EXTRAHOP NETWORKS, INC.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the services agreement or electronic or other written agreement between ExtraHop Networks, Inc. and/or its affiliates ("**ExtraHop**") and **Customer** (the entity receiving Services) (collectively, the "**Agreement**") 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 Data Protection Law, 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 three parts: the main body of the DPA, Attachment 1 (EU standard contractual clauses), and Attachment 2 (UK international data transfer addendum).

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 and sign Annex 1 to Attachment 1.

(c) Complete any missing information and sign Attachment 2.

(d) Complete and sign Appendix 1 to Attachment 2.

(e) 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 Law**" means (a) the General Data Protection Regulation (Regulation (EU) 2016/679) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (b) the UK General Data Protection Regulation as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, (c) the UK Data Protection Act 2018, (d) the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et seq. and its implementing regulations ("CCPA"), and (e) any replacement directive or regulation imposing equivalent obligations.

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

1.3. "**standard contractual clauses**" means, collectively (i) the controller-to-processor module for the transfer of personal data to third countries set out in the Annex to the European Commission's Implementing Decision (EU) 2021/914 as set forth in Attachment 1; and (ii) the UK international data transfer addendum to the European Commission's standard contractual clauses as set forth in Attachment 2.

1.4. "**Good Industry Practice**" means, in relation to any activity and under any circumstance, exercising the same skill, expertise and judgement 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 Law and any applicable industry standards including any recognized 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 Law.

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 any Customer personal data in its possession.

3.5. ExtraHop will take reasonable steps to assist Customer in meeting Customer's obligations under applicable Data Protection Law, 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 organizational measures to protect the personal data against unauthorized 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 organizational measures. These measures shall be appropriate to the harm which might result from any unauthorized 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 Law 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 and United Kingdom.

Customer acknowledges and agrees that any personal data processed by ExtraHop in providing the Services may be transferred outside of the EEA and UK. Where ExtraHop transfers personal data outside of the EEA and/or UK, ExtraHop shall make such transfers pursuant to: (i) countries that have been recognized by the European Commission or the Information Commission Office as providing an adequate level of protection for personal data; or (ii) countries covered by a suitable framework recognized by relevant authorities or courts as providing an adequate level of protection for personal data.

6. Subprocessors.

Customer consents generally to ExtraHop's engagement of subprocessors required to deliver the Services and perform under the Agreement. ExtraHop will provide written notice to Customer of any new or replacement subprocessors. If Customer objects to the use of a new subprocessor, Customer shall notify ExtraHop in writing within ten (10) business days after receipt of ExtraHop's notice, and ExtraHop will work with Customer to resolve its objection. If the objection cannot be resolved within thirty (30) days, Customer may terminate the applicable Service. 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.

If ExtraHop becomes aware of any unauthorized 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 Law; (iii) take reasonable steps to mitigate the effects of the Security Breach; and (iv) carry out reasonable actions necessary to remedy the Security Breach.

9. State Privacy Law

9.1. ExtraHop shall comply with the applicable provisions of the CCPA.

9.2. ExtraHop shall not sell or share Personal Data it Processes in connection with the Agreement.

9.3. ExtraHop shall only Process Personal Data for the specific business purposes of providing services and performing under the Agreement, and Customer discloses Personal Data to ExtraHop only for those limited and specified business purposes, except as expressly permitted by Data Protection Law.

9.4. ExtraHop shall not combine Customer Data with Personal Data obtained from, or on behalf of, sources other than Customer, except as expressly permitted under by Data Protection Law.

9.5. ExtraHop is prohibited from retaining, using, or disclosing the Personal Data collected pursuant to the Agreement: (i) for a commercial purpose other than the specified business purpose, or (ii) outside of the direct business relationship between the parties, unless expressly permitted by Data Protection Law.

9.6. ExtraHop shall notify ExtraHop promptly if it makes a determination that it can no longer meet its obligations under Data Protection Law.

10. General.

10.1. 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.

10.2. 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.

10.3. 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 indicated below.

DocuSigned by: Lauren Zajac 164C9BD4EABB4C3...	
Signature	Signature
Lauren Zajac	
Name	Name
Chief Legal Officer	
Title	Title
3/31/2023	
Date	Date
ExtraHop Networks, Inc.	
(“ExtraHop”)	(“Customer”)

ATTACHMENT 1

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer controller to processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 5 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter:

Name: Customer

Address: As specified in the Agreement

Contact person's name, position and contact details: As specified in the Agreement

Activities relevant to the data transferred under these Clauses: The provision of products and services pursuant to the Agreement and as further described in ExtraHop's documentation.

Signature and date:

Role: Controller

Data importer:

Name: ExtraHop Networks, Inc.

Address: 520 Pike Street, Suite 1600, Seattle, WA 98101, United States of America

Contact person's name, position and contact details: Legal Department, contractnotices@extrahop.com

Activities relevant to the data transferred under these Clauses: The provision of products and services pursuant to the Agreement and as further described in ExtraHop's documentation.

Signature and date: DocuSigned by: Lauren Zajac 164C9BD4EABB4C3... 3/31/2023

Role: Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Customer may submit personal data to ExtraHop, which may include but is not limited to personal data relating to the following categories of data subjects:

- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, and contractors of Customer (who are natural persons)
- Customer's authorized users of ExtraHop's products and services

Categories of personal data transferred

Customer may submit personal data to ExtraHop for the products and services, the extent of which is determined and controlled by the Customer, and which for the sake of clarity may include, but is not limited to, names, contact information, device information, connection data, and localization data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Customer may submit special categories to ExtraHop for the products and services, the extent of which is determined and controlled by the Customer in its sole discretion, and which for the sake of clarity may include, but is not limited to, information revealing racial or ethnic origin, criminal background, and professional trade memberships. The applicable security measures are described in ExtraHop's documentation applicable to the specific products and services purchased by Customer, as updated from time to time, and as further described in the Agreement.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis depending on the use of the products and services by Customer.

Nature of the processing

The provision of the products and services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

ExtraHop will process personal data as necessary to provide the products and services pursuant to the Agreement, as further specified in ExtraHop's documentation, and as further instructed by Customer in its use of the product and services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

ExtraHop will process personal data for the duration of the Agreement, unless otherwise agreed upon in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors will process personal data as necessary to provide the products and services pursuant to the Agreement. The sub-processor will process personal data for the duration of the Agreement, unless otherwise agreed in writing. Identities of the sub-processor used for the provision of products and services and their country of location can be found on ExtraHop's customer portal.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

Where ExtraHop processes Customer personal data originating from the EEA, the competent supervisory authority shall be the Irish Data Protection Commission.

Where ExtraHop processes Customer personal data originating from the UK, the competent supervisory authority shall be the UK Information Commissioner's Office.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

ExtraHop will maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of personal data as described in the documentation applicable to the specific products and services purchased by Customer and as set forth in the Agreement. ExtraHop will not materially decrease the overall security of its products and services during a subscription term.

ATTACHMENT 2

STANDARD DATA PROTECTION CLAUSES TO BE ISSUED BY THE COMMISSIONER UNDER S119A(1) DATA PROTECTION ACT 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

Table 1: Parties

Start date	Effective on the same start date as the EU Commission Standard Contractual Clauses	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: ExtraHop Networks, Inc. Trading name (if different): N/A Main address (if a company registered address): 520 Pike Street, Suite 1600, Seattle, WA 98101, United States of America Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Legal Team Job Title: N/A Contact details including email: contractnotices@extrahop.com
Signature (if required for the purposes of Section 2)		DocuSigned by: Lauren Zajac 164C9BD4EABB4C3...

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	Not used	Not used	General	N/A	
3						
4						

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As detailed in Annex I above

Annex 1B: Description of Transfer: As detailed in Annex I above

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As detailed in Annex II above

Annex III: List of Sub processors (Modules 2 and 3 only): As detailed in Annex I, N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to Law (or specific provisions of Law) means that Law (or specific provision) as it may change over time. This includes where that Law (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.