GLOBAL DATA PROTECTION AGREEMENT

INSTRUCTIONS for CREATING A LEGALLY BINDING DPA:

This Data Protection Agreement ("DPA") has been pre-signed on behalf of CrowdStrike, Inc. ("CrowdStrike").

This DPA will become legally binding on all parties when Customer or a Customer Group Member (both defined below):

1. Complete the information in the signature box on page 11 of this DPA;
2. Sign the DPA on page 11 (add signature boxes and/or pages if you wish to add affiliates to the DPA);
3. Send the signed DPA to CrowdStrike by email to *dpa@crowdstrike.com;* AND
4. CrowdStrike has received the validly completed and signed DPA via dpa@crowdstrike.com.

By signing this DPA, Customer (and/or Customer Group Member) enters into this DPA on behalf of itself and, to the extent required and allowed under Applicable Laws, in the name and on behalf of each Customer Group Member, if and to the extent CrowdStrike processes the Customer Group Member's Personal Data.

For avoidance of doubt, signature of the DPA on page 11 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices. For Customers who require an executed Standard Contractual Clauses (EU)2021/914, Customer should also sign on page 28. For Customers who require an executed Standard Contractual Clauses (EU)2010/593, complete the information as the Data Exporter on page 35 and complete the information in the signature box and sign on page 41.

******End of instructions******

This **Data Protection Agreement** ("DPA") supplements any existing and currently valid CrowdStrike Terms and Conditions, Master Purchase Agreement or other similar agreement (each "Agreement") previously made between CrowdStrike, Inc. ("CrowdStrike") and the party named below in the signature area ("Customer") (collectively, the "Parties"), if and to the extent required under Applicable Laws (defined below), where CrowdStrike Processes Customer Personal Data (both defined below). Upon execution by both Parties, this DPA supersedes and replaces any prior Data Protection Agreement, or any other prior understanding or agreement, related to the processing of Customer Personal Data in connection with the Agreement.

Notwithstanding this DPA, the terms of the Agreement shall remain in full force and effect.

1. Definitions

1.1 Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. Cognate terms shall be construed accordingly.

1.1.1 "**Applicable Laws**" means any laws that regulate the Processing, privacy or security of Customer Personal Data and that are directly applicable to each respective party to this DPA in the context of CrowdStrike Processing Customer Personal Data;

1.1.2 "**CrowdStrike Affiliate**" means an entity belonging to the CrowdStrike group of companies named in Exhibit G as a CrowdStrike Affiliate;

1.1.3 "**Customer Affiliate**" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise, and is authorized to use the Services consistent with the Agreement and CrowdStrike Processing Affiliate's Customer Personal Data;

1.1.4 "**Customer Group Member**" means Customer and any Customer Affiliate;

1.1.5 "**Customer Personal Data**" means any Personal Data Processed by CrowdStrike or a Subprocessor on behalf of a Customer Group Member in the provision of the Services;

1.1.6 "**GDPR**" means the General Data Protection Regulation 2016/679 ("GDPR") and any local laws implementing or supplementing the GDPR;

1.1.7 "**Offerings**" means collectively, any Products, Product-Related Services or Professional Services from CrowdStrike;

1.1.8 "**Onward Transfer**" means any transfer of Customer Personal Data from CrowdStrike to a Subprocessor;

1.1.9 "**Restricted Transfer**" means any export of Customer Personal Data from its country of origin to a third country in the course of CrowdStrike's provision of the Services set forth in the Agreement that is prohibited under Applicable Laws, unless (a) the destination has been recognized as providing an adequate level of data protection by competent data protection authority, or otherwise in a legal binding way, or (b) the Parties adhere to an appropriate, under Applicable Laws recognized adequacy mechanism ensuring an adequate level of data protection; and

1.1.10 "**Subprocessor**" means any contracted service provider (including any third party and CrowdStrike Affiliate, but excluding an employee of CrowdStrike or CrowdStrike sub-contractors) Processing Customer Personal Data in the course of CrowdStrike's provisioning of the Services set forth in the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", **"Processor",** "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

1.3 The word "**include**" shall be construed to mean include without limitation.

2. Authority

Only if and to the extent required under Applicable Laws, CrowdStrike enters into this DPA for (i) itself and (ii) its Affiliates (as an agent), to the extent such entity is Processing Customer Personal Data duly and effectively authorized (or subsequently ratified).

3. Processing of Customer Personal Data

3.1 The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer determines the purposes and means of the Processing of Customer Personal Data, and CrowdStrike processes Customer Personal Data on Customer's behalf in the provisioning of the Services agreed to.

3.2 CrowdStrike shall:

3.2.1 Process Customer Personal Data only on relevant Customer Group Member's documented instructions, as set out in the Agreement and this DPA, unless Processing is required by Applicable Laws. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to CrowdStrike for the Processing of Customer Personal Data. Any additional or alternate instructions, having an impact to the Services agreed to, must be agreed upon separately; and

3.2.2 Unless prohibited by Applicable Law, CrowdStrike shall inform the Customer in advance if (i) a Customer Group Member's instructions conflict with Applicable Law; or (ii) Applicable Law requires any processing contrary to the Customer Group Member's instructions.

3.3 Customer Group Member shall:

3.3.1 Be responsible for complying with Applicable Laws when making decisions and issuing instructions for the Processing of Customer Personal Data, including securing all permissions, consents or authorizations that may be required.

3.3.2 Indemnify CrowdStrike and its Subprocessors for any action brought against them arising from Customer's breach of this Section, whether by a Data Subject or a government authority. This provision does not diminish Customer Group Member or Data Subject's rights under Applicable Laws related to CrowdStrike's adherence to its obligations under Applicable Laws.

4. CrowdStrike Personnel

CrowdStrike shall:

4.1 Take reasonable steps to ensure the reliability of any person authorized to access Customer Personal Data;

4.2 Ensure access to Customer Personal Data is strictly limited to those individuals who need to know/access the relevant Customer Personal Data, as reasonably necessary for the purposes outlined in the Agreement or required under Applicable Laws;

4.3 Ensure all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms

of natural persons, CrowdStrike shall in relation to the Processing of Customer Personal Data maintain appropriate technical and organizational measures as specified in the Agreement and designed to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in Applicable Laws.

5.2 In assessing the appropriate level of security, CrowdStrike shall take into account the nature of the data and the Processing activities in assessing the risks posed by a potential Personal Data Breach.

6. Subprocessing

6.1 Each Customer Group Member authorizes CrowdStrike to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.

6.2 CrowdStrike may continue to use those Subprocessors already engaged as of the date of this DPA specified in Exhibit G, subject to CrowdStrike in each case meeting the obligations set out in section 6.5.

6.3 Customer agrees to CrowdStrike maintaining and updating its list of Subprocessors online, for the Falcon Platform and Humio as outlined in Exhibit G.

6.4 CrowdStrike shall provide notice of a proposed new Subprocessor to the Customer through the Falcon Platform / Humio, where Customer may elect to subscribe to such notices. Customers may sign up for email Subprocessor notifications at https://www.crowdstrike.com/subprocessor-notification/. Notice of a proposed new Subprocessor will be sent to Customer at least 30 days prior to CrowdStrike's use of the new Subprocessor to Process Customer Personal Data. During the notice period, Customer may object to a change in Subprocessor in writing, and CrowdStrike will use reasonable efforts to resolve Customer's objection, including commercially reasonable options to provide the Offerings without use of the proposed Subprocessor. Where such an alternative cannot be made available by CrowdStrike to Customer within 90 days of Customer providing notice of its objection, and notwithstanding anything in the Agreement, then Customer may terminate the Agreement to the extent that it relates to the Offerings which require the use of the proposed Subprocessor.

6.5 With respect to each Subprocessor, CrowdStrike shall:

6.5.1 Before the Subprocessor first Processes Customer Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by Applicable Laws, this DPA and the Agreement;

6.5.2 Ensure that the arrangement between CrowdStrike and Subprocessor is governed by a written contract which offers substantially the same level of protection for Customer Personal Data as required by this DPA and Applicable Laws, including Customer's ability to protect the rights of Data Subjects in the event CrowdStrike is insolvent, liquidated or otherwise ceases to exist.

6.5.3 Apply an adequacy mechanism recognized by Customer's Supervisory Authority as ensuring an adequate level of data protection under Applicable Laws where Subprocessor's Processing of Customer Personal Data involves a Restricted Transfer

6.5.4 Maintain copies of the agreements with Subprocessors as Customer may request from time to time. To the extent necessary to protect Confidential Information, CrowdStrike may redact the copies prior to sharing with Customer;

6.5.5 Remain fully responsible to Customer for the performance of Subprocessor's obligations in accordance with the Agreement; and

6.5.6 Notify Customer of Subprocessor's relevant failure to comply with obligations set out by Applicable Laws, this DPA and the Agreement.

7. Data Subject Rights

7.1 Customer represents and warrants to provide appropriate transparency to any Data Subjects concerned of CrowdStrike's Processing of Customer Personal Data, and respond to any request filed by Data Subjects as required under Applicable Laws.

7.2 Taking into account the nature of the Customer Personal Data Processing, CrowdStrike shall:

7.2.1 Not respond to the Data Subject request itself or by Subprocessor unless required by Applicable Laws;

7.2.2 Notify Customer without undue delay if CrowdStrike or any Subprocessor receive a request from a Data Subject under any Applicable Laws in respect to Customer Personal Data;

7.2.3 Reasonably assist Customer through appropriate technical and organizational measures to fulfil Customer's obligation to respond to Data Subject requests arising under Applicable Law, and where Customer is unable to respond to Data Subject requests through the information available by the Offerings.

8. Personal Data Breach

8.1 CrowdStrike shall notify Customer without undue delay, and within the timeframes required by Applicable Laws, upon CrowdStrike or any Subprocessor becoming aware of any Personal Data Breach affecting Customer Personal Data, providing Customer Group Member with sufficient information to meet obligations to report or inform Data Subjects of the Personal Data Breach under Applicable Laws.

8.2 CrowdStrike shall cooperate with Customer Group Member and take commercially reasonable steps to assist in the investigation, mitigation and remediation of such Personal Data Breach.

9. Obligations to Assist Customer

Taking into account the nature of the Processing and information available to Customer Group Member, in each case solely in relation to CrowdStrike's Processing of Customer Personal Data, CrowdStrike shall provide reasonable assistance to each Customer Group Member with any:

9.1.1 Necessary data protection impact assessments required of any Customer Group Member by Applicable Laws;

9.1.2 Consultations with or requests of a competent data protection authority;

9.1.3 Demonstration of compliance with Applicable Laws and this DPA; and

9.1.4 Inquiries about CrowdStrike's Processing of Customer Personal Data pursuant to the Agreement and this DPA.

10. Deletion of Customer Personal Data

10.1 Processing of Customer Personal Data by CrowdStrike shall only take place for the duration specified in Exhibit A.

10.2 At the end of the duration specified in Exhibit A or upon termination of the Services and pursuant to the Agreement, Customer Personal Data will be deleted within 90 days of being deprovisioned, unless the retention of Customer Personal Data is required under Applicable Laws. Upon Customer's written request, CrowdStrike shall:

10.2.1 Make Customer Personal Data available for return to Customer by reasonably providing Customer with a means to retrieve Customer Personal Data from the Falcon Platform or Humio;

10.2.2 Provide a written certification of deletion of Customer Personal Data to Customer.

11. Audit Rights

11.1 Subject to sections 11.2 to 11.4, CrowdStrike shall make available to Customer on request information necessary to demonstrate compliance with Applicable Laws and this DPA.

11.2 To the extent required by Applicable Laws, CrowdStrike shall contribute to audits by Customer or an independent auditor mandated by Customer, that is not a competitor of CrowdStrike, in relation to the Processing of the Customer Personal Data.

11.3 Information and audit rights of the Customer Group Members only arise under section 11.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Laws.

11.4 Notwithstanding the foregoing, CrowdStrike may exclude information and documentation that would reveal the identity of other CrowdStrike customers or information that CrowdStrike is required to keep confidential. Any information or records provided pursuant to this assessment process shall be considered CrowdStrike's Confidential Information and subject to the Confidentiality section of the Agreement.

12. Restricted Transfers from the European Economic Area, Switzerland, Israel, United Kingdom, Argentina

12.1 Where CrowdStrike makes a Restricted Transfer of Customer Personal Data originating from the EEA, Switzerland and/or Israel to a third country not determined by the European Commission, on the basis of Article 45 of the GDPR, offering an adequate level of data protection, and where CrowdStrike has not adopted another legally sufficient adequacy mechanism, the Standard Contractual Clauses (EU)2021/914 (Exhibit B) will be incorporated into this DPA and shall apply as follows:

12.1.1 CrowdStrike will be a Processor of Customer Personal Data;

12.1.2 Customer will be a Controller of Customer Personal Data;

12.1.3 Module 2 (Controller to Processor) shall apply;

12.1.4 Clause 7 (Docking Clause) does not apply;

12.1.5 The option in Clause 11(a) (Redress) does not apply;

12.1.6 The Parties choose Option 2 of Clause 17;

12.1.7 Clause 8.1 (Instructions). This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to CrowdStrike for the Processing of Customer Personal Data. Any additional or alternate instructions must be agreed upon separately. The following is deemed an instruction by the Customer Group Member to process Customer Personal Data: (a) Processing in accordance with the Agreement and any applicable orders; (b) Processing initiated by users in their use of the CrowdStrike Offerings, and (c) Processing to comply with other reasonable documented instructions provided by Customer Group Member (e.g., via email) where such instructions are consistent with the terms of the Agreement.

12.1.8 Clause 8.5 (Duration of processing and erasure or return of data). Customer acknowledges and expressly agrees that the process described in Section 10 of the DPA shall govern the fulfillment of requirements related to data erasure and return of data.

12.1.9 Clause 8.9(c, d) (Audit). The Parties agree that the audits described in Clause 8.9(c, d) shall be carried out in accordance with Section 11 of this DPA. To the extent Clause 8.9(c, d) additionally requires CrowdStrike's facilities be submitted for inspection, Customer Group Member may contact CrowdStrike through prior written notice to request an on-site audit of the procedures relevant to the protection of Customer Personal Data. Customer shall reimburse CrowdStrike for any time expended for any such on-site audit at CrowdStrike's then-current professional services rates, which shall be made available to Customer group Member upon request. Before the commencement of any such on-site audit, Customer Group Member and CrowdStrike shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer Group Member shall promptly notify CrowdStrike with information regarding any noncompliance discovered during the course of an audit.

12.1.10 Clause 9 (Use of sub-processors). Customer acknowledges and expressly agrees that CrowdStrike may engage new Subprocessors as described in Section 6 of the DPA.

12.1.11 Where CrowdStrike makes a Restricted Transfer of Customer Personal Data originating from Switzerland to a third country, the following additional requirements shall apply to the extent that the data transfers are exclusively subject to the Swiss Data Protection Act (FADP) or are subject to both the FADP and the GDPR: (i) The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of these Standard Contractual Clauses. (ii) Insofar as the data transfers underlying these Standard Contractual Clauses are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP. Insofar as the data transfers underlying these Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP

insofar as the data transfers are subject to the FADP. (iii) Until the revised Swiss Data Protection Act (rev. FADP) enters into force, the provisions of these Standard Contractual Clauses and all Exhibits also protect the Customer Personal Data of Customer Group Members to the extent that these provisions are applicable to them under Swiss law.

12.2 Where CrowdStrike makes a Restricted Transfer of Customer Personal Data originating from the United Kingdom ("UK") to a third country not determined by the British Information Commissioner Office offering an adequate level of data protection, and where CrowdStrike has not adopted another legally sufficient adequacy mechanism, the Standard Contractual Clauses (EU)2010/593 (Exhibit H) will be incorporated into this DPA and shall apply as follows:

12.2.1 Where the British Information Commissioner Office adopts an agreement that would be used as a safeguarding mechanism for restricted transfers of data covered by the UK GDPR such as the International Data Transfer Agreement (IDTA), then this may be used by the Parties in lieu of the Standard Contractual Clauses (EU)2010/593 to govern the handling and safeguarding of Customer Personal Data in line with the UK GDPR.

12.2.2 These Standard Contractual Clauses and the additional terms specified in this Section 12.2 of this DPA shall apply to (i) the legal entity that has executed the DPA, and (ii) its Customer Group Members established within the United Kingdom, which have implemented CrowdStrike's Offerings consistent with the Agreement and CrowdStrike processes their Customer Personal Data. With regard to these Standard Contractual Clauses and this Section 12.2, the aforementioned entities shall be deemed "Data Exporters".

12.2.3 Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to CrowdStrike for the Processing of Customer Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of these Standard Contractual Clauses, the following is deemed an instruction by the Customer Group Member to process Customer Personal Data: (a) Processing in accordance with the Agreement and any applicable orders; (b) Processing initiated by users in their use of the CrowdStrike's Offerings, and (c) Processing to comply with other reasonable documented instructions provided by Customer Group Member (e.g., via email) where such instructions are consistent with the terms of the Agreement.

12.2.4 Appointment of new Subprocessors and List of current Subprocessors. Pursuant to Clause 5(h) of these Standard Contractual Clauses (EU)2010/593, Customer acknowledges and expressly agrees that (a) CrowdStrike's Affiliates may be retained as Subprocessors; and (b) CrowdStrike and CrowdStrike's Affiliates respectively may engage third-party Subprocessors in connection with the provision of CrowdStrike's Offerings. CrowdStrike shall make available to Customer the current list of Subprocessors in accordance with Section 6a and 12.3 of this DPA.

12.2.5 Notification of New Subprocessors and Objection Right for new Subprocessors. Pursuant to Clause 5(h) of these Standard Contractual Clauses and consistent with Article 28 of the GDPR, Customer acknowledges and expressly agrees that CrowdStrike may engage new Subprocessors as described in Section 6 of the DPA.

12.2.6 Sub-processor Agreements. The parties agree that Subprocessing obligations pursuant to Clause 11 of these Standard Contractual Clauses shall be carried out in accordance with GDPR Article 28. The parties agree that the copies of the Subprocessor agreements that must be provided by CrowdStrike to Customer pursuant to Clause 5(j) of these Standard Contractual Clauses may have all commercial and confidential information, or clauses unrelated to these Standard Contractual Clauses or their equivalent, redacted by CrowdStrike beforehand; and, that such copies will be provided by CrowdStrike, in a manner to be determined in its discretion, only upon written request by Customer.

12.2.7 Audits. The Parties agree that the audits described in Clause 5(f) and Clause 12(2) of these Standard Contractual Clauses shall be carried out in accordance with Section 11 of this DPA. To the extent these Standard Contractual Clauses (EU)2010/593 additionally require CrowdStrike's facilities be submitted for inspection, Customer Group Member may contact CrowdStrike through prior written notice to request an on-site audit of the procedures relevant to the protection of Customer Personal Data. Customer shall reimburse CrowdStrike for any time expended for any such on-site audit at CrowdStrike's then-current professional services rates, which shall be made available to Customer group Member upon request. Before the commencement of any such on-site audit, Customer Group Member and CrowdStrike shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer Group Member shall promptly notify CrowdStrike with information regarding any noncompliance discovered during the course of an audit.

12.2.8 Certification of Deletion. The Parties agree that the certification of deletion of Customer Personal Data that is described in Clause 12(1) of these Standard Contractual Clauses shall be provided by CrowdStrike to Customer Group Member only upon Customer Group Member's request pursuant to Section 10.2 of this DPA.

12.2.9 Liability Cap. The Parties agree that the total combined liability of either Party and its Affiliates towards the other Party and its Affiliates under or in connection with the Agreement and these Standard Contractual Clauses combined will be limited to the Limitation of Liability applicable cap (maximum) for the relevant party set forth in the Agreement.

12.3 Where CrowdStrike makes a Restricted Transfer of Customer Personal Data originating from Argentina to a third country not determined by the Agencia de Acceso a la Información Pública (AAIP) as offering an adequate level of data protection, and in the event this DPA is not deemed to provide adequate guarantees under the law, then where CrowdStrike has not adopted another legally sufficient adequacy mechanism the Standard Contractual Clauses made under Regulation No. 60-E/2016 will be incorporated into this DPA and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate guarantees.

12.4 Where Exhibit B and H apply, Customer acknowledges that CrowdStrike maintains an up-to-date List of Subprocessors online as outlined in Exhibit G.

13. General Terms

Governing law and jurisdiction

13.1 The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

13.2 This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

13.3 Nothing in this DPA reduces CrowdStrike's obligations under the Agreement in relation to the protection of Customer Personal Data or permits CrowdStrike to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Agreement.

13.4 Any conflict between the terms of the Agreement and this DPA related to the processing of Customer Personal Data are resolved in the following order of priority: (1) the Standard Contractual Clauses (Exhibits B and H - in the case of Restricted Transfers where it materially affects the adequacy of the transfer); (2) the DPA; (3) the Agreement.

Severance

13.5 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

LIMITATION OF LIABILITY

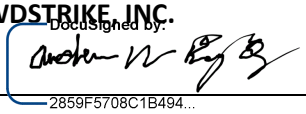
13.6 Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Customer Affiliates and CrowdStrike, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement and the applicable cap (maximum) for the relevant party set forth in the Agreement. Any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

13.7 For the avoidance of doubt, CrowdStrike and CrowdStrike Affiliates' total liability for all claims from Customer and all of Customers Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Customer Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Customer Affiliate that is a contractual party to any such DPA.

13.8 To the extent required by Applicable Laws, (i) this section is not intended to modify or limit the Parties' liability for Data Subject claims made against a Party where there is joint and several liability, or (ii) limit either Party's responsibility to pay penalties imposed on such Party by a regulatory authority.

The Parties by their duly authorized representatives have executed this DPA to be effective as of the Effective Date.

CROWDSTRIKE, INC.

By: DocuSigned by:  2859F5708C1B494...

Name: Drew Bagley

Title: VP & Counsel, Privacy & Cyber Policy

Date: 9/29/2021

Customer Name: _____

By: _____

Name: _____

Title: _____

Date: _____

Send notices to:

150 Mathilda Place, 3rd Floor
Sunnyvale, CA 94086
With a copy to: legal@crowdstrike.com

Notice Address: _____

EXHIBIT A

DESCRIPTION OF PROCESSING OF CUSTOMER PERSONAL DATA

This Exhibit A includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter, nature and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this DPA.

Purpose for which the Personal Data is Processed on Behalf of Customer Group Member

The purposes of the Processing of the Customer Personal Data set out in the Agreement and this DPA may include:

Provisioning/Use of Offerings. Personal Data that may be collected and used during the provisioning and use of the Offerings to deliver, support and improve the Offerings, administer the Agreement and further the business relationship between Customer and CrowdStrike, comply with law, act in accordance with Customer's written instructions, or otherwise in accordance with this Agreement.

Professional Services. Personal data gathered in connection with Professional Services for example as part of computer imaging, diagnostics and remediation in connection with the delivery of incident response or other forensics-oriented Professional Services.

File/Document Analysis. Personal data that is present in unknown or suspicious files or documents that are submitted to the Offerings for analysis for adversary activity or vulnerabilities. These unknown or suspicious files and other related information are used for security analysis and response or, when submitting crash reports, to make the product more reliable and/or improve CrowdStrike's products and services or enhance cybersecurity.

Support; Account Information. Customer employees' names and contact may be received in connection with technical support of the Offerings.

Categories of Personal Data Processed

As to the Falcon Platform, Depending on the Offerings and the Controller's naming conventions and environment, personal data, such as that possibly found in a computer name, user name or file name or the technical artifacts contemplated in the purposes above as well as personal data stored on data carriers of and provided or otherwise made accessible by the controller as part of our aforementioned services. Personal data associated with the provisioning and operation of the Offerings includes data included in machine event data, threat actor data, and Controller submitted data processed to protect Controller's devices from adversary activity and to provide additional applications, modules, functionality, and services selected by Controller.

As to Humio, depending on the Offerings and the log events generated by Customer software applications and the infrastructure on which they run, that may include Customer Personal Data.

Categories of Data Subjects whose Personal Data is Processed

Data subjects, such as Controller's computer system users or other individuals whose Personal Data Controller is responsible for and which Personal Data is processed in connection with the Offerings.

EXHIBIT B

STANDARD CONTRACTUAL CLAUSES
for the transfer of personal data to third countries pursuant to the GDPR

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 personal 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 Exhibit C (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 Exhibit C (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 Exhibit D.

(d) The Appendix to these Clauses containing the Exhibits 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 Exhibit D.

Clause 7 – Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Exhibit C.

(b) Once it has completed the Appendix and signed Exhibit C, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Exhibit C.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 2 (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 Exhibit D, 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 Exhibit F 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 Exhibit D. 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 Exhibit F. 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 Exhibit D.

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.

MODULE 3 (Transfer processor to processor)

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller.

The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 Exhibit D, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 Exhibit D. 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 controller 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, they 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 subject. 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 or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Exhibit F. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out in Exhibit D.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only

be disclosed to a third party located outside the European Union (6) (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 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:

iii. 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:

iv. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679:

v. 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

vi. 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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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 2 (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 30 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.

MODULE 3 (Transfer processor to processor)

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. (9) 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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 2 (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 Exhibit F 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.

MODULE 3 (Transfer processor to processor)

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Exhibit F 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 controller, as communicated by 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.

(b) The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular

sequence in seeking redress.

(c) 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.

(d) 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.

(e) 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.

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

(g) 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

(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

(a) 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 Exhibit E, 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

(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

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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18 - Choice of forum and jurisdiction

(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 the Netherlands.

(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.

EXHIBIT C

LIST OF PARTIES

Data exporter:

Name: Customer

Address: As specified in the Agreement

Contact person's name, position and contact details: As specified on page 10

Activities relevant to the data transferred under these Clauses: As specified in Exhibit D.

Role (controller/processor): Controller

Data importer:

Name: CrowdStrike Inc.

Address: 150 Mathilda Place, 3rd Floor, Sunnyvale, CA 94086, USA

Contact person's name, position and contact details: VP of Privacy, privacy@crowdstrike.com

Activities relevant to the data transