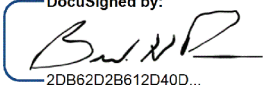




EU Data Processing Addendum

This EU Data Processing Addendum (“**Addendum**”) is made and entered into by and between AlienVault, Inc., a Delaware corporation (“**AlienVault**”) and the customer specified in the table below (“**Customer**”).

<p>AlienVault, Inc.</p> <p>DocuSigned by:  <small>2DB62D2B612D40D...</small> Brandon Pearce</p> <p>Name: _____</p> <p>Title: AVP, AT&T Cybersecurity</p> <p>Address: 208 S Akard Street Dallas, Texas 75201 Attention: General Counsel</p>	<p>Customer Name (Required): _____ (Full legal entity name)</p> <p>By (Signature Required): _____</p> <p>Your Printed Name (Required): _____</p> <p>Signature Date (Required): _____</p> <p>Customer Address (Required): _____ _____ _____</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

This Addendum, including Exhibit A, supplements the Master Services Agreement or other agreement, if any, (the “**Agreement**”) by and between AlienVault and Customer (each a “**Party**” and collectively the “**Parties**”) as such may be amended from time to time. Any liability arising hereunder between the Parties and/or any of their Affiliates shall be subject to the limitation of liability under the Agreement. For avoidance of doubt, if no such Master Services Agreement exists between the Parties, then this Addendum shall stand on its own as an enforceable agreement with respect to the Services. This Addendum will be effective as of the date AlienVault receives a complete and executed Addendum from Customer in accordance with the instructions Sections 1 and 2 below. Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control. Subject to the preceding sentences regarding liability, in the event of a conflict between the Standard Contractual Clauses and the Agreement and/or the Addendum, the Standard Contractual Clauses shall prevail (where these apply). If any provision or part-provision of this Addendum causes the Standard Contractual Clauses to become an invalid export mechanism in the relevant Extended EEA Country, it shall be deemed deleted but that shall not affect the validity and enforceability of the rest of this Addendum and the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

1. Instructions This Addendum (including the Standard Contractual Clauses, as defined below) has been pre-signed on behalf of AlienVault. To enter into this Addendum, Customer must:

- a) Complete the table above by signing and providing customer full legal entity name, address, and signatory information; and
- b) Submit the completed and signed Addendum to AlienVault via email to CyberPrivacy@att.com.

2. Effectiveness

- a) This Addendum will be effective only if it is executed and submitted to AlienVault in accordance with Section 1 above this Section 2, and all items identified as “Required” in the table are completed accurately and in full. If Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void. The Addendum will only apply to Customer’s Affiliates, contractors and agents working on AlienVault accounts.
- b) This Addendum applies to AlienVault Services purchased by Customer.
- c) Customer signatory represents to Customer that he or she has the legal authority to bind Customer and is lawfully able to enter into contracts (e.g. is not a minor).
- d) This Addendum will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this Addendum.

3. Definitions

3.1 “**Anonymous Data**” means Personal Data that has been Processed in such a manner that it can no longer be attributed to a Data Subject.

3.2 “**Authorized Employee**” means an employee of AlienVault who has a need to know or otherwise access Personal Data to enable AlienVault to perform their obligations under this Addendum or the Agreement.

3.3 “**Authorized Individual**” means an Authorized Employee or Authorized Subcontractor.

3.4 “**Authorized Subcontractor**” means a third-party subcontractor, agent, reseller, or auditor who has a need to know or otherwise access Personal Data to enable AlienVault to perform its obligations under this Addendum or the Agreement, and who is either (1) listed in the List (as defined in Section 6.2) or (2) authorized by Customer to do so under Section 6.2 of this Addendum.

3.5 “**Controller**” shall have the meaning given to it in the GDPR.

3.6 “**Customer Data**” means the data inputted by Customer or its authorized users for the purpose of using the Services.

3.7 “**Data Subject**” means an identified or identifiable person to whom Personal Data relates.

