ALERT LOGIC

DATA PROCESSING AGREEMENT

PARTIES

This Data Processing Agreement ("**DPA**") is entered into by Customer and Alert Logic as of the Effective Date.

INTERPRETATION

(i) This DPA, including to the extent applicable, **Annex 1 (*2021 Standard Contractual Clauses*)**, **Annex 2 (*UK Transfers)***, **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 or solution agreement according to which Alert Logic provides Services (the "**Agreement**"). All capitalized terms not defined in this DPA have the same meanings as attributed to them in 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) If Customer previously entered into any data processing, security, and/or privacy terms applicable to the Services, this DPA will replace such terms from the Effective Date onwards.

(iv) In the event of a conflict between the Agreement and this DPA as regards to the Data Protection Legislation or the CCPA, this DPA shall take precedence. To the extent of any conflict or inconsistency between this DPA and any applicable Standard Contractual Clauses, the Standard Contractual Clauses 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 a party. "**Control**" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of such party.

"**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., including as amended by the California Privacy Rights Act of 2020 and any subsequent amendments or its implementing regulations.

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

“**Customer**” means the party that is entering into or has entered into a current Order Form with Alert Logic.

"**Customer Data**" means all personal data or, for purposes of the CCPA, Customer Personal Information, transmitted by or on behalf of Customer or an Authorized Affiliate to Alert Logic for the purposes of providing the Services.

"**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 and the Data Protection Act 2018 (and regulations made thereunder) and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (each as amended, superseded or replaced) ("**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.

"**Effective Date**" means either the effective date as set forth in the Agreement or, if Customer was a party to an Agreement prior the date this DPA was published, the date on which Customer later accepted this DPA.

"**EU 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 (including 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 is part of the "Agreement" above.

"**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.

"**Services**" means any and all services, products, or solutions provided by Alert Logic that process Customer Data upon Customer's Instruction, where those services, products, or solutions are identified in an authorized Order Form governed by the Agreement.

"**Standard Contractual Clauses**" means, depending on the circumstances, any of the following:

(i) To the extent the EU GDPR applies, the Standard Contractual Clauses approved by the European Commission in decision 2021/914 (the "**2021 Standard Contractual Clauses**"), and as further set out at **Annex 1 (*2021 Standard Contractual Clauses*)**; and

(ii) To the extent the UK GDPR applies, the 2021 Standard Contractual Clauses = and the UK Addendum on UK Transfers and as set out at **Annex 2 (*UK Addendum)***.

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

"**UK GDPR**" has 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 Agreement. If no definition is in the Agreement, "User" means a Customer employee or independent contractor who is authorized by Customer to access the Services 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.

(iv) Alert Logic shall inform Customer if, in Alert Logic's opinion, 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 as set forth in the Agreement, or, if the Agreement is silent on the duration of processing, 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'' Warranties. Customer represents and warrants that**:

(i) the Data Protection Legislation does not prevent Alert Logic from fulfilling the Instructions, or from performing any 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 the measures referenced in **Annex 3 (*Description of Technical and Organisational Measures*)** are appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Data as well as the risks to individuals).

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 to Customer Data.

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 its 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 any 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, but no more than once per a twelve month period, 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 is 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 or systems 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, in particular the implementation of the technical and orgnisational measures as described herein.

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) Customer shall subscribe to the Listing Site to receive notifications of any intended addition to or replacement of Alert Logic's subprocessors. Alert Logic shall provide notification of additions or replacements to its subprocessors via the Listing Site, thereby giving Customer the opportunity to object to such changes. Alert Logic will provide notification no less than thirty (30) calendar days prior to any such addition or replacement. In order to exercise its right to object to such additions or replacements, Customer must notify Alert Logic prior to the effective date of such subprocessor's appointment by sending an email to privacy@alertlogic.com.

(ii) 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 Services or recommend a commercially-reasonable change to Customer's configuration or use of the Services to prevent processing of Customer Data by the objected-to new 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 Services that cannot be provided by Alert Logic without the use of the objected-to new subprocessor by providing notice as allowed in the Agreement.

(iii) Pursuant to 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.

(ii) The parties agree that the copies of the subprocessor agreements that must be provided by Alert Logic to Customer pursuant to 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 Alert Logic 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 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 thirty (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 the applicable clauses in the Standard Contractual Clauses, in the event that Alert Logic: (1) 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 (2) 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 (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;

(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, then 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 the relevant provisions 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, Alert Logic shall 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. To the extent Customer Data includes Customer Personal Information, then this Section 3.2 shall apply to Customer Data to such extent. 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 Data.** Alert Logic shall not disclose, release, transfer, make available or otherwise communicate any Customer Data 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 DPA. Notwithstanding the foregoing, nothing in this DPA shall restrict Alert Logic's ability to disclose Customer Data 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 Data to another business or third party for monetary or other valuable consideration without the consent of Customer or the consumer to whom the Customer Data 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 Data 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 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 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 the Agreement and 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 Agreement; provided, that if no amount is set forth in the Agreement, 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 (12) months preceding the event giving rise to the claim. Notwithstanding anything to the contrary in the Agreement, neither party shall be liable for any indirect, consequential, exemplary, incidental, or punitive damages, including lost profits, goodwill, loss of business, or loss of data, even if the party has been advised of the possibility of such damages.

(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 either be (i) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible, or if this is not possible, (ii) construed, in all respects, as if such invalid or unenforceable provision had been omitted as if it had never been contained herein and shall not affect the validity and enforceability of the other provisions hereof.

List of Schedules:

Annex 1: 2021 Standard Contractual Clauses

Annex 2: UK Transfers

Annex 3: Description of Technical and Organisational Measures

Annex 4: Description of Processing

ANNEX 1

2021 STANDARD CONTRACTUAL CLAUSES

The parties agree that the 2021 Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area or Switzerland, either directly or via onward transfer, to any country or recipient outside the European Economic Area or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data. For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

1. Module Two (Controller to Processor) of the 2021 Standard Contractual Clauses will apply where Customer is a controller of Customer Data and Alert Logic is processing such Customer Data.

2. For Module Two (Controller to Processor), the following will apply:

   a. In Clause 7, the optional docking clause will apply;

   b. In Clause 9 of the 2021 Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in 3.1(i) of this DPA;

   c. in Clause 11 of the 2021 Standard Contractual Clauses, the optional language will not apply;

   d. in Clause 17, Option 1 will apply, the 2021 Standard Contractual Clauses will be governed by Irish law;

   e. in Clause 18(b) of the 2021 Standard Contractual Clauses, disputes will be resolved before the courts of the Republic of Ireland;

   f. in Annex I, Part A (List of Parties) of the 2021 Standard Contractual Clauses the following will apply:

      Data Exporter: Customer.

      Contact details: The physical and email address(es) designated by Customer in the Order Form.

      Data Exporter Role: The Data Exporter's role is set forth in Section 3.1(a) (The Parties' Roles) of this DPA.

      Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed the 2021 Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date.

      Data Importer: Alert Logic

      Contact details: DPA@AlertLogic.com

      Data Importer Role: The Data Importer's role is set forth in Section 3.1(a) (The Parties' Roles) of this DPA.

      Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date.

   g. in Annex I, Part B (Description of Transfer) of the 2021 Standard Contractual Clauses:

      The categories of data subjects are described in **Annex 4 (Description of Processing)**.

Alert Logic does not intentionally process any sensitive data. Pursuant to the terms of the Agreement, Alert Logic requires that sensitive data be encrypted if transmitted at all to Alert Logic. Customer's transfer of sensitive data to Alert Logic is determined and controlled by Customer in its sole discretion.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is described in described in **Annex 4 (Description of Processing)**.

The purpose of the processing is described in **Annex 4 (Description of Processing)**.

The duration of processing will be as set forth in Section 3.1(a) of the DPA, except as determined by applicable law or otherwise agreed between the parties.

For transfers to sub-processors, the subject matter and nature of the processing is set forth at https://www.alertlogic.com/sub-processor-listing/. 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.

h. in Annex I, Part C (Competent Supervisory Authority) of the 2021 Standard Contractual Clauses:

The competent supervisory authority shall be determined in accordance with Clause 13 of the 2021 Standard Contractual Clauses.

i. in Annex II of the 2021 Standard Contractual Clauses:

Alert Logic will implement and maintain security standards as set forth in **Annex 3** ***(Technical and Organizational Measures)*** of this DPA.

j. in Annex III of the 2021 Standard Contractual Clauses:

The list of sub-processors is set forth at https://www.alertlogic.com/sub-processor-listing

ANNEX 2

UK TRANSFERS

The parties agree that the UK Addendum shall apply to a UK Transfer and this Annex 2 is effective from 21 March 2022. For the avoidance of doubt, defined terms set out in Annex 2 of this Appendix 2 are set out in Part 2 Mandatory Clauses below.

Part 1: Tables

Table 1 of the Addendum shall be completed as follows:

- Data Exporter: Customer
- Contact details: as detailed in the Agreement

Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed this Addendum incorporated herein, as of the Effective Date of the Agreement.

- Data Importer: Alert Logic
- Contact details: As detailed in the Agreement

Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed this Addendum, incorporated herein, as of the Effective Date of the Agreement.

Table 2 of the Addendum shall be completed as follows:

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Shall not apply	Shall not apply	General Authorisation	As set out in Paragraph 3.1.i. of the DPA	No

Table 3 of the Addendum

Annex IA shall be completed as follows:

- Data Exporter: Customer
- Contact details: As detailed in the Agreement.
- Data Exporter Role: Module Two: The Data Exporter is a data controller.
- Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed the Approved EU SCCs, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

- Data Importer: Alert Logic
- Contact details: As detailed in the Agreement.
- Data Importer Role: Module Two: The Data Importer is a data processor.
- Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed the Approved EU SCCs, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Annex I.B shall be completed as follows:

- The categories of data subjects are described in Annex 4 (Description of Processing) of this DPA.
- The categories of personal data are described in Annex 4 (Description of Processing) of this DPA.
- The Parties do not intend for Sensitive Data to be transferred.
- The frequency of the transfer is a continuous basis for the duration of the Agreement.
- The nature of the processing is described in Annex 4 (Description of Processing) of this DPA.
- The purpose of the processing is described in Annex 4 (Description of Processing) of this DPA.
- The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.
- In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth at the Listing Site.
- The Description of Technical and Organisational Safeguards attached as Annex 3 of this DPA serves as Annex II.
- Annex III: List of Sub-processors shall not apply as Alert Logic has a general written authorisation to use Sub-processors.

Table 4 of the Addendum

The Importer may end this Addendum as set out in Section 19.

Part 2: Mandatory Clauses

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

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

Interpretation of this Addendum

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

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

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	Has the meaning as defined in the DPA.

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

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

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

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

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

Hierarchy

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

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

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

Incorporation of and changes to the EU SCCs

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

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

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

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

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

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

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

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

b. In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.8(i) of Module 2 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

e. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

k. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

l. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

m. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

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

Amendments to this Addendum

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

Scotland or Northern Ireland.

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

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

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

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

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

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

b. its risk under the Addendum,

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

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

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 Alert Logic 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 is 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 does 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 (e.g., 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 processes 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.

9. Vendor Risk Management Program

Measures to ensure all vendors are evaluated for security and privacy requirements:

Alert Logic IT Audit & Compliance team regularly monitors vendors to ensure the vendors have implemented security and privacy controls associated with the services offered. As part of the IT vendor risk management program, the following risks are assessed but not limited to the following:

- **Assess information security policies, procedures, and services provided pertaining to incident response, security awareness, business continuity and disaster recovery planning;**
- **Identify and review if third parties are storing, processing, and/or transmitting any sensitive and confidential information including PII;**
- **Obtain regulatory compliance reports for assessments such as SSAE 18 (SOC 1/SOC 2 reports), PCI DSS 3.2, ("ISO/IEC") 27001:2013, ISO 27701:2019 and other compliance mandates including vendor responses to Alert Logic's Information Security questionnaire; and**
- **Agreements are established with third parties that include clearly defined terms, conditions, and responsibilities as they relate to security, confidentiality, privacy, integrity, and availability.**

10. Information Security Program

Alert Logic's information security policies and program are based on the ("ISO/IEC") 27001:2013 standard. This international standard consists of a comprehensive set of controls comprising best practices in information security and provides a solid framework for building a secure infrastructure.

Alert Logic's security policies and programs are designed to maintain the security and availability of its systems and of its customers' data. Information security policies have been established that details the procedures for restricting logical access to electronic network resources and data from an external location including a physical access policy for restricting access to Alert Logic facilities. Alert Logic's defense-in-depth security strategy encompasses:

- **Organizational and security personnel;**
- **Physical Security ;**
- **Application Data Security;**
- **Network Security; and**
- **Privacy and Data Integrity.**

11. Incident Response Program

As part of its security program, the security staff has established a computer security incident response program so Alert Logic can recognize, analyze, and handle information security incidents and threats. Incidents or events impacting Alert Logic are processed utilizing Incident Management and Handling processes which cover Alert Logic's computing, network, data, physical and human resources components of the system. The incident handling plan includes preparation, identification, containment, eradication, recovery and lessons learned phases. Incident handling plans, processes and procedures are reviewed and tested at least annually.

ANNEX 4

Description of Processing

Data subjects

Data Exporter may submit Customer Data to the Services, 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
- Network data (including source and destination IP addresses)
- Log data

Processing operations / Purpose of processing
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 Services under the Agreement and at the instruction of the Data Exporter.