EXTRAHOP NETWORKS, INC.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the services agreement or electronic or other written agreement (collectively, the "**Agreement**") between ExtraHop Networks, Inc. and/or its affiliates ("**ExtraHop**") and the entity receiving Services listed on the signature pages hereto ("**Customer**") to reflect the parties' agreement with regard to the processing of personal data. To the extent ExtraHop is providing services (the "**Services**") under the Agreement that require or involve processing personal data on behalf of Customer in accordance with applicable Data Protection Legislation, the provisions of this DPA shall apply. References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

This DPA consists of two parts: the main body of the DPA and Attachment 1 (the standard contractual clauses).

How to Execute this DPA:

To complete this DPA, Customer should:

(a) Sign the main body of this DPA in the signature section below.

(b) Complete any missing information and sign the standard contractual clauses at the end of Attachment 1.

(c) Complete and sign Appendix 1 to Attachment 1.

(d) Send the completed and signed DPA to ExtraHop via email at contractnotices@extrahop.com. Upon receipt of the validly completed DPA, this DPA will be legally binding (provided that Customer has not overwritten or modified any of the terms beyond completing the missing information).

Data Processing Terms:

1. Definitions.

1.1. "**Data Protection Legislation**" means the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any replacement directive or regulation imposing equivalent obligations, including the General Data Protection Regulation (Regulation (EU) 2016/279).

1.2. "**data controller**", "**data processor**", "**subprocessor**", "**data subject**", "**personal data**", "**processing**", and "**appropriate technical and organisational measures**" shall be interpreted in accordance with the Data Protection Legislation.

1.3. "**standard contractual clauses**" shall mean the model controller-to-processor contract for the transfer of personal data to third countries issued by the European Commission on the basis of Article 26(4) of Directive 95/46/EC pursuant to Decision 2010/87/EU.

1.4. "**Good Industry Practice**" means, in relation to any activity and under any circumstance, exercising the same skill, expertise and judgment and using facilities and resources of a similar or superior quality as would be expected from a person who: (a) is skilled and experienced in providing the Services in question, seeking in good faith to comply with his contractual obligations and seeking to avoid liability arising under any duty of care that might reasonably apply; (b) takes all proper and reasonable care and is diligent in performing his obligations; and (c) complies with all applicable legislation and any applicable industry standards including any recognised industry quality standards and applicable law.

2. Scope.

The parties agree that Customer is a data controller and that ExtraHop is a data processor in relation to personal data that ExtraHop processes on behalf of Customer in the course of providing Services under the Agreement. The subject-matter of the data processing, the types of personal data processed, and the categories of data subjects will be defined by, and/or limited to that necessary to carry out the Services described in, the Agreement. The processing will be carried out until the date ExtraHop ceases to provide the Services to the Customer.

3. Processing of Personal Data.

3.1. ExtraHop will process the personal data only in accordance with written instructions from Customer. Such instructions may be specific or of a general nature as set out in this DPA, the Agreement, applicable product or service documentation, or as otherwise notified by Customer to ExtraHop in writing from time to time. The nature and purposes of the processing shall be limited to those necessary to carry out such instructions or for any other purposes, except as required by law. ExtraHop may only correct, delete, or block the personal data processed on behalf of Customer as and when instructed to do so by Customer. If ExtraHop is required by law to process the personal data for any other purpose, ExtraHop will inform Customer of such requirement prior to the processing unless prohibited by law from doing so.

3.2. ExtraHop will comply with applicable data protection laws to the extent that such laws by their terms impose obligations directly upon ExtraHop as a processor in connection with the Services specified in the Agreement.

3.3. ExtraHop will notify Customer immediately if, in ExtraHop's opinion, an instruction given by Customer for the processing of personal data infringes applicable Data Protection Legislation.

3.4. ExtraHop will not retain any of the personal data for longer than is necessary to provide the Services. At the end of the Services, or upon Customer's request, ExtraHop will securely destroy or return (at Customer's election) the personal data to Customer.

3.5. ExtraHop will take reasonable steps to assist Customer in meeting Customer's obligations under applicable Data Protection Legislation, including Customer's obligations to respond to requests by data subjects to exercise their rights with respect to personal data, adhere to data security obligations, respond to data breaches and other incidents involving personal data, conduct data protection impact assessments, and consult with supervisory authorities.

4. Security.

4.1. ExtraHop will implement and maintain appropriate technical and organisational measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure, including, but not limited to, a process for regularly testing, assessing and evaluating the effectiveness of the implemented technical and organisational measures. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and as a minimum shall be in accordance with the Data Protection Legislation and Good Industry Practice.

4.2. ExtraHop will take reasonable steps to ensure the reliability and competence of any ExtraHop personnel who have access to the personal data. ExtraHop will ensure that all ExtraHop personnel required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set forth in this DPA.

5. Transfer of Personal Data from the European Economic Area.

Customer acknowledges and agrees that any personal data processed by ExtraHop in providing the Services may be transferred outside of the EEA. Where ExtraHop transfers personal data outside of the EEA, ExtraHop shall make such transfers: (i) to countries that have been recognized by the European Commission as providing an adequate level of protection for personal data; (ii) to countries covered by a suitable framework recognized by relevant authorities or courts as providing an adequate level of protection for personal data, such as the EU-US Privacy Shield or binding corporate rules; or (iii) pursuant to the standard contractual clauses.

6. Subprocessors.

ExtraHop will not give access to or transfer any personal data to any third party without the prior written consent of Customer. Customer hereby authorizes: (i) ExtraHop to engage its affiliates as subprocessors; and (ii) ExtraHop or any such affiliate to engage third parties from time to time to process personal data in connection with the Services. ExtraHop shall make available to Customer a current list of subprocessors for the Services upon Customer's written request. ExtraHop will only disclose personal data to subprocessors that are parties to written agreements with ExtraHop including obligations substantially similar to those in this DPA. ExtraHop shall be liable for the acts and omissions of its subprocessors to the same extent ExtraHop would be liable if performing the services of each subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. Audit.

7.1. Customer may audit ExtraHop's compliance with this DPA if: (i) ExtraHop notifies Customer of a Security Breach, as defined below; (ii) Customer reasonably believes that ExtraHop is not in compliance with its security commitments under this DPA; or (iii) such audit legally is required by applicable law. Such audit must be conducted in accordance with the procedures set forth in this Section 7 and may not be conducted more than once per calendar year. If Customer engages a third party to conduct the audit, the third party must be mutually agreed to by Customer and ExtraHop and must execute a written confidentiality agreement acceptable to ExtraHop before conducting the audit.

7.2. To request an audit, Customer must submit a detailed audit plan to ExtraHop at least six (6) weeks in advance of the proposed audit date. The audit plan must describe the proposed scope, duration, and start date of the audit. ExtraHop will review the audit plan and provide Customer with any concerns or questions. ExtraHop will work cooperatively with Customer to agree on a final audit plan. If the scope of the requested audit is addressed in an audit report such as SOC 2 or other similar audit report performed by a qualified third-party auditor within the prior twelve (12) months and ExtraHop confirms there are no known material changes in the controls audited, then Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

7.3. Audits must be conducted during regular business hours, subject to ExtraHop's applicable policies, and may not unreasonably interfere with ExtraHop's business activities. Audits, including the engagement of a third-party auditor, shall be at Customer's sole expense. Any request for ExtraHop to provide assistance with an audit is considered a separate service and ExtraHop will provide its reimbursement rate for which Customer shall be responsible.

7.4. After conducting an audit or receiving an audit report from ExtraHop, Customer must notify ExtraHop of the specific manner, if any, in which ExtraHop does not comply with the obligations of this DPA, if applicable. Upon such notice, ExtraHop will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

7.5. Customer will, at no charge, provide ExtraHop any audit reports generated in connection with any audit under this Section 7, unless prohibited by law. Customer may use the audit reports solely for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA. Any audit reports, notices, and information provided or produced under this Section 7 will be deemed ExtraHop's confidential information.

8. Security Breach.

8.1. If ExtraHop becomes aware of any unauthorised or unlawful destruction, loss, disclosure of, access to or handling of personal data that is processed by ExtraHop in the course of providing Services under the Agreement (a "**Security Breach**"), ExtraHop will: (i) without undue delay, inform Customer of the Security Breach; (ii) investigate the Security Breach and provide information reasonably requested by Customer to fulfil its obligations under Data Protection Legislation; (iii) take reasonable steps to mitigate the effects of the Security Breach; and (iv) carry out reasonable actions necessary to remedy the Security Breach.

8.2. The parties agree to coordinate in good faith on developing the contents of any related public statements or any required notices for the affected data subjects and/or notices to the relevant data protection authorities.

9. General.

9.1. This DPA shall only become legally binding between Customer and ExtraHop when fully executed and will terminate when the Agreement terminates, without further action required by either party.

9.2. In the event that any provision of this DPA shall be determined to be illegal or unenforceable, that provision will be limited or eliminated to the minimum extent necessary so that this DPA shall otherwise remain in full force and effect and enforceable.

9.3. Except as amended by this DPA, the Agreement will remain in full force and effect. In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall control.

IN WITNESS WHEREOF, the parties hereto have executed this DPA as of the date first above written.

EXTRAHOP NETWORKS, INC.	
("**ExtraHop**")	("**Customer**")
DocuSigned by: Thomas M. O'Brien 2A65452FBDF2419...	
Signature	Signature
Thomas O'Brien	
Name	Name
VP of Legal	
Title	Title
April 27, 2018	
Date	Date

ATTACHMENT 1 – STANDARD CONTRACTUAL CLAUSES

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 of the data exporting organisation: ....

Address: ....

Tel.: .... ; fax: ....; e-mail:...

Other information needed to identify the organisation:

……………………………………………………………

(the data **exporter**)

And

Name of the data importing organisation: ExtraHop Networks, Inc.

Address: 520 Pike Street, Suite 1700, Seattle, WA 98101

Tel.: (877) 333 9872; e-mail: contractnotices@extrahop.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;

(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.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

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

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer: ExtraHop Networks, Inc.

Name (written out in full): Thomas O’Brien

Position: VP of Legal

Address: 520 Pike Street, Suite 1700, Seattle, WA 98101

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

DocuSigned by:

Thomas M. O'Brien

Signature……………………………………….
2A65452FBDF2419...

(stamp of organisation)

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):

The data exporter is (i) the legal entity that has executed the Clauses as data exporter; and (ii) all affiliates established within the European Economic Area and Switzerland.

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

ExtraHop Networks, Inc. is a wire data analytics company.

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

Data exporter may submit personal data to data importer, which may include but is not limited to personal data relating to the following categories of data subjects:

- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, and contractors of data exporter (who are natural persons)
- Data exporter's authorized users of data importer's Services

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

Data exporter may submit personal data to data importer for the Services, the extent of which is determined and controlled by the data exporter, and which for the sake of clarity may include but is not limited to names, contact information, connection data, and localisation data.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories to data importer for the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which for the sake of clarity includes but is not limited to information revealing racial or ethnic origin, criminal background, and professional trade memberships.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of the processing of personal data by data importer is the performance of the Services pursuant to the agreement between data importer and data exporter.

DATA EXPORTER:

Name:………………………………

Authorised Signature ……………………

DATA IMPORTER: EXTRAHOP NETWORKS, INC.

Name: Thomas O'Brien

Authorised Signature ………

DocuSigned by:
Thomas M. O'Brien
2A65452FBDF2419...

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data as described in its internal security and privacy policies and documentation, which are made reasonably available by data importer upon request. Data importer will not materially decrease the overall security of its Services during the Agreement term.