3.8 “**Data Protection Law**” has the meaning given in Section 4.1.

3.9 “**EU**” means the European Union.

3.10 “**Extended EEA Country**” means either a country within the European Economic Area; Switzerland; or the United Kingdom, and “**Extended EEA Countries**” means the foregoing countries collectively.

3.11 “**Extraterritorial Processing Entity**” has the meaning given in Section 8.1.2.

3.12 “**GDPR**” means the General Data Protection Regulation (Regulation (EU) 2016/67).

3.13 “**Instruction**” means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Customer to AlienVault and directing AlienVault to Process Personal Data.

3.14 “**Personal Data**” means any information relating to Data Subject which AlienVault Processes on behalf of Customer other than Anonymous Data.

3.15 “**Personal Data Breach**” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

3.16 “**Process**” or “**Processing**” means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

3.17 “**Processor**” has the meaning given to it in the GDPR.

3.18 “**Services**” means the AlienVault web-based service and sensors (the “**Application**”), maintenance and technical support services for the applicable Application, and any professional services, including software implementation, training, configuration, and consulting services performed by or on behalf of AlienVault for Customer.

3.19 “**Standard Contractual Clauses**” means the “standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission decision of 4 June 2021” and published under document number C(2021) 3972, available [here](#).

3.20 “**Sub-Data Processor**” means the person or entity which Processes Personal Data on behalf of the Processor.

3.21 “**Supervisory Authority**” means, as applicable, an independent public authority which is established by a member state of the European Union, Iceland, Liechtenstein, Norway, Switzerland, or the UK.

3.22 “**Third Country**” means a country not deemed adequate to receive the Personal Data under the Data Protection Laws of the applicable Extended EEA Country.

3.23 “**Transferring Customer Entity**” has the meaning given in Section 8.1.

4. Processing of Data

4.1 The rights and obligations of the Customer with respect to this Processing are described herein. Customer shall, in its use of the Services, at all times Process Personal Data, and provide Instructions for the Processing of Personal Data, in compliance with the GDPR and all applicable laws, rules and regulations concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or processing of Personal Data (the “**Data Protection Laws**”). Customer shall ensure that the Processing of Personal Data in accordance with Customer’s Instructions will not cause AlienVault to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to AlienVault by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the Instructions it provides to AlienVault regarding the Processing of such Personal Data. Customer shall not provide or make available to AlienVault any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services and shall indemnify AlienVault from all claims and losses in connection therewith.

4.2 AlienVault shall Process Personal Data only (i) for the purposes set forth in the Agreement; (ii) in accordance with the terms and conditions set forth in this Addendum and any other documented instructions provided by Customer; and (iii) in compliance with the GDPR. Customer hereby instructs AlienVault to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Customer in its use of the Services.

4.3 Following completion of the Services, at Customer’s written request, AlienVault shall return or delete the Personal Data, except as required to be retained by the Data Protection Laws. By entering into the Standard Contractual Clauses as described in Section 8 (Transfers

of Personal Data to Third Countries), the parties agree that the certification of deletion of Personal Data that is described in the Standard Contractual Clauses shall be provided by AlienVault to Customer only upon Customer's written request.

4.4 The details of the Processing of Personal Data are set out in Exhibit 1.

5. Authorized Employees

5.1 AlienVault shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

5.2 AlienVault shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and from the consequences of improperly disclosing or otherwise Processing, both during and after their engagement with AlienVault, any Personal Data except in accordance with their obligations in connection with the Services.

5.3 AlienVault shall take commercially reasonable steps to limit access to Personal Data to only Authorized Individuals.

6. Authorized Subcontractors

6.1 Customer acknowledges and agrees that AlienVault may (1) engage its Affiliates and the Authorized Subcontractors listed in the List (as defined in Section 6.2) to this Addendum to access and Process Personal Data in connection with the Services; and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data.

6.2 A list of AlienVault's current Authorized Subcontractors (the "List") is available at www.alienvault.com/legal/GDPR (such URL may be updated by AlienVault from time to time). At least ten (10) days before enabling any third party other than Authorized Subcontractors to access or participate in the Processing of Personal Data, AlienVault will add such third party to the List and notify Customer of that update via email.

6.2.1 If Customer reasonably objects to an engagement in accordance with Section 6.2, AlienVault shall provide Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If AlienVault, in its sole discretion, cannot provide any such alternative(s), or if Customer does not agree to any such alternative(s) if provided, AlienVault may terminate this Addendum. Termination shall not relieve Customer of any fees owed to AlienVault under the Agreement.

6.2.2 If Customer does not object to the engagement of a third party in accordance with Section 6.2 within ten (10) days of notice by AlienVault, that third party will be deemed an Authorized Subcontractor for the purposes of this Addendum.

6.3 AlienVault shall require that all Authorized Subcontractors have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement by AlienVault, any Personal Data except in accordance with their obligations in connection with the Services.

6.4 AlienVault shall, by way of contract or other legal act under European Union or European Union member state law (including without limitation approved codes of conduct and standard contractual clauses), require that every Authorized Subcontractor is subject to obligations regarding the Processing of Personal Data that are no less protective than those to which the AlienVault is subject under this Addendum.

6.5 AlienVault shall be liable to Customer for the acts and omissions of Authorized Subcontractors to the same extent that AlienVault would itself be liable under this Addendum had it conducted such acts or omissions.

6.6 By entering into the Standard Contractual Clauses as described in Section 8 (Transfers of Personal Data to Third Countries), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by AlienVault of the Processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Subcontractors that must be provided by AlienVault to Customer pursuant the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the AlienVault beforehand, and that such copies will be provided by the AlienVault only upon request by Customer.

7. Security of Personal Data

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, AlienVault will maintain appropriate technical and organizational measures to provide a level of security appropriate to the risk of Processing Personal Data as set out in Exhibit 2 below.

8. Transfers of Personal Data to Third Countries

Application of the Standard Contractual Clauses

8.1 Subject to Section 8.2, where the Customer, or, where applicable, a Customer Affiliate which is a party to the Agreement, acting as a Controller or a Processor (as applicable) of the Personal Data:

8.1.1 is located in an Extended EEA Country; or

8.1.2 is not located in an Extended EEA Country, but Processes Personal Data originating from an Extended EEA Country and: (i) is directly subject to the Data Protection Laws of the Extended EEA Country in relation to such Processing; or (ii) is contractually obliged to impose safeguards that are equivalent to those safeguards required under the Data

Protection Laws of the Extended EEA Country on any third parties with whom they share the Personal Data (“**Extraterritorial Processing Entity**”).

and such Customer or Customer Affiliate transfers, or facilitates the transfer of, such Personal Data to AlienVault y (each such Customer entity referred to in this section as the “**Transferring Customer Entity**”) located in a Third Country, the transfer will be undertaken on the basis of: (i) an export derogation recognised by the applicable Data Protection Law; or (ii) where (i) does not apply, adherence to an applicable framework recognised by the applicable Data Protection Law or relevant Supervisory Authority or courts in the Extended EEA Country as providing an adequate level of protection for the Personal Data (excluding the Standard Contractual Clauses); or (iii) where (i) and (ii) do not apply, the Standard Contractual Clauses as set out in Sections 8.3-8.11 below.

8.2 The Standard Contractual Clauses shall not apply as between the Transferring Customer Entity and AlienVault in respect of any Personal Data where AlienVault is established: (i) in the EU (where the Transferring Customer Entity is established or from which the Personal Data originates is within the EU); or (ii) in the EU or relevant Extended EEA Country (where the Extended EEA Country in which the Transferring Customer Entity is established or from which the Personal Data originates is outside the EU). In such cases, AlienVault shall be responsible for maintaining that any export of Personal Data to a Third Country complies with the Data Protection Laws.

Allocation of responsibilities

8.3 In all cases, for the purpose of Section III, Clause 14 of the Standard Contractual Clauses, AlienVault and the Customer, also acting on behalf of the Transferring Customer Entities as parties to the Standard Contractual Clauses acknowledge and agree that, as between the parties, the Transferring Customer Entity (acting as data exporter) is responsible for: (i) assessing the laws of the country to which the Transferring Customer Entity transfers the Transferred Personal Data; and (ii) determining whether or not the transfer meets the requirements of Section III, Clause 14(a) of the Standard Contractual Clauses. Where AlienVault (as data importer) provides information to the Transferring Customer Entity (acting as data exporter) for assisting the Transferring Customer Entity in the Transferring Customer Entity’s assessment, such information is provided on an “as is” basis for informational purposes only. Without prejudice to Section III, Clause 14(c) of the Standard Contractual Clauses, AlienVault (as data importer) shall not be liable for any losses suffered by the Transferring Customer Entity (or its Affiliates) in connection with their assessment.

8.4 Where requested by AlienVault, the Customer or Transferring Customer Entity (as applicable) shall be responsible for issuing such communications to Data Subjects as are required in order for AlienVault to comply with its obligations under the Standard Contractual Clauses.

Governing law, jurisdiction, Supervisory Authority and interpretation

8.5 AlienVault and the Customer, also acting on behalf of the Transferring Customer Entities as parties to the Standard Contractual Clauses agree that their respective obligations under the Standard Contractual Clauses shall be governed by the law(s) of, and subject to the jurisdiction of the courts of:

- 8.5.1 where the Transferring Customer Entity is established in the EU, the Netherlands;
- 8.5.2 where the Transferring Customer Entity is an Extraterritorial Processing Entity and the Transferred Personal Data originates from the EU, the Netherlands;
- 8.5.3 where the Transferring Customer Entity is established outside the EU, but within an Extended EEA Country, the Extended EEA Country in which the Transferring Customer Entity is established; and
- 8.5.4 subject to Section 8.5.2 above, where the Transferring Customer Entity is an Extraterritorial Processing Entity and the Personal Data originates from the Extended EEA, the Extended EEA Country from which the Personal Data originated.

8.6 Annex I, Part C (*Competent Supervisory Authority*) of the Standard Contractual Clauses is hereby deemed to be completed as follows:

- 8.6.1 where Section 8.5.1 of this Addendum applies, the Supervisory Authority shall be the Supervisory Authority of the EU member state in which the Transferring Customer Entity is established;
- 8.6.2 where clause Section 8.5.2 of this Addendum applies, the Supervisory Authority shall be the Supervisory Authority of the EU member state in which the Transferring Customer Entity’s has appointed an EU representative under Article 27(2) of the GDPR (“**EU Representative**”). Where an EU Representative has not been appointed, the Supervisory Authority shall be the Supervisory Authority of the Netherlands;
- 8.6.3 where Section 8.5.3 of this Addendum applies, the Supervisory Authority shall be the Supervisory Authority of the Extended EEA Country in which the Transferring Customer Entity is established; and
- 8.6.4 where Section 8.5.4 of this Addendum applies, the Supervisory Authority shall be the Supervisory Authority of the Extended EEA Country from which the Personal Data originated.

8.7 Where the applicable Extended EEA Country in which the Transferring Customer Entity is established or from where the Transferred Personal Data originated is not a member state of the EU, references in the Standard Contractual Clauses to:

- 8.7.1 “Member States of the European Union” shall refer to the applicable Extended EEA Country in which the Transferring Customer Entity is established or from where the Transferred Personal Data originated (as applicable) as determined by Section 8.5 above;

- 8.7.2 “the GDPR” shall refer to the applicable Data Protection Laws of the Extended EEA Country in which the Transferring Customer Entity is established or from where the Transferred Personal Data originated (as applicable) as determined by Section 8.5 above; and
- 8.7.3 “supervisory authority” shall refer to the Supervisory Authority in the Extended EEA Country as determined by Section 8.6 above.

8.8 Where Section 8.5.3 or Section 8.5.4 above apply and the Extended EEA Country is the UK, this Section 8 shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws and disputes between the data importer and the data exporter shall be governed by the laws of, and subject to the jurisdiction of the courts of, England & Wales.

Incorporation and interpretation of the Standard Contractual Clauses

8.9 Where the Standard Contractual Clauses apply to a transfer pursuant to Section 8.1 above and the Transferring Customer Entity agrees to comply with the obligations of a data exporter and AlienVault agrees to comply with the obligations of a data importer as set out in the Standard Contractual Clauses which are incorporated herein by reference and construed as follows:

- 8.9.1 the Standard Contractual Clauses shall constitute a separate agreement between each Transferring Customer Entity acting as a data exporter and AlienVault acting as data importer;
- 8.9.2 where the applicable sections of the Standard Contractual Clauses require the data exporter and the data importer to select a module, the Transferring Customer Entity acknowledges that:
- (i) Module Two of the Standard Contractual Clauses (*Transfer controller to processor*) shall apply where AlienVault, as data importer, is acting as the Transferring Customer Entity’s Processor; and
- (ii) Module Three of the Standard Contractual Clauses (*Transfer processor to processor*) shall apply where AlienVault, as data importer, is acting as the Transferring Customer Entity’s Sub-Data Processor.
- 8.9.3 where Module Three applies to the Transferred Personal Data (i.e. where AlienVault, as the data importer, is acting as a Sub-Data Processor), at the request of AlienVault (as data importer), the Transferring Customer Entity (as data exporter) shall provide AlienVault (as data importer) with such assistance as AlienVault (as data importer) may reasonably request to engage, consult or communicate with the Data Controller where required under Module Three of the Standard Contractual Clauses, including communicating with the Data Subject on AlienVault’s (as data importer) behalf;
- 8.9.4 for the purposes of Section II, Clause 8.1 (Module Two) and Section II, Clause 8.1 (Module Three) (as applicable) of the Standard Contractual Clauses, the instructions to AlienVault (as data importer) shall be an instruction to Process Personal Data shall be as per Section 4.1 and 4.2 of this Addendum, which in the case of Module Three constitute the instructions of the relevant Data Controller(s);
- 8.9.5 for the purposes of Section II, Clause 8.5 (Module Two) and Section II, Clause 8.5 (Module Three) (as applicable) of the Standard Contractual Clauses, AlienVault’s (as data importer) storage, erasure and return of Personal Data shall be construed by reference to Section 4.3 of this Addendum;
- 8.9.6 for the purposes of Section II, Clause 8.9 (Module Two) and Section II, Clause 8.9 (Module Three) (as applicable) of the Standard Contractual Clauses, any audit of AlienVault’s (as data importer) Processing activities covered by the Standard Contractual Clauses shall be construed by reference to Section 10.3 of this Addendum; and
- 8.9.7 for the purposes of Section II, Clause 9 (Module Two) and Section II, Clause 9 (Module Three) of the Standard Contractual Clauses, AlienVault’s (as data importer) ability to engage subcontractors shall be construed by reference to Section 6 (Authorized Subcontractors) of this Addendum.

Completion of the Annexes of the Standard Contractual Clauses

Annex I, Part A (List of parties) of the Standard Contractual Clauses is hereby deemed to be completed with: (i) the details of the exporting Transferring Customer Entity (as data exporter and Controller or Processor (as applicable)); and (ii) the details of AlienVault (as data importer and Processor or Sub-Data Processor (as applicable)), in each case as set out in Exhibit 1 of this Addendum.

8.10 Annex I, Part B (Description of the transfer) of the Standard Contractual Clauses is hereby deemed to be completed with the information set out in Exhibit 1 of this Addendum.

8.11 Annex II of the Standard Contractual Clauses (The Technical and organisational measures including technical and organisational measures to ensure the security of the data) is hereby deemed to be completed by reference to Section 7 (Security of Personal Data) of this Addendum.

9. Rights of Data Subjects

9.1 AlienVault will, to the extent permitted by law, promptly notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject’s right of: access, rectification, restriction of Processing, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively “**Data Subject Request(s)**”). If AlienVault receives a Data Subject Request in relation to Customer’s

Data, AlienVault will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

9.2 AlienVault will, at the request of the Customer, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without AlienVault's assistance, and (ii) AlienVault is able to do so in accordance with all applicable laws, rules, and regulations. Customer will be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by AlienVault.

10. Actions and Access Requests

10.1 AlienVault will, taking into account the nature of the Processing and the information available to AlienVault, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer will be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by AlienVault.

10.2 AlienVault will, taking into account the nature of the Processing and the information available to AlienVault, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer will be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by AlienVault.

10.3 Upon Customer's request, AlienVault will, no more than once per calendar year, make available for Customer's review copies of certifications or reports demonstrating AlienVault's compliance with prevailing data security standards applicable to the Processing of Customer's Personal Data

10.4 In the event of a Personal Data Breach, AlienVault will, without undue delay, inform the affected Customer of the Personal Data Breach and take such steps as AlienVault in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within AlienVault's reasonable control).

10.5 In the event of a Personal Data Breach, AlienVault will, taking into account the nature of the Processing and the information available to AlienVault, provide the affected Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority, and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

10.6 The obligations described in Sections 10.4 and 10.5 will not apply to a Personal Data Breach results from the actions or omissions of Customer. AlienVault's obligation to report or respond to a Personal Data Breach under Sections 10.4 and 10.5 will not be construed as an acknowledgement by AlienVault of any fault or liability with respect to the Personal Data Breach.

Exhibit 1

Details of Processing pursuant to Section 4.4 of this Addendum and Annex I, Part A and Part B of the Standard Contractual Clauses (where applicable)

(a) Data Controller/Data Processor (as applicable) (and data exporter where the Standard Contractual Clauses apply)

The data exporter is the Customer identified in the Addendum.

(b) Data Processor/Sub-Data Processor (as applicable) (and data importer where the Standard Contractual Clauses apply)

The data importer is AlienVault, Inc.

Amazon Web Services is a sub-data processor.

(c) Categories of Data Subjects

The Personal Data transferred of Data Subjects are Customer's end users/customer and Customer employees and contractors.

(e) Categories of Personal Data

The personal data transferred concern the following categories of data: individual name; employing company; phone number; fax number; email address; mailing address, including country; IP address; log data; device identifiers; and metadata.

(f) Sensitive data (if applicable)

The safeguards applied are as per Section 7 (Security of Personal Data) of the Addendum.

(g) Nature of Processing

The nature of processing will be subject to basic processing activities consisting of computing, storage, and content delivery on the AlienVault application.

(h) Purposes of the Processing and further Processing

The purpose of Processing is the provision of the Services and/or products and related obligations under the Agreement. Further processing may include compliance with legal and regulatory obligations; and evaluation, supporting and enhancing the performance, efficiency and security of the data importer's business and products and/or services.

(i) The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

The criteria used to determine the period for which the Personal Data will be retained is (1) service type, (2) Agreement duration, (3) custom Agreement requirements, and (4) legal requirements.

(j) For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing

As per (g) and (h) above.

Exhibit 2
Security of Personal Data

AlienVault shall maintain administrative, physical and technical safeguards for the protection of security, confidentiality, and integrity of Personal Data, including Personal Data in our SaaS offering, as set forth by achieving compliance with the ISO27001 certification/framework. A copy of applicable reports can be obtained through an account executive.