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 vendor specified in the table below ("**Vendor**").

AlienVault, Inc.

By: DocuSigned by: Andy Johnson DAECEB06DAE94D0...

Name: Andy Johnson

Title: CFO

Address: 1100 Park Place, Suite 300
San Mateo, CA 94403
Attention: General Counsel

Vendor Name (Required): _____
(Full legal entity name)

By (Signature Required): _____

Your Printed Name (Required): _____

Signature Date (Required): _____

Vendor Address (Required): _____

_____

_____

This Addendum, including Exhibit A, supplements the master services agreement or other agreement executed with Vendor (the "Agreement") by and between AlienVault and Vendor (each a "Party" and collectively the "Parties"). This Addendum will be effective as of the date AlienVault receives a complete and executed Addendum from Vendor 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.

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, Vendor must:

a) Complete the table above by signing and providing vendor full legal entity name, address, and signatory information; and

b) Submit the completed and signed Addendum to AlienVault via email to GDPR-VENDOR-DPA@alienvault.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 Vendor makes any deletions or other revisions to this Addendum, then this Addendum will be null and void. The Addendum will only apply Vendor's affiliates, contractors, and agents working on AlienVault accounts.

b) This Addendum applies to Vendor service offerings purchased by AlienVault.

c) Vendor signatory represents to Vendor that he or she has the legal authority to bind Vendor and is lawfully able to enter into contracts (e.g. is not a minor).

d) This Addendum will terminate automatically up termination of the Agreement, or as earlier terminated pursuant to the terms of this Addendum.

3. Definitions

3.1 "**Applicable Law(s)**" means any state, federal or foreign law(s), rule(s) or regulation(s) applicable to the Addendum, the Agreement, or the Processing, as well as applicable Industry Standards, including those concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or processing of Personal Data. Applicable Laws expressly include, if applicable, the United Kingdom Data Protection Act 1998 (the "**UK Data Protection Act**"), including any superseding regulation, the EU-US and Swiss-US Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework (collectively the "**Privacy Shield Framework and Principles**"), EU Directive 95/46/EC (the "**Data Directive**"), and, when effective, the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"), EU Directive 2002/58/EC (the "**ePrivacy Directive**"), and, when effective, any regulation expressly superseding the ePrivacy Directive, as well as the laws, rules, and regulations of each nation in the European Economic Area ("**Member State Law(s)**").

3.2 "**Authorized Employee**" means an employee of Vendor or a Vendor Affiliate who has a need to know or otherwise access Personal Data in order to enable Vendor to perform its obligations under this Addendum or the Agreement and who has undergone appropriate background screening and training by Vendor.

3.3 "**Authorized Person**" means an Authorized Employee or Authorized Subcontractor.

3.4 "**Authorized Subcontractor**" means a third-party subcontractor, agent, reseller, or auditor engaged by Vendor, or employee of same, that has a need to know or otherwise access Personal Data to enable Vendor to perform its obligations under this Addendum or the Agreement and that has been previously approved by AlienVault in writing to do so, and who is bound in writing by a data processing agreement pursuant to which their duties and obligations to protect Personal Data are in strict accordance with the terms hereof.

3.5 "**AlienVault Affiliate**" means any entity that owns or controls, is owned or controlled by, or is under common control or ownership with AlienVault (where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by contract, exercise of voting rights, common management, or otherwise).

3.6 "**Data Subject**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.7 "**Data Subject Rights**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.8 "**Data Protection Impact Assessment**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.9 "**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

3.10 "**Including**" and its derivatives (such as "include" and "includes") (whether or not capitalized) means "including, without limitation" unless expressly indicated otherwise.

3.11 "**Industry Standards**" means the then-current industry best data protection and data processing practices relating to the Processing of the Personal Data.

3.12 "**Instruction**" means a direction issued by AlienVault to Vendor and/or any Authorized Person, documented either in textual form (including without limitation by e-mail) or by using a software or online tool, regarding the Processing of Personal Data.

3.13 "**Personal Data**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.14 "**Personal Data Breach**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.15 "**Privacy Shield Principles**" means the privacy and data protection principles outlined in the Privacy Shield Framework and Principles, available at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.

3.16 "**Process**" or "**Processing**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.17 "**Vendor Affiliate**" means any entity that owns or controls, is owned or controlled by, or is under common control or ownership with Vendor (where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by contract, exercise of voting rights, common management, or otherwise) and that assists or enables Vendor to fulfill its obligations under the Agreement and Addendum.

3.18 "**Restricted Transfer**" means a transfer of Personal Data from the European Economic Area or Switzerland to any country or recipient: (i) not deemed by the European Commission as providing an adequate level of protection for Personal Data, and (ii) not covered by or a suitable framework or certification recognized by the relevant Supervisory Authority as providing an adequate level of protection for Personal Data, such as the Privacy Shield Framework and Principles.

3.19 "**Services**" shall have the meaning set forth in the Agreement.

3.20 "**Standard Contractual Clauses**" means the agreement executed by and between AlienVault and Vendor and attached hereto as Exhibit A.

3.21 "**Supervisory Authority**" shall have the same meaning as in Regulation (EU) 2016/679 (General Data Protection Regulation).

3.22 "**Technical and Organizational Security Measures**" means measures taken by Vendor and Authorized Persons aimed at (i) ensuring the confidentiality, security, integrity, and availability of Personal Data, including protecting against an Incident, a Personal Data Breach, or other accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access to Personal Data (in particular where Processing involves the transmission of Personal Data over a network) and other unlawful forms of Processing and/or (ii) assisting and enabling AlienVault to comply with its obligations to respond to requests by Data Subjects to exercise their Data Subject Rights.

4. Processing of Data

4.1 Vendor agrees to comply with this Addendum, at no additional cost to AlienVault, at all times during the term of the Agreement. Any failure by Vendor to comply with the obligations set forth in this Addendum, or any Personal Data Breach, will be considered a material breach of the Agreement, and AlienVault will have the right, without limiting any of the rights or remedies under this Addendum or the Agreement, or at law or in equity, to immediately terminate the Agreement for cause. Vendor acknowledges that AlienVault may be the controller of the Personal Data or may be a processor of the Personal Data on behalf of another controller.

4.2 The rights and obligations of the AlienVault with respect to Processing are described herein and in the Agreement. The duration of the Processing shall be for the term of the Agreement, unless earlier terminated. The categories of Data Subject shall include AlienVault end users/customer and AlienVault employees and contractors. The types of Personal Data collected shall include: Individual Name, Employing Company, Phone, Email address, State, Country, Status.

5. AlienVault end-users/customers AND AlienVault employees

5.1 Vendor acknowledges and agrees that it shall only Process Personal Data for the limited and specified purpose of processing Personal Data on behalf of AlienVault solely pursuant to the Agreement and in strict compliance with the terms and conditions set forth in this Addendum and in any Instructions.

5.2 Vendor represents and warrants that its Processing of Personal Data does and will comply with all Applicable Laws.

5.3 To the extent that any Personal Data is transmitted, transferred, shared or otherwise disclosed to Vendor from any Member State, Vendor represents, warrants, and covenants that it shall comply with the Directive and, when effective, the GDPR, with respect to any Processing, including in particular any transfer, of such Personal Data.

6. Security of Data

6.1 At a minimum, and without limiting the foregoing, Vendor represents and warrants that it shall maintain all Personal Data in strict confidence, using a degree of care and Technical and Organizational Security Measures that meet or exceed applicable Industry Standards and that ensure a level of security appropriate to the particular risks of accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access of Personal Data presented by the Processing and the Personal Data (collectively, "**Risks**"), including (i) limiting access to Personal Data to Authorized Persons only; (ii) ensuring that all Authorized Persons are made aware of the confidential nature of Personal Data before they may access such data; (iii) securing its physical, technical, and administrative infrastructure, including all relevant business facilities, data centers, paper files, servers, networks, platforms, databases, cloud computing resources, back-up systems, passwords and credentials, hardware, and mobile devices; (iv) implementing authentication and access controls within all relevant media, applications, networks, operating systems and equipment; (v) encrypting Personal Data at all times and Personal Data when transmitted over public or wireless networks or where otherwise appropriate in light of the Risks; (vi) strictly segregating Personal Data from information of Vendor or its employees or other customers; (vii) maintaining appropriate personnel security and integrity procedures and practices, as set forth in Section 7; (viii) maintaining and regularly testing processes for restoring the availability and access to Personal Data in a timely manner in the event of an Incident or Suspected Incident; (ix) regularly testing, assessing, and evaluating the effectiveness of all Technical and Organizational Security Measures; and (x) any other measures necessary to ensure the ongoing confidentiality, integrity, and availability of Personal Data and the ongoing security and resilience of systems and services used for Processing.

6.2 Upon AlienVault's written request, or, upon the termination or expiration of the Agreement for any reason, Vendor shall, and shall ensure that all Authorized Persons, (i) promptly and securely dispose of or return to AlienVault in an encrypted format, at AlienVault's choice, all copies of Personal Data, including backup or archival copies, and (ii) promptly certify in writing to AlienVault when the measures described in subsection (i) hereof have been completed. Vendor shall, and shall ensure that all Authorized Persons, comply with all Instructions provided by AlienVault with respect to the return or disposal of Personal Data. Any disposal of Personal Data must ensure that such data is rendered permanently unreadable and unrecoverable. Vendor and/or Authorized Persons shall be excused from performing the foregoing obligations only if, and solely to the extent that, Applicable Law(s) explicitly prevent them from doing so.

7. Authorized Persons

7.1 Vendor represents, warrants, and covenants that it has previously informed AlienVault and obtained its prior written consent to any Processing of Personal Data by third parties other than Vendor and its Authorized Employees. Vendor shall promptly send AlienVault a copy of any Authorized Subcontractor agreement relevant to this Addendum.

7.2 Vendor shall perform appropriate screening of all Authorized Persons, including without limitation background checks in accordance with Applicable Laws, and shall ensure the reliability and appropriate training of all Authorized Persons.

7.3 Vendor represents, warrants, and covenants that it has executed written agreements with each Authorized Subcontractor that bind them to all obligations set forth in this Addendum with respect to the Processing of the Personal Data.

7.4 Vendor represents, warrants, and covenants that it has executed confidentiality agreements with each Authorized Person that prevents them from disclosing or otherwise Processing, both during and after their engagement by Vendor, any Personal Data except in accordance with their obligations in connection with the Services.

7.5 Vendor shall be fully responsible for the acts and omissions of Authorized Subcontractors and any other of its subcontractors, independent contractors, and other service providers to the same extent that Vendor would itself be liable under this Addendum had it conducted such acts or omissions, and shall fully indemnify AlienVault for all losses arising from or related to such acts and omissions.

8. Suspected Incident, Incident, and Personal Data Breach Notification

8.1 Vendor shall notify AlienVault of a Personal Data Breach as soon as reasonably practicable, but in any event, not less than seventy-two (72) hours after becoming aware of such Personal Data Breach. If such Personal Data Breach becomes an Incident or a Personal Data Breach, Vendor shall notify AlienVault pursuant to Section 8.2.

8.2 Vendor shall notify AlienVault immediately upon becoming aware of a Personal Data Breach and shall, in a written report, provide sufficient information to enable AlienVault to comply with its obligations under Applicable Laws with respect to such Personal Data Breach,

including any obligation to report or notify such Personal Data Breach to Supervisory Authorities and/or Data Subjects, as applicable. Such report will include (i) a description of the nature of the Personal Data Breach, (ii) the categories and approximate number of Data Subjects and Personal Data sets affected or alleged to be affected, (iii) the likely consequences of the Personal Data Breach, and (iv) any measures that have been or may be taken to address and mitigate the Personal Data Breach.

8.3 As soon as reasonably practicable after providing the report described in Section 8.2, Vendor shall provide AlienVault with a comprehensive report on its initial findings regarding the Personal Data Breach, and thereafter shall provide regular updates describing subsequent findings with respect to such Personal Data Breach. As soon as reasonably practicable after Vendor has concluded its examination of the Personal Data Breach, it shall provide AlienVault with a comprehensive final report regarding the Personal Data Breach.

8.4 Vendor and/or any relevant Authorized Subcontractor shall use its best efforts to immediately mitigate and remedy any Personal Data Breach, and prevent any further Personal Data Breach or recurrence thereof, at Vendor's own expense and in accordance with Applicable Laws.

8.5 Neither Vendor nor any Authorized Subcontractor shall publicly disclose any information regarding any Suspected Incident, Incident or Personal Data Breach without AlienVault's prior written consent, *except that* Vendor and any relevant Authorized Subcontractor may disclose any Personal Data Breach to (i) its own employees, customers, advisors, agents, or contractors, or (ii) where and to the extent explicitly compelled to do so by Applicable Laws, to applicable Supervisory Authorities and/or Data Subjects without AlienVault's prior written consent.

8.6 Vendor and/or any relevant Authorized Subcontractor shall, at Vendor's expense, fully cooperate with AlienVault and provide any assistance necessary for AlienVault to comply with any obligations under Applicable Laws with respect to an Personal Data Breach, including obligations to report or notify an Personal Data Breach to Supervisory Authorities and/or Data Subjects. Such assistance may include drafting disclosures, press releases and/or other communications for AlienVault with respect to such Personal Data Breach.

9. Rights of Data Subjects

9.1 Vendor shall, to the extent permitted by Applicable Laws, provide all necessary assistance to AlienVault in responding to requests by Data Subjects to exercise Data Subject Rights, including, as applicable, a Data Subject's right to: (a) confirm whether his or her Personal Data has been or is being Processed; (b) access a copy of all Personal Data of his or hers that has been or is being Processed; (c) rectify or supplement his or her Personal Data; (d) transfer his or her Personal Data to another AlienVault; (e) confirm that his or her Personal Data has been or is being subject to Processing that constitutes automated decision-making; (f) restrict or cease the Processing of his or her Personal Data; and (g) withdraw consent to the Processing of his or her Personal Data held by Vendor. Such assistance shall also include (x) maintaining records sufficient to demonstrate Vendor's performance of its obligations under Applicable Laws with respect to Data Subject Rights, (y) promptly notifying AlienVault if Vendor or an Authorized Subcontractor receives a request from a Data Subject to exercise a Data Subject Right and refraining from responding to such requests (and ensuring that Authorized Subcontractors refrain from responding to such requests) except upon receipt of, and in accordance with, Instructions from AlienVault, and (z) informing AlienVault in the event that Applicable Laws or any judicial, law enforcement, or Supervisory Authority operate to prevent Vendor (or any Authorized Subcontractor) from performing the obligations described in this Section 9.1, before Vendor (or an Authorized Subcontractor) responds to a request to exercise a Data Subject Right.

10. Transfers of Personal Data

10.1 The Parties hereby acknowledge and agree that the Standard Contractual Clauses shall apply to any Restricted Transfers made in connection with the Services.

10.2 Vendor represents, warrants, and covenants that no Authorized Subcontractor will be permitted to undertake or receive a Restricted Transfer before executing the Standard Contractual Clauses.

10.3 Vendor represents and warrants that every Restricted Transfer made by Vendor or any Authorized Subcontractor shall be undertaken in accordance with the Standard Contractual Clauses.

10.4 If Vendor is Privacy Shield certified, Vendor represents, warrants, and covenants that every transfer of Personal Data by Vendor from the European Economic Area or Switzerland to the United States shall be made pursuant to the Privacy Shield Framework and Principles, and further represents and warrants that it self-certifies to, and complies with, the Privacy Shield Framework and Principles, and shall maintain such self-certification and compliance for the duration of the Agreement.

11. Actions and Access Requests

11.1 Upon AlienVault's request, Vendor shall make available to AlienVault all information available to Vendor and to Authorized Subcontractors that AlienVault reasonably deems necessary to demonstrate compliance by AlienVault with its obligations under Applicable Laws (including in particular the GDPR, when effective) relating to the Personal Data and the Processing conducted by Vendor and Authorized Subcontractors.

11.2 Upon AlienVault's request, Vendor shall provide all necessary assistance to AlienVault in connection with any data protection impact assessments ("**DPIA(s)**") that AlienVault determines (in its sole discretion) it must conduct or cause to be conducted in order to comply with Applicable Laws, to the extent that such DPIA(s) relate to the Processing.

11.2.1 Upon AlienVault's request, AlienVault shall provide all necessary assistance to AlienVault in connection with any consultation with a Supervisory Authority that AlienVault determines (in its sole discretion) it must undertake as a result of a DPIA, to the extent that such DPIA relates to the Processing.

11.3 Upon AlienVault's request, Vendor shall provide all necessary assistance to AlienVault in the event of any investigation, action, or request made by a Supervisory Authority, to the extent that such investigation, action, or request relates to the Personal Data or the Processing.

11.4 Upon AlienVault's request, Vendor shall provide AlienVault, and any Supervisory Authority with whom AlienVault is consulting or cooperating, with a designated contact for all queries and requests relating to the Processing of Personal Data.

11.5 Upon AlienVault's request, Vendor shall provide all necessary assistance to AlienVault in connection with any certification or re-certification efforts by AlienVault with respect to the EU-US Privacy Shield Framework.

11.6 In the event Vendor determines that any Processing violates Applicable Laws (including the valid exercise of a Data Subject Right) or this Addendum, it shall immediately inform AlienVault and follow Instructions for stopping such Processing and/or remediating the violation.

11.7 Without limiting the foregoing, in the event of a change in Applicable Laws affecting this Addendum, Vendor agrees to work in good faith with AlienVault to make any amendments to this Addendum pursuant to Section 14.2, and further agrees to make any changes to its Technical and Organizational Security Measures as are reasonably necessary to ensure continued compliance with Applicable Laws.

12. Audit Rights

12.1 Vendor shall use external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed by independent third-party security professionals at Vendor's selection and expense; and (c) will result in the generation of an audit report ("**Report**"), which will be Vendor's Confidential Information. Vendor shall maintain complete and accurate records in connection with Vendor's performance under this Addendum, and shall retain such records for a period of three (3) years after the termination or expiration of the Agreement.

12.2 At AlienVault's written request, Vendor will provide AlienVault with a confidential Report so that AlienVault can reasonably verify Vendor's compliance with the security obligations under this Addendum.

13. Indemnity

13.1 Vendor shall, at its own expense, protect, defend, indemnify and hold harmless AlienVault and its officers, directors, employees, successors, assigns, distributors, contractors, agents, affiliates and customers, from all claims or actions, damages, liabilities, assessments, losses, costs, and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses and breach notification expenses) arising out of or resulting from (a) any breach by Vendor of its warranties or representations in this Addendum, (b) any acts and omissions of any Authorized Subcontractors with respect to the Processing of any Personal Data; or (c) any Incident or Personal Data Breach (collectively, "**Claims**").

13.2 AlienVault shall provide Vendor with prompt written notice of any Claim. Upon receipt of any such notice, Vendor must immediately take all necessary and appropriate action to protect AlienVault's interests with regard to any Claims. AlienVault shall provide reasonable cooperation, information, and assistance in connection with any Claim (except that failure to do so shall only excuse Vendor from its obligations to the extent such failure materially prejudiced the defense of the Claim). Vendor shall have sole control and authority to defend, settle or compromise any Claim, provided that Vendor shall not make any settlement that requires a materially adverse act or admission by AlienVault without AlienVault's written consent (such consent not to be unreasonably delayed, conditioned or withheld). If Vendor provides counsel for the defense of any Claim and AlienVault, in its sole discretion, determines that such counsel is unacceptable or that a conflict of interest exists between AlienVault and such counsel, AlienVault may request Vendor replace the counsel. If Vendor fails to timely replace counsel, the Vendor agrees that its counsel shall work in good faith with AlienVault's counsel until the Claim is resolved.

14. Miscellaneous

14.1 This Addendum and the Standard Contractual Clauses will terminate simultaneously and automatically with the termination of the Agreement, except that all provisions intending to survive shall survive, including specifically, Sections 4, 6.2, 7.5, 8, 11.3, 11.4, 12.1, 12.2, 13, 14.

14.2 This Addendum may be amended or modified only by a writing signed by both Parties. Vendor acknowledges and agrees that the AlienVault (whether it is acting as a controller or a processor on behalf of another controller) may disclose this Addendum to third parties (including other controllers, data subjects and regulators) for purposes of demonstrating compliance with Applicable Laws.

14.3 The Parties hereby acknowledge and agree that any remedies arising from any Personal Data Breach or any breach by Vendor or any Authorized Person of the terms of this Addendum are not and shall not be subject to any limitation of liability provision that applies to Vendor under the Agreement.

14.4 This Addendum shall be governed by the law of the same jurisdiction as the Agreement, except where and to the extent that Applicable Laws require that the Addendum be governed by the law of another jurisdiction.

REMAINDER OF ADDENDUM IS LEFT INTENTIONALLY BLANK

EXHIBIT A
Standard Contractual Clauses

For the purposes of GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: AlienVault, Inc. ("data exporter")

Name of the data importing organisation: Vendor identified in Addendum ("data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Regulation (EU) 2016/679 ("General Data Protection Regulation or GDPR");

(b) '*the data exporter'* means AlienVault and any AlienVault Affiliate;

(c) *'the data importer'* means Vendor and any Vendor Affiliate;

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the

required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature page on page 1 of the Addendum, the parties will be deemed to have signed this Appendix 1.

Data exporter
The data exporter is AlienVault, Inc.
……
……

Data importer
The data importer is the Vendor identified in the Addendum.
……
……

Data subjects
The personal data transferred concern the following categories of data subjects (please specify): AlienVault end users/customer and AlienVault employees and contractors.
……
……

Categories of data
The personal data transferred concern the following categories of data (please specify): Individual Name, Employing Company, Phone, Email address, State, Country, Status.
……
……

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify): Not applicable.

……
……

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify): Compute, storage and content delivery on the AlienVault application.
……
……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the signature page on page 1 of the Addendum, the parties will be deemed to have signed this Appendix 2.

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

Vendor shall maintain administrative, physical and technical safeguards for the protection of security, confidentiality, and integrity of Customer Data. Vendor will not materially decrease the overall security of the Service during a subscription term.