Data Processing Agreement with Standard Contractual Clauses

Last modified: October 5, 2020

This Data Protection Agreement with Standard Contractual Clauses ("**DPA**") forms part of the PerimeterX Subscription Agreement or other written or electronic agreement that expressly references this DPA ("**Agreement**") between PerimeterX, Inc. ("**PerimeterX**") and Subscriber for the purchase of website security and monitoring services ("**Services**") identified in an ordering document Subscriber has signed with PerimeterX ("**Order Form**"). By signing the Order Form, Subscriber enters into this DPA on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent PerimeterX processes Personal Data for that Authorized Affiliate. For the purposes of this DPA only, and except where indicated otherwise, the term "Subscriber" shall include Subscriber and Authorized Affiliates. All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. **Definitions**.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity where "control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Subscriber's Affiliate(s) that is permitted to use the Services pursuant to the Agreement between Subscriber and PerimeterX but has not signed its own Order Form with PerimeterX.

"**CCPA**" means California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, et. seq. and its implementing regulations.

"**Controller**" means the entity which determines the purposes and means of the processing of Personal Data.

"**Data Privacy Laws**" means applicable national, federal, state and provincial laws relating to data privacy, the protection of Personal Data, and the cross-border transfer of Personal Data (e.g., to the extent applicable, the CCPA and GDPR), excluding any law that requires data to be stored in a specific country.

"**Data Subject Request**" means a request from a data subject to exercise the data subject's right under applicable Data Privacy Laws, including, as applicable, rights to data rectification, data portability, access data, data erasure ("the right to be forgotten"), not to be subject to automated decision making, right not to have Personal Data sold, to request for information, not to be discriminated against for exercising rights, restriction or objection to processing, and the applicable rights under CCPA §§ 1798.100(d), 1798.105, 1798.110, 1798.120, 1798.130(a)(2), 1798.140(y), 1798.145(g) and GDPR Art. 12-23.

"**GDPR**" means the General Data Protection Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

“**Personal Data**” means (i) any information relating to an identified or identifiable natural person where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier or (ii) is defined as “Personal Information” or “Personal Data” by applicable Data Privacy Laws (e.g., CCPA § 1798.140(o) or GDPR Art. 4).

"**Process**" and its cognates means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which processes Personal Data on behalf of the Controller, including, as applicable, any "service provider" as that term is defined by the CCPA.

“**Subprocessor**” means any Processor engaged by PerimeterX to process Subscriber’s Personal Data.

“**Subscriber**” means “Customer” or “Subscriber” as defined in the Order Form.

“**Supervisory Authority**” means an independent public authority which is (i) established by a European Union member state pursuant to Article 51 of the GDPR; or (ii) the public authority governing data protection, which has authority and jurisdiction over Subscriber.

2. **Processing of Data**. PerimeterX will only process Subscriber Personal Data (i) in compliance with the instructions received from Subscriber and (ii) for the purposes expressly set forth in the Agreement, including providing, supporting and improving the Services. PerimeterX will not use or process the Subscriber Personal Data for any other purpose. PerimeterX will promptly inform Subscriber in writing if it cannot comply with the requirements of this DPA, in which case Subscriber may terminate the Agreement or take any other reasonable action, including suspending data processing operations.

3. **Compliance with Law; Duty to Inform**. PerimeterX will comply with all applicable Data Privacy Laws, including, as applicable, the CCPA and the GDPR. PerimeterX will promptly inform Subscriber if, in its opinion, a processing instruction from Subscriber violates Data Privacy Laws.

4. **No Sale of Personal Information**. PerimeterX will not “sell” any “personal information” as defined under the CCPA (§ 1798.140(d)).

5. **Roles of the Parties**. The parties agree that with respect to processing Personal Data that Subscriber is the Controller and PerimeterX is the Processor.

6. **Confidentiality**. All PerimeterX personnel and any Subprocessors are required to comply with the confidentiality obligations related to Subscriber Personal Data, including after the end of their respective employment, contract or assignment.

7. **Standard Contractual Clauses**. To the extent any Personal Data of European Economic Area (“**EEA**”) or United Kingdom (“**UK**”), or Swiss data subjects is processed, the EU Controller-to-Processor standard contractual clauses (“**SCC**”) in Exhibit A of this DPA apply, provided that for Swiss data subjects the SCC extends protection to the Personal Data of legal entities and personality profiles. For the avoidance of doubt, with respect to transfers of EEA, UK and Swiss Personal Data for processing by PerimeterX in a jurisdiction other than an EU member state,

PerimeterX agrees to comply with applicable Data Privacy Laws in connection with that cross-border transfer of data (e.g., Art. 46 of the GDPR).

8. **Data Subject Requests**. PerimeterX will, to the extent legally permitted, promptly notify Subscriber if PerimeterX receives a Data Subject Request relating to a data subject's Personal Data that is being processed for Subscriber. On request, PerimeterX will provide all necessary assistance and cooperation, materials and/or documentation as may be necessary for Subscriber to comply with its obligations under the Data Privacy Laws in connection with all Data Subject Requests.

9. **Notice of Investigation, Complaint or Subpoena**. PerimeterX will promptly inform Subscriber if it (a) receives any notice or inquiry from a Supervisory Authority relating to the processing of Subscriber Personal Data, (b) any complaint by a data subject regarding the processing of Subscriber Personal Data, and (c) any legally binding request for disclosure of Subscriber Personal Data by a law enforcement authority unless PerimeterX is prohibited by applicable law to inform Subscriber.

10. **Cooperation**. On request, PerimeterX will provide Subscriber with a summary of its security and privacy polices. On request, PerimeterX will cooperate with the Supervisory Authority and promptly provide Subscriber with all information in PerimeterX's possession or control in relation to the processing of the Personal Data under this Agreement.

11. **Data Breach**. PerimeterX will notify Subscriber within twenty-four (24) hours after discovery of any unauthorized disclosure of or access to Personal Data while in the possession or control of PerimeterX or its Subprocessors ("**Security Incident**"). PerimeterX will promptly provide Subscriber with all information in its possession or control in relation to any Security Incident, including a description of the nature of the Security Incident; the categories and approximate number of data subjects concerned and the records of Personal Data affected; the name and contact details of PerimeterX's point of contact from whom further information can be obtained; a description of the consequences of the Security Incident and the measures taken or proposed to be taken by PerimeterX to address the Security Incident; and with all reasonable assistance and cooperation as is necessary in order for the Subscriber to seek to mitigate the effects of the Security Incident and comply with its own obligations under the Data Privacy Laws with respect to the Security Incident. Except as may be required by applicable law, PerimeterX will not make any public announcement or notify any data subject about the Security Incident unless expressly authorized by Subscriber.

12. **Subprocessors**. If PerimeterX intends to engage Subprocessors, PerimeterX will (i) remain liable to Subscriber for the Subprocessors' acts and omissions with regard to their processing; (ii) exclusive of the list of Subprocessors PerimeterX maintains online (currently available at http://www.perimeterx.com/legal/subprocessors), obtain the prior written consent of Subscriber to such subcontracting, such consent to not be unreasonably withheld; and (iii) enter into contractual arrangements with such Subprocessors binding them to provide a similar level of data protection provided for in this DPA. Further, PerimeterX will comply with Data Privacy Laws when engaging a Subprocessor (e.g., GDPR Art. 28(2) and 28(4)).

13. **DPIA and Consultations**. Upon request, PerimeterX will provide Subscriber with assistance in the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

14. **Audits**.

(A) Supervisory Authority Audit. If a Supervisory Authority requires an audit of the data processing facilities from which PerimeterX processes Subscriber Personal Data in order to ascertain or monitor

Subscriber's compliance with Data Privacy Laws, PerimeterX will cooperate with such audit. Subscriber is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time PerimeterX expends for any such audit, in addition to the rates for services performed by PerimeterX.

(B) Subscriber Audits. On request, PerimeterX will provide to Subscriber each year an opinion or Service Organization Control report provided by an accredited, third-party audit firm under the Statement on Standards for Attestation Engagements (SSAE) No. 18 ("**SSAE 18**") (Reporting on Controls at a Service Organization) or the International Standard on Assurance Engagements (ISAE) 3402 ("**ISAE 3402**") (Assurance Reports on Controls at a Service Organization) standards applicable to the services under the Agreement (each such report, a "**Report**"). If a Report does not provide, in Subscriber's reasonable judgment, sufficient information to confirm PerimeterX's compliance with the terms of this DPA, then Subscriber or an accredited third-party audit firm agreed to by both Subscriber and PerimeterX may audit PerimeterX's compliance with the terms of this DPA during regular business hours, with reasonable advance notice to PerimeterX and subject to reasonable confidentiality procedures. Subscriber is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time PerimeterX expends for any such audit, in addition to the rates for services performed by PerimeterX. Before the commencement of any such audit, Subscriber and PerimeterX shall mutually agree upon the scope, timing, and duration of the audit. Subscriber shall promptly notify PerimeterX with information regarding any non-compliance discovered during the course of an audit. Subscriber may not audit PerimeterX more than once annually unless there is a Security Incident.

15. **Data Destruction**. PerimeterX will destroy all Personal Data within sixty (60) days following the expiration or termination of this Agreement or Subscriber's request, cause its Subprocessors to do the same, and demonstrate to the satisfaction of Subscriber that it has taken such measures, unless Data Privacy Laws prevent PerimeterX from destroying all or part of the Subscriber Personal Data disclosed. For clarity, PerimeterX may continue to process Personal Data that has been aggregated in a manner that does not identify individuals or customers to improve Subscriber's systems and services and data that PerimeterX, in good faith, believes it has identified as a threat (e.g., malware, a denial of service attack or other malicious activity) without identifying Subscriber as the source of the data.

16. **Technical and Organizational Safeguards**. PerimeterX will implement appropriate technical and organizational safeguards designed to protect Personal Data (i) from unauthorized or unlawful processing, (ii) against accidental or unlawful disclosure, alteration or loss, and/or (iii) unauthorized disclosure or access, including as applicable Art. 32 of the GDPR. PerimeterX will comply with strict internal controls in line with industry best practices, such as SOC2 guidelines. PerimeterX will implement security controls in the form of mandatory policies and procedures for all PerimeterX's employees who have access to Subscriber Personal Data to follow. These policies and procedures cover: (1) measures, standards, norms, procedures, and rules to address the appropriate level of security, (2) the meaning and importance of Personal Data and the need to keep it secure, confidential, and accessed only on a need to know basis, (3) staff functions, obligations and access rights, (4) procedures for reporting, managing and responding to security incidents and (5) procedures for making backup copies and recovering Personal Data.

17. **Miscellaneous**. Neither party will assign the DPA in whole or in part without the other party's prior written consent (which consent will not be unreasonably denied, delayed or conditioned), except to an Affiliate or a successor that is made in connection with a merger or sale of all or substantially all of a party's assets or stock. Any attempted assignment in violation of this restriction is void. The DPA shall bind and inure to the benefit of the parties, their respective successors and permitted assigns. If a conflict exists between any of the terms in the DPA and the Order Form, then this DPA will govern. This DPA can be executed electronically and in counterparts, each of which is

deemed to be an original and together comprise a single document. Each party represents and warrants that the individual binding a party under this DPA is authorized to do so.

Exhibit A

Standard Contractual Clauses (Processors)

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

Name and location of the data exporting organisations: Subscriber with address identified on the Order Form and and its Authorized Affiliates.

(the data exporter)

And

Name and location of the data importing organisation: PerimeterX, Inc., S. 400 El Camino Real, Suite 1400, San Mateo, CA 94402 and its Affiliates.

(the data importer)

each a “party”; together “the parties”,

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to

bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12

Obligation after the termination of personal data processing services

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

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

APPENDIX 1 TO THE 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 (please specify briefly your activities relevant to the transfer):

Is receiving website secuirty and monitoring services from PerimeterX.

Data importer

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

Is the service provider for Data Exporter.

Data subjects

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

An identifiable or identified natural person ("***User***") who uses the Subscriber "Websites" and/or "Apps" (as defined and identified in the Order Form).

Categories of data

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

Data Importer may record certain information about how a User uses the Subscriber Websites or Apps, including a User's Internet Protocol (IP) address and other user engagement and interaction metrics and other statistics. Data Importer does not collect any of the following information from Users: name, email address, credit card information, usernames or passwords or other login credentials.

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):

Data Importer will provide Data Exporter website monitoring and security services set forth in the Order Form.

Appendix 2 re: security and organizational measures:

Data Importer will at a minimum institute the technical and organizational measures to ensure a level of security appropriate with the risk, as is required in Art. 32 of the GDPR. Data Importer will comply with strict internal controls in line with industry best practices, such as SOC2 guidelines. Data Importer will implement security controls in the form of mandatory policies and procedures for all Data Importer employees who have access to Data Exporter's data to follow. These policies and procedures cover: (1) measures, standards, norms, procedures, and rules to address the appropriate level of security, (2) the meaning and importance of personal data and the need to keep it secure, confidential, and accessed only on a need to know basis, (3) staff functions, obligations and access rights, (4) procedures for reporting, managing and responding to security incidents and (5) procedures for making backup copies and recovering personal data.

Previous Versions