Tripwire, Inc.
DATA PROCESSING ADDENDUM
Last updated April 2021

This Data Processing Addendum, including its exhibits, ("**DPA**") is incorporated by reference into the master subscription agreement or other negotiated or electronic agreement between Tripwire, Inc. ("**Tripwire**") and the customer identified in the Agreement ("**Customer**") for Tripwire Products and/or Services (the "**Agreement**").

This DPA supplements the Agreement and sets out the terms that apply when Personal Data is Processed by or for Tripwire under the Agreement, to ensure that the Processing is done in accordance with Applicable Data Protection Law, and with due respect for the rights and freedoms of individuals whose Personal Data is Processed (as these terms are defined below). Capitalized terms used but not defined in this DPA have the same meanings as in the Agreement.

HOW TO EFFECT THIS DPA:

This DPA includes the main body, Exhibit 1 (Information Security Standards), Exhibit 2 (Standard Contractual Clauses), and Appendices 1 and 1 to Exhibit 2. For Customer purchases under a Tripwire SaaS Subscription Agreement, this DPA will become a legally binding addendum to the Agreement for the duration of the Subscription Term. For a Customer purchase under the Tripwire ExpertOps Service Agreement, this DPA will become a legally binding addendum to the Agreement for the duration of the Term. For any other purchases, this DPA will become a legally binding addendum to the Agreement when the DPA is fully executed. To complete this DPA, Customer must do all of the following:

1. Complete the information in the signature box and have an authorized representative sign on page 5.
2. Complete the information as the data exporter on page 9.
3. Complete the information in the signature boxes and have an authorized representative sign on pages 13, 14 and 15.
4. Return a complete scanned copy of the signed DPA to Tripwire via email to TW-Contracts@tripwire.com

If you would prefer to receive an electronic copy for electronic signature, please send your request to TW-Contracts@tripwire.com and we will send you this DPA for signature via DocuSign.

HOW THIS DPA APPLIES:

A. If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.
B. If the Customer entity signing this DPA has executed an order with Tripwire pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that order and applicable renewal orders.
C. If the Customer entity signing this DPA is lawfully permitting an Affiliate to order under the Agreement, that Affiliate is a party to this DPA.
D. If the Customer entity signing this DPA is not an Affiliate and is neither a party to an order nor to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement execute this DPA.

Customer may terminate this DPA, including the Standard Contractual Clauses, at any time by written notice to Tripwire.

DATA PROCESSING TERMS:

Sections preceded by an asterisk (*) apply only to the extent that Customer is established within the EEA, or Tripwire Processes Personal Data of Data Subjects located in the EEA on behalf of Customer or a Customer Affiliate (as such terms are defined below).

1. Definitions

1.1 ***"Controller"**, "**Processor**", "**Data Subject**", and "**Special Categories of Data**" shall have the meanings given in Applicable Data Protection Law;

1.2 "**Applicable Data Protection Law**" means, as applicable to the Personal Data that may be included in Customer Data and Administrative Data: (a) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General

Data Protection Regulation); (b) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the protection of privacy in electronic communications sector (as amended or replaced from time to time) and applicable laws implementing that directive in European Union Member States; and (c) the applicable data protection laws of Switzerland and the United Kingdom;

1.3 "**Authorized Persons**" means any person authorized by Tripwire to Process Personal Data (including Tripwire's staff, agents and subcontractors);

1.4 "**Data Privacy Contact**" means the email address identified below each Party's signature below, or such updated address as a Party may notify to the other Party's Data Privacy Contact.

1.5 "**EEA**" means the European Economic Area, which constitutes the member state of the European Union, Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, Switzerland and the United Kingdom.

1.6 "**Information Security Standards**" means the information security standards described in Exhibit 1;

1.7 "**Personal Data**" means any information relating to (a) an identified or identifiable natural person and, (b) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under Applicable Data Protection Law), where for each (a) or (b), such data is Customer Data.

1.8 "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9 "**Security Incident**" means the unauthorized, accidental or unlawful access to or Processing of Personal Data.

2. Roles and Responsibilities

2.1 ***Relationship of the parties**. Customer, as Controller, appoints Tripwire as a Processor to Process Personal Data on behalf of Customer for the purpose of providing the Products and/or Services. In some circumstances, Customer may be a Processor with respect to the Personal Data, in which case Customer appoints Tripwire as Customer's sub-processor, which shall not change the obligations of Customer or Tripwire under this DPA. In some circumstances, Customer may appoint Tripwire as a Controller to Process Personal Data for the purposes of providing the Products and/or Services, which shall not change the obligations of Customer or Tripwire under this DPA.

2.2 **Purpose limitation.** Tripwire shall Process the Personal Data for the purposes set forth in the Agreement and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law (the "**Permitted Purpose**"). This DPA and the Agreement set out Customer's complete instructions to Tripwire in relation to Processing of Personal Data. Any Processing of Personal Data required outside of the scope of these instructions will require prior written agreement of the Parties.

2.3 **Training**. Tripwire shall ensure that its Authorized Persons receive appropriate training regarding their responsibilities and obligations with respect to the Processing, protection and confidentiality of Personal Data.

2.4 ***Compliance**. Tripwire, as Processor or Controller, will comply with Applicable Data Protection Law. Customer, as Controller, is responsible for ensuring that, in connection with the Products or Services and Customer Data, it complies with Applicable Data Protection Law and has the right to transfer or provide access to the Personal Data to Tripwire for Processing in accordance with the terms of the Agreement and this DPA.

3. Security

3.1 **Security.** Tripwire shall implement and maintain appropriate technical and organizational measures, no less stringent than the Information Security Standards, to protect the Personal Data from Security Incidents. Such measures shall have regard to 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 Data Subjects.

3.2 **Processing Confidentiality**. Tripwire shall ensure that each Authorized Person shall be subject to a duty of confidentiality that shall survive the termination of their employment or contractual relationship.

3.3 **Security Incidents**. When it becomes aware of a Security Incident, Tripwire shall inform the Customer Data Privacy Contact immediately (and in any event within 72 hours) and shall provide such timely information and cooperation as Customer may reasonably require to enable Customer to fulfil its data breach reporting obligations under Applicable Data Protection Law. Tripwire shall further take all measures and actions as are reasonably necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer up to date of all developments in connection with the Security Incident.

4. *Sub-Processing

4.1 **Sub-Processors.** Customer agrees that Tripwire may engage Tripwire Affiliates and third-party sub-processors (collectively, "**Sub-Processors**") to Process Personal Data on Tripwire's behalf in connection with the provision of the Products and Services. The list of Sub-Processors currently engaged by Tripwire and authorized by Customer ("**Sub-Processor List**") is available at www.tripwire.com/terms/ or by email request to the Tripwire Data Privacy Contact. Customer may request to receive notifications of updates to the Sub-Processor List by sending a request to the Tripwire Data Privacy Contact. Tripwire shall impose on such Sub-Processors data protection terms that protect the Personal Data to the same standard provided for in the Agreement and this DPA, to the extent applicable to the nature of the services provided by such Sub-Processor. Tripwire shall remain liable for any breach of the Agreement or this DPA caused by a Sub-Processor.

4.2 **Changes to Sub-Processors**. Customer may reasonably object to Tripwire's use of a new Sub-Processor (e.g., if making Personal Data available to the Sub-Processor may violate Applicable Data Protection Law or weaken the protections for such Personal Data) by notifying the Tripwire Data Privacy Contact within ten (10) business days after receipt of Tripwire's notice in accordance with the notification mechanism described in Section 4.1 above. Such notice must explain the reasonable grounds for the objection. If Customer objects to a new Sub-Processor as permitted in this Section 4.2, Tripwire will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening Customer. If Tripwire is unable to make available such change within a reasonable period of time (not exceeding thirty (30) days), Customer may terminate without penalty the Agreement with respect only to those Services that cannot be provided by Tripwire without the use of the objected-to new Sub-Processor by providing written notice to the Tripwire Data Privacy Contact. Tripwire will refund any fees that were prepaid to Tripwire covering the remainder of the term of such Agreement following the effective date of termination with respect to the terminated Services.

4.3 **Emergency Replacement.** Tripwire may replace a Sub-Processor if the need for the change is urgent and necessary to provide the Services and the reason for the change is beyond Tripwire's reasonable control. In such instance, Tripwire shall notify Customer of the replacement as soon as reasonably practicable and without undue delay, and Customer shall retain the right to object to the replacement Sub-Processor pursuant to Section 4.2 above.

5. *Cooperation and Data Subjects' Rights

5.1 **Cooperation.** Tripwire shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer to enable Customer to respond to: (a) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Personal Data. Customer requests under this Section 5.1 must be made to the Tripwire Data Privacy Contact. If any

such request, correspondence, inquiry or complaint is made directly to Tripwire, Tripwire shall promptly (and in any event within five business days) inform the Customer Data Privacy Contact, providing full details of the request, correspondence, enquiry or complaint.

5.2 **Data Protection Impact Assessment.** Tripwire shall, to the extent required by Applicable Data Protection Law, provide Customer with reasonable assistance with data protection impact assessments and/or prior consultations with supervisory authorities that Customer is required to carry out under Applicable Data Protection Law.

6. Retention, Deletion or Return of Personal Data and Customer Data.

6.1 **Retention Period**. Retention periods for Customer Data is specific to the Service purchased. Customer can find default retention periods and instructions on how to change the retention period in the Documentation.

6.2 **Deletion of Personal Data.** On expiration of the retention period, termination of Customer's Agreement, or earlier on Customer's request to Tripwire's Data Privacy Contact, Tripwire shall (at Customer's election) promptly destroy or return to Customer all Personal Data in its possession or control, including any Personal Data subcontracted to a third party for Processing. This requirement shall not apply to the extent that Tripwire is required by law to retain some or all of the Personal Data, in which event Tripwire shall isolate and protect the Personal Data from any further Processing except to the extent required by such law.

7. Security Reports and Audits. At Customer's request to the Tripwire Data Privacy Contact, Tripwire shall provide a copy of its most current available SOC2 audit report, if any, subject to the confidentiality terms of the Agreement. At Customer's request to the Tripwire Data Privacy Contact, Tripwire shall allow Customer (or Customer's independent third party auditor) to conduct an on-site audit of the procedures relevant to the protection of Personal Data, subject to the confidentiality provisions of the Agreement. Customer and Tripwire will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit. Tripwire reserves the right to charge a fee (based on Tripwire's reasonable costs) for any such audit, and Tripwire will provide further details of any applicable fee and the basis of its calculation to Customer in advance of such audit. Tripwire will also cooperate with any audit if and when required by instruction of a competent data protection authority under Applicable Data Protection Law, without fee.

8. *Transfer Mechanism for International Data Transfers

8.1 *Standard Contractual Clauses. During the term of the Agreement, to the extent there are any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories,, the provisions of the Standard Contractual Clauses in Exhibit 2 shall apply. In such case:

(a) The terms "data importer" means Tripwire, "data exporter" means Customer and its Affiliates.

(b) For the purposes of Clause 5(a) of Exhibit 2, the following are deemed to be Customer's instructions to process Personal Data: (i) Processing accordance with the Agreement; (ii) Processing initiated by Users in their use of the Services; (iii) Processing to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) where such instructions are consistent with the terms of the Agreement.

(c) Pursuant to Clauses 5(h) and 11 of Exhibit 2, Customer acknowledges and expressly agrees that (i) Tripwire may engage Sub-Processors in connection with the provision of the Services under the terms in Sections 4 and 8.2 of this DPA; (ii) Tripwire will provide the current list of Sub-Processors as described in Section 4.1 of this DPA; and (iii) Tripwire may engage new Sub-Processors as described in Sections 4.2 and 4.3 of this DPA.

(d) Copies of Sub-Processor agreements that must be provided by Tripwire to Customer pursuant to Clause 5(j) of Exhibit 2 may have all commercial information and clauses unrelated to the requirements of Exhibit 2 removed or redacted, and that such copies will be provided only on Customer's request.

(e) The audits described in Clauses 5(f) and 12(2) of Exhibit 2 shall be carried out in accordance with Section 7 of this DPA.

8.2 ***Sub-Processors**. To the extent that Tripwire permits a Sub-Processor to Process Personal Data that originated in the EEA, Tripwire shall impose on such Sub-Processors data protection terms that protect the Personal Data to the same standard provided for by the Agreement, this DPA and the Applicable Data Protection Law. Without limiting the foregoing, Tripwire shall ensure that transfers of such EEA-origin Personal Data shall be transferred under a European Commission approved method of ensuring an adequate level of protection, such as under approved binding corporate rules or under signed standard contractual clauses.

9. Liability. Each party's liability, taken together in the aggregate, arising out of or related to this DPA whether in contract, tort or under any theory of liability, is subject to the "Limitation of Liability' sections of the Agreement. Any reference in such section to the liability of a party means the aggregate liability of that party under the Agreement and this DPA together.

10. General Terms. In relation to the Processing of Personal Data by Tripwire, to the extent there is any conflict or inconsistency between this DPA and the Agreement or any other terms, agreements or contracts between the Parties, the terms of this DPA shall prevail. The provisions of this DPA will enure to the benefit of and will be binding upon the Parties and their respective successors and assigns. The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this DPA will remain in full force and effect. Any notice, letter or other communication contemplated by this DPA will be communicated by email to the respective Data Privacy Contacts. This Agreement may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. This Agreement will be governed by and construed in accordance with the governing law identified in the Agreement, except to the extent that Applicable Data Protection Law requires otherwise, in which event this DPA will be governed in accordance with Applicable Data Protection Law.

TRIPWIRE, INC.		**CUSTOMER:**	
By:	_____	By:	_____
Printed Name:	_____	Printed Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date	_____
Tripwire Data Privacy Contact:		**Customer Data Privacy Contact:**	
Email:	privacy@tripwire.com	Email:	_____

Exhibit 1

Information Security Standards

These Information Security Standards supplement but do not replace any security requirements set forth in the Agreement. In the event of a conflict between this Exhibit 1 and the security requirements in the Agreement, the requirement requiring the greater protection for the data shall prevail.

Tripwire will implement and maintain a comprehensive information security policy mandatory for all Tripwire employees and applicable contractors that is reviewed and tested at least annually and updated as necessary. At a minimum, the information security policy must meet the security standards identified below. In addition, Tripwire will conduct annual risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of systems used by Tripwire to process Personal Data. If any audits reveal material vulnerabilities, Tripwire shall promptly correct each vulnerability at Tripwire's sole cost and expense.

1. **Physical access control**

   Technical and organizational measures to prevent unauthorized access to data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data is processed, including:

   - Physical entry controls and management: barriers, door locking, badge-controlled entry points (ID reader, magnetic card, chip card), surveillance (video/CCTV monitor, alarm system) and manned reception desks.
   - Access authorization policy for employees and third parties
     - use of an access badge will be logged
     - access will be limited by job role and subject to authorized approval
     - any guest authorized to enter the premises will be registered, provide proof of identity upon registration, and will be escorted by authorized personnel
     - access is revoked upon a) separation of an authorized employee or b) the authorized employee no longer has a valid business need for access

2. **System access control**

   Technical and organizational measures to prevent data processing systems from being used by unauthorized persons including:

   - User access control:
     - identification and authentication procedures
     - access is restricted to minimum access required for employee to complete work responsibilities
     - access is reviewed on a regular basis
     - documented authorization process and logging of privileged access
     - employee termination procedures
   - Comprehensive ID/password security procedures
     - special characters, minimum length, reset procedure
     - automatic blocking and monitoring of the user ID upon multiple erroneous passwords attempts

3. **Data access control**

   Technical and organizational measures to ensure that employees authorized to access Customer Data gain access only to such Customer Data in accordance with their access rights, and that Customer Data cannot be read, copied, modified or deleted without authorization, including:

   - Documented policies, procedures and training regarding access, use, change and deletion of Customer Data
   - Differentiated access rights (profiles, roles, transactions and objects)
   - Monitoring and logging of access, and retention of logs

- Maintaining reports of access
- Maintaining a security awareness program to train personnel about their security obligations, including training about data classification obligations, physical security controls, security practices, and Security Incident reporting
- Taking disciplinary action against employees who access Customer Data without authorization

4. Disclosure control

Technical and organizational measures to ensure that Customer Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage (in physical or electronic form), and that the recipient of the Customer Data can be identified, including:

- Encryption requirements:
  - Encrypt all Customer Data transmitted in connection with the Services by the use of the then-current TLS cryptographic protocol or a stronger cryptographic protocol.
  - Encrypt all Customer Data while at rest by the use of AES-256 or a stronger cryptographic protocol.
- Logging:
  - Maintain electronic records of transfers and Processing as required by Applicable Data Protection Law
- Secure destruction of media that may have contained Customer Data after the media is removed from service

5. Control of subcontractors

Technical and organizational measures to ensure that any Customer Data processed by permitted subcontractors is processed solely in accordance with Tripwire instructions, including:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Security review of the subcontractor.

6. Availability control

Technical and organizational measures to ensure that Customer Data is protected against accidental destruction or loss (physical/logical), including:

- Backup procedures:
  - Daily backups performed
  - Georedundant backups separate from production systems
  - Data restoration testing process implemented and maintained
- Uninterruptible power supply (UPS)
- Remote storage
- Use of current anti-virus/firewall systems;
- Disaster recovery plan.
- Patch Management:
  - Implement and maintain a process to assess, test, and apply security advisory patches to applicable systems.
  - Implement patches pursuant to documented severity and risk assessment guidelines
- Vulnerability Assessments:
  - Automated management and routine verification of systems' compliance with security configuration requirements
  - Remediate identified vulnerabilities or noncompliance with security configuration requirements based on associated risk, exploitability, and impact.
  - Maintain policies and procedures to manage risks associated with the application of changes to systems.

7. Separation control

Technical and organizational measures to ensure that Customer Data collected for different purposes can be processed separately, including:

- Logical separation of Customer Data to prevent unauthorized access or exposure
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

8. Security incident response

Technical and organizational measures to address, respond to and remediate Security Incidents, including:

- Maintaining and following documented incident response policies consistent with NIST guidelines for computer security incident handling and in compliance with applicable data breach notification requirements
- Notifying the Customer Data Privacy Contact promptly (and in no event later than 72 hours) of a suspected Security Incident, including providing Customer with reasonably requested information about the Security Incident and status of any remediation and restoration activities
- Fully cooperating with Customer in investigating the Security Incident and in providing information to governmental or regulatory authorities or notices regarding the Security Incident that Customer deems appropriate
- Taking all reasonable actions necessary or requested by Customer to remediate and mitigate the effects and to minimize any damage resulting from the Security Incident (including taking all commercially reasonable steps to enforce against any person that is or may be engaging in activities relating to the Security Incident any rights Tripwire has to require such person to cease such activities relating to the Security Incident)
- Performing post-Security Incident reviews of events and actions taken, if any, and, without derogating from its obligations hereunder, making any required changes in its practices relating to protection of Customer Data or Tripwire systems, including upgrading information safeguards as necessary to limit risks
- Maintaining written records of every Security Incident (including in accordance with any requirements prescribed Applicable Data Protection Laws) and the responsive actions taken in connection with the Security Incident and, on Customer's request and permitting such records to be disclosed to governmental and regulatory authorities
- Testing and reviewing the Security Incident response plan at least annually

Exhibit 2

Standard Contractual Clauses (processors) (if required under Section 8.1(b) of the Agreement)

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

Name of the data exporting organization: _____

Address: _____

Tel: _____ Fax: _____

Email: _____

Other information needed to identify the organisaton: _____

(the data **exporter**), and

Name of the data importing organisation: Tripwire, Inc.

Current Address: 308 SW Second Ave, Suite 400, Portland, Oregon 97204-3413

Tel: 503-276-7500 Fax: 503-223-0182 Email: privacy@tripwire.com

Other information needed to identify the organisation: _____

(the data **importer**)

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

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer[2]

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;

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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[3]. 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 Netherlands.
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.

---

[3] 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.

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.

On behalf of the data exporter (Company):

Name (written out in full):

Position:

Address:

On behalf of the data importer (Tripwire):

Name (written out in full): Andrea Flanagan

Position: Senior Director of Legal Services

Address: 308 SW 2nd Ave., Suite 400
Portland, Oregon 97204-3413

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

Signature:

Signature:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Data exporter
The data exporter is the legal entity that has executed these Clauses as a data exporter and all Affiliates (as defined in the DPA to which these Clauses are attached) of the data exporter on whose behalf data importer processes personal data of data subjects located in the European Economic Area, Switzerland or the United Kingdom.

Data importer
The data importer is a provider of cybersecurity products, managed services, and SaaS (the "Services") which may involve processing personal data provided by, and pursuant to the insturctions and directions of, the data exporter in accordance with the terms of athe DPA and services agremment, and all related orders between data exporter and data importer (the "Agreement").

Data subjects
The categories of data subjects whose personal data may be processed in connection with the Services are determined and controlled by the data exporter in its sole discretion and may include but are not limited to: employees and contractors of the data exporter, and employees and contractors of the data exporters customers, suppliers and partners.

Categories of data
The categories of personal data may include but are not limited to:

- Business contact information, including name, business role, professional title, business contact information (address, phone number, fax number, email address);
- Electronic identification and access credentials for business-managed assets, including IP address, user name, password;
- Log data, configuration data and diagnostic output of business-managed assets; and
- Other categories of personal data determined by the data exporter in its sole discretion.

Special categories of data
The Parties do not intend that special categories of data shall be processed under the Agreement.

Processing operations
Data importer will process personal data as necessary to perform the Services pursuant to the Agreement and to comply with the Applicable Data Protection Law and other laws to which the data exporter and data importer may be subject. Such processing operations may include collecting, recording, organizing, storage, use, alteration, disclosure, transmission, combining, tretireval, consultation, archiving and/or destruction.

Processing may be performed in the European Economic Area, Switzerland, United Kingdom, United States, and such other countries where data importer Affiliates or Sub-Processors are located, in accordance with these Clauses and the Agreement.

DATA EXPORTER _____

Authorised Signature _____

Printed Name: _____

DATA IMPORTER **Tripwire, Inc.**

Authorised Signature _____

Printed Name: Andrea Flanagan

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

Data importer will, as a minimum, implement the security measures described in Exhibit 1 to the DPA to which these Clauses are attached.

DATA EXPORTER	
Authorised Signature	
Printed Name:	
DATA IMPORTER	**Tripwire, Inc.**
Authorised Signature	
Printed Name:	Andrea Flanagan