the Commissioner.

"**Service(s)**" means any and all services provided by Alert Logic that process Customer Data upon Customer's Instruction, where those Services are identified in an Order Form.

"**Standard Contractual Clauses**" means:

(i) To the extent the EU GDPR applies, the European Commission's Standard Contractual Clauses for the transfer of Customer Data from the European Union to processors established in third countries, as set out at **Annex 1 (*EU GDPR - Standard Contractual Clauses*)**; and

(ii) To the extent the UK GDPR applies, the United Kingdom's Standard Contractual Clauses for the transfer of Customer Data from the UK to processors established in third countries, as set out at **Annex 2 (*UK GDPR - Standard Contractual Clauses)***.

"**UK**" means the United Kingdom.

"**UK GDPR**" has the meaning given to it in the meaning given to it in Section 3(10) (as supplemented by Section 205(4)) of the DPA 2018.

"**User**" has the meaning given to it in the Order Form. If no definition is in the Order Form, "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.

The terms "**controller**", "**processor**", "**process/processing**", "**data subject**", "**personal data**", "**personal data breach**", and "**supervisory authority**" shall all have the same meanings as given them in the Data Protection Legislation.

3. DPA TERMS.

3.1 The Data Protection Legislation

a. **The Parties' Roles.**

(i) The parties agree that with regard to the processing of Customer Data under the Data Protection Legislation, Customer is a controller and Alert Logic is a processor.

(ii) Alert Logic shall only process Customer Data on behalf of Customer in accordance with and for the purposes set out in the Instructions.

(iii) To the extent that the processing of Customer Data is:

(a) subject to the EU GDPR, Alert Logic may only process Customer Data otherwise in accordance with Customer's Instructions to the extent that Alert Logic is required to do so by European Union or Member State law to which Alert Logic is subject; or
(b) subject to the UK GDPR, Alert Logic may only process Customer Data otherwise in accordance with Customer's Instructions to the extent that it is required to do so by UK law to which Alert Logic is subject,

and in each case, Alert Logic shall inform Customer of that legal requirement prior to performing any processing, unless that law prohibits such notification on important grounds of public interest.

(iv) Alert Logic shall inform Customer if, in Alert Logic's opinion that Customer's Instructions violate the Data Protection Legislation.

(v) Particulars of the processing:

(a) **Annex 4** (***Description of Processing***) sets out the scope, nature and purpose of processing under this DPA, the duration of the processing and the types of Customer Data and categories of data subject.

(b) Alert Logic may process Customer Data as part of Customer's use of the Services contemplated in the Agreement.

(c) The duration of processing will be the same as the duration of the Agreement, except as determined by applicable law or otherwise agreed between the parties.

(d The categories of data subjects are set out in **Annex 4 (*Description of Processing*)**.

(e) The types of Customer Data processed by Alert Logic are set out in **Annex 4 (*Description of Processing*)**.

b. **Customer's Warranties.** Customer represents and warrants that:

(i) the Data Protection Legislation does not prevent Alert Logic from fulfilling the Instructions, or from performing Customer's obligations under this DPA;

(ii) it has complied and continues to comply with the Data Protection Legislation, including (but not limited to):
(a) obtaining any necessary consents from and/or giving any necessary notices to data subjects in respect of the

Customer Data; and (b) ensuring a lawful basis is in place to disclose the Customer Data to Alert Logic, to enable the lawful processing of Customer Data as set out in this DPA and as contemplated by the Agreement; and

(iii) it has reviewed and assessed the requirements of the Data Protection Legislation and confirms that such security measures referenced in **Annex 3 (*Description of Technical and Organisational Measures*)** are appropriate to the risks that are presented by processing the Customer Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Customer Data, having regard to the state of technological development, the cost of implementing any measures and the nature, scope, context and purposes of the processing, in accordance with the Data Protection Legislation, and Customer.

c. **Security Measures.** Alert Logic shall implement appropriate technical and organisational security measures, as further specified in **Annex 3 (*Description of Technical and Organisational Measures*)**, to ensure a level of security appropriate to the risk.

d. **Duty of Confidentiality**

Alert Logic shall ensure that any personnel engaged and authorised by Alert Logic to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality.

e. **Notification of Personal Data Breach**

(i) Alert Logic shall notify Customer without undue delay and in any case within forty-eight hours of Alert Logic confirming that a personal data breach, to the extent involving Customer Data, has occurred;

(ii) Alert Logic shall make reasonable efforts to identify the cause of such an incident and take steps as Alert Logic deems necessary and reasonable in order to remediate the cause, to the extent that any such remediation is within Alert Logic's reasonable control. The obligations under this **Clause 3.1(e)(ii)** shall not apply to incidents that are caused by Customer or its Users.

f. **Audit and Inspection**

(i) Alert Logic shall, upon reasonable written request from Customer make available to Customer all information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA.

(ii) Alert Logic shall allow for and contribute to reasonable audits by Customer or Customer's designated auditor, to demonstrate compliance with the obligations set forth in this DPA.

(iii) Customer agrees that any such audit or inspection under **Clause 3.1(f)(ii)** of this DPA and **Clause 5(f)** and **Clause 12(2)** of the Standard Contractual Clauses must be carried out in accordance with the following requirements:

(a) at Customer's expense (including, but not limited to, Customer promptly reimbursing Alert Logic for any time expended in any such inspection at Alert Logic's then-current professional services rates, which shall be made available upon request);

(b) agreed in advance between the parties in writing;

(c) at reasonable intervals, during local business hours of Alert Logic and upon not less than thirty (30) calendar days of advance written notice unless in Customer's reasonable belief an identifiable, material non-conformance has arisen;

(d) conducted in a way which does not interfere with Alert Logic's day-to-day business;

(e) subject to the confidentiality obligations in the Agreement or, where Customer's designated auditor conducts the audit, such auditor must be a professional bound by a duty of confidentiality or subject to a suitable non-disclosure agreement; and

(f) each audit or inspection shall, in the first instance, be carried out virtually (off-premises or without access to physical facilities of Alert Logic). Inspections at the premises or physical facilities of Alert Logic may only take place if, in the opinion of Customer (acting reasonably, which shall include taking into account, without limitation, relevant certifications (for example, ISO27001 or similar industry certifications) held by Alert Logic) such virtual audit or inspection does not sufficiently demonstrate Alert Logic's compliance with the obligations set forth in this DPA.

g. **Data Subject Requests**. At Customer's reasonable written request, Alert Logic shall provide reasonable assistance to Customer:

(i) insofar as this is possible (taking into account the nature of the processing and the information available to Alert Logic) to support Customer's obligations in relation to a data subject's rights under the Data Protection Legislation; and

(ii) in ensuring Customer's compliance with its obligations under the Data Protection Legislation with respect to security, data protection impact assessments and consultations with a Regulator.

Customer shall reimburse Alert Logic for any time expended by Alert Logic arising from Alert Logic's provision of such assistance under this **Clause 3.1(g)** at Alert Logic's then-current professional services rates, which shall be made available to Customer upon request.

h. **Subprocessors (general authorization)**. Customer provides its prior, general authorisation for Alert Logic to appoint subprocessors (including Alert Logic's Affiliates) to assist Alert Logic with respect to Alert Logic's performance of the Services. Alert Logic is responsible for the acts or omissions of such subprocessors to the same extent as if Alert Logic were providing the Services directly.

i. **Subprocessors (changes and objections)**

(i) Alert Logic shall notify Customer of any intended changes concerning the addition or replacement of its subprocessors, thereby giving Customer the opportunity to object to such changes. Customer shall subscribe via the Listing Site to receive any notifications. Alert Logic shall provide notification of additions or replacements to the subprocessors via the Listing Site. In order to exercise its right to object to such changes, Customer shall notify Alert Logic promptly (and in any event within fifteen (15) calendar days after receipt of Alert Logic having notified Customer of such change) by sending an email to privacy@alertlogic.com.

(ii) Alert Logic shall provide notification of additions or replacements to the subprocessors via the Listing Site.

(iii) In the event that Customer objects to the change concerning the addition or replacement of a subprocessor and:

(a) cannot demonstrate, to Alert Logic's reasonable satisfaction, that the objection is due to an actual or likely breach of Data Protection Legislation, Customer shall indemnify Alert Logic (or Alert Logic's Affiliates) for any losses, damages, costs (including legal fees) and expenses suffered by Alert Logic (or Alert Logic's Affiliates) in accommodating the objection; or
(b) can demonstrate, to Alert Logic's reasonable satisfaction, that the objection is due to an actual or likely breach of Data Protection Legislation, Alert Logic will use reasonable efforts to modify the Service or recommend a commercially-reasonable change to Customer's configuration or use of the Service to prevent processing of Customer Data by the objected-tonew subprocessor without unreasonably burdening either party.

In either case, if Alert Logic is unable to make such change within a reasonable time period (not to exceed thirty (30) days), Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Service that cannot be provided by Alert Logic without the use of the objected-to new subprocessor by providing notice as allowed in the Agreement.

(iv) Pursuant to **Clause 5(h)** of the Standard Contractual Clauses, Customer agrees that Alert Logic may engage new subprocessors as described under this **Clause 3.1(i)**.

j. **Subprocessor (agreements)**

(i) Alert Logic shall ensure that it has a written agreement in place with all subprocessors which comply with the Data Protection Legislation that contains terms substantially the same as those set out in this **Clause 3.1**.

(ii) 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 Standard Contractual Clauses may be redacted as regards terms unrelated to the Standard Contractual Clauses (for example, pricing terms) and that such copies will be provided by Alert Logic in a manner to be determined in its discretion, only upon request by Customer.

k. **Return of Customer Data.** Upon termination or expiration of the Agreement, Alert Logic shall, at the written direction of Customer, delete or return Customer Data and copies thereof. To the extent that the processing of Customer Data is:

(i) subject to the EU GDPR, Alert Logic may continue to store such Customer Data, to the extent that Alert Logic is required to do so by European Union or Member State law to which Alert Logic is subject; or

(ii) subject to the UK GDPR, Alert Logic may continue to store such Customer Data, to the extent that Processor is required to do so by UK law to which Alert Logic is subject.

l. **Standard Contractual Clauses**

(i) Customer provides its prior, general authorization for Alert Logic to transfer Customer Data outside of the UK or EEA (as applicable) as required to provide the Services, provided that the Alert Logic shall ensure that all such transfers are effected in accordance with Data Protection Legislation. For these purposes, Customer shall promptly comply with any reasonable request of Alert Logic, including any request to enter into the Standard Contractual Clauses (or other standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the Commissioner from time to time (where the UK GDPR applies to the transfer).

(ii) Alert Logic may, at any time on not less than 30 calendar days' notice, replace the Standard Contractual Clauses and any other applicable provisions of this DPA with alternative standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the Commissioner from time to time (where the UK GDPR applies to the transfer).

(iii) The parties agree that the additional terms of this DPA, which supplement the Standard Contractual Clauses, concern business related issues that do not contradict the Standard Contractual Clauses.

m. **Access by public authorities**

(i) In addition to Clause 5(d)(i) of the Standard Contractual Clauses, in the event that Alert Logic: (i) receives a legally binding request from a public authority, under the laws of the country of destination for the disclosure of Customer Data transferred pursuant to this DPA; or (ii) becomes aware of any direct access by public authorities to Customer Data transferred pursuant to this DPA in accordance with the laws of the country of destination, Alert Logic shall:

(a) promptly notify Customer and, where reasonably possible, relevant data subjects promptly (if necessary with the help of Customer), unless prohibited under the laws of the country of destination, and, if prohibited from making such notifications, use its reasonable efforts to obtain the right to waive the prohibition in order to communicate as

much information as possible to Customer and/or relevant data subjects, as soon as possible; and

(b) review the legality of the request for disclosure and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Alert Logic shall, under the same conditions, assess possibilities of appeal. When challenging a request, Alert Logic shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. Alert Logic shall not disclose the Customer Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of Alert Logic under Clause 5(b) of the Standard Contractual Clauses;

(c) Where permissible under the laws of the country of destination, Alert Logic agrees to provide Customer, at regular intervals for the duration of the DPA, with as much relevant information as possible on the requests received (in particular, number of requests, type of Customer Data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.);

(d) provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request;

(e) document its legal assessment and any challenge to the request for disclosure and preserve this for the duration of the DPA. To the extent permissible under the laws of the country of destination, make the documentation available to Customer. It shall also make it available to the competent supervisory authority on request.

3.2 California Consumer Privacy Act

a. **Role of the Parties and Instructions for Processing.** Alert Logic acknowledges that Customer Data may include Customer Personal Information about individual consumers (as defined by the CCPA) and which is protected under the California Consumer Privacy Act. For the purposes of the CCPA, Alert Logic will act as a Service Provider in its performance of its obligations pursuant to the Agreement, and will only retain, use or disclose Customer Personal Information for the purpose of performing its obligations under the Agreement, and otherwise only as permitted by the CCPA or as required by applicable law.

b. **No Disclosure of Customer Personal Data.** Alert Logic shall not disclose, release, transfer, make available or otherwise communicate any Customer Personal Information to another business or third party without the prior written consent of Customer unless and to the extent that such disclosure is made to an Affiliate or Subcontractor for a business purpose pursuant to a written agreement with substantially similar CCPA provisions as provided in this Agreement. Notwithstanding the foregoing, nothing in this Agreement shall restrict Alert Logic's ability to disclose Customer Personal Information to comply with applicable laws or as otherwise permitted by the CCPA.

c. **No Sale of Customer Personal Data.** Alert Logic shall not sell, license, rent, disclose, release, transfer, make available or otherwise communicate any Customer Personal Information to another business or third party for monetary or other valuable consideration without the consent of Customer or the consumer to whom the Customer Personal Information relates. Notwithstanding the foregoing, disclosures to a Service Provider or disclosures to a third party in the context of a merger, acquisition, bankruptcy or other transaction shall be permitted in accordance with the terms of the Agreement.

d. **Access and Deletion.** Alert Logic shall Process Customer Personal Information in compliance with its obligations under the CCPA and, where possible, assist Customer to comply with Customer's obligations under the CCPA, and specifically Alert Logic shall upon Customer's request and at Customer's reasonable expense, provide Customer with the ability to delete, access or procure a copy of Customer Personal Data.

e. **Certification of Compliance.** Alert Logic certifies that it understands the foregoing obligations and shall comply with them for the duration of the Agreement and for as long as Alert Logic Processes Customer Personal Data.

3.3 Additional Terms

a. **Liability.**

(i) To the extent permitted by applicable law, Alert Logic's and all of its Affiliates' total liability, taken together in the aggregate, arising out of or related to the performance or contemplated performance of this DPA or any DPA between any Authorized Affiliate and Alert Logic, whether in contract, tort (including negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or under any other theory of liability, is set forth and limited in the Order Form; provided, that if no amount is set forth in the Order Form, then such total liability is equivalent to the total amount of fees actually received by Alert Logic from Customer for the Services under the applicable Order Form during the twelve months preceding the event giving rise to the claim.

(ii) Except where applicable Data Protection Legislation requires the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Alert Logic directly by itself, the parties agree that (1) solely the Customer that is the contracting party to the Order Form shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (2) the Customer that is the contracting party to the Order Form shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together.

b. **Interpretation.** Any ambiguity in this DPA shall be resolved in favor of a meaning that permits compliance with the Data Protection Legislation. The titles and headings set forth at the beginning of each Section are 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.

c. **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.

List of Schedules:

Annex 1: EU GDPR - Standard Contractual Clauses

Annex 2: UK GDPR - Standard Contractual Clauses

Annex 3: Description of Technical and Organisational Measures

Annex 4: Description of Processing

IN WITNESS WHEREOF, the parties have caused this DPA to be executed.

CUSTOMER

Signature:_____

Customer Legal Name: _____

Print Name:_____

Title: _____

Date: _____

ALERT LOGIC, INC.

Signature: DocuSigned by: Brett Stewart 83E5842D1F41498...

Print Name: Brett Stewart

Title: Senior Vice President, Business Operations

Date: 8/16/2021

ALERT LOGIC UK LTD

Signature: DocuSigned by: Brett Stewart 83E5842D1F41498...

Print Name: Brett Stewart

Title: Senior Vice President, Business Operations

Date: 8/16/2021

ANNEX 1

EU GDPR
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.

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 700, 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 following Contractual Clauses (the Clauses) 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.

Clause 1: Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the

Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not

violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law

enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory

authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clause. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the

subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE EU GDPR STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual 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):

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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):

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

DATA EXPORTER

Name: ……

Authorised Signature: ……

DATA IMPORTER: ALERT LOGIC, INC.

Name: Brett Stewart, Senior Vice President, Business Operations

Authorised Signature: ……DocuSigned by: Brett Stewart 83E5842D1F41498…

APPENDIX 2 TO THE EU GDPR STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual 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):

AS DESCRIBED IN ANNEX 3 (DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES)

DATA EXPORTER: ……

Name: ……

Authorised Signature: ……

DATA IMPORTER: ALERT LOGIC, INC.

Name: Brett Stewart, Senior Vice President, Business Operations

Authorised Signature: DocuSigned by: Brett Stewart 83E5842D1F41498...

ANNEX 2

UK GDPR
Standard Contractual Clauses (processors)

For the purposes of Article 46(2)(c) of the UK GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

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 700, 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 following Contractual Clauses (the Clauses) 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.

Clause 1: Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'Commissioner'* shall have the same meaning as in the UK GDPR;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the

applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses;

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been

otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

   (b) to refer the dispute to the UK courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9: Governing Law

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England and Wales.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the

personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE UK GDPR STANDARD CONTRACTUAL CLAUSES

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

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

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):

AS DESCRIBED IN ANNEX 4 (DESCRIPTION OF PROCESSING)

DATA EXPORTER

Name: ……

Authorised Signature: ……

DATA IMPORTER: ALERT LOGIC, INC.

Name: Brett Stewart, Senior Vice President, Business Operations

Authorised Signature: DocuSigned by: Brett Stewart 83E5842D1F41498...

APPENDIX 2 TO THE UK GDPR STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual 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):

AS DESCRIBED IN ANNEX 3 (DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES)

DATA EXPORTER: ……

Name: ……

Authorised Signature: ……

DATA IMPORTER: ALERT LOGIC, INC.

Name: Brett Stewart, Senior Vice President, Business Operations

Authorised Signature: ……Brett Stewart
DocuSigned by:
83E5842D1F41498...

ANNEX 3

Description of Technical and Organisational Measures

1. Physical access monitoring

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

Corporate Offices:

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 multiple ingress and egress points and recordings retained for at least 90 days.

Two factor authentication access systems are installed at each Company exterior door. Access to general office areas that are accessible by elevator during business hours requires an Alert Logic badge. Access to those same areas after business hours requires both an Alert Logic badge and PIN authentication for entry.

Visitors to our corporate offices are required to wear visitor badges and have an employee escort. These security mechanisms control access to the building during business and non-business hours and restrict resources to appropriate personnel.

Data Centers:

Alert Logic's Data Centers are located in highly secure co-location facilities. These facilities are protected with various physical access and environmental controls. The buildings are reinforced with 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 24×7×365.

Alert Logic employees when visiting the data center 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. Alert Logic co-location 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:

Alert Logic 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 master 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 Alert Logic's 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.

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 Customer 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. Alert Logic 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 is 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 Customer 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 Customer 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. Intrusion Detection services uses the Advanced Encryption Standard (AES) with 256- bit symmetric keys. Depending on the performance needs, Log Management and Web Application Firewall 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 Customer 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 Customer Data, which are processed under commission, can be processed only in accordance with the Controller's Instructions:

Alert Logic process 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 subprocessors.

7. Availability monitoring

Measures to ensure Customer 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 or private database, and these private spaces are never shared across customers. In addition, all customer-specific data is stored in a namespace associated with that customer and all application users must first authenticate as a user in that namespace to gain access to the data. Namespaces that are accessed are not directly specified by user input and are always assigned by low-level components only after verifying a specific user, customer, and password combination. This combination is verified on every individual data request.

ANNEX 4

Description of Processing

Data exporter

WHERE ANNEX 1 APPLIES:

Data exporter is the legal entity (or its Authorized Affiliate) that has executed the DPA based on the Standard Contractual Clauses as a Data Exporter established within the European Economic Area and Switzerland that will benefit from the Service on the basis of one or more Order Form(s).

WHERE ANNEX 2 APPLIES:

Data exporter is the legal entity (or its Authorized Affiliate) that has executed the DPA based on the Standard Contractual Clauses as a Data Exporter established within the United Kingdom that will benefit from the Service on the basis of one or more Order Form(s).

Data importer

Data importer, Alert Logic, Inc., is a cyber security service provider which processes Customer 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

Data exporter may submit Customer 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 Customer 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

Data exporter may submit Customer 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 Customer 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

Processing operations
The Customer Data transferred will be subject to the following basic processing activities (please specify):

The processing of Customer Data by the Data Importer is solely pursuant to the performance of the Service under the Agreement and at the instruction of the Data Exporter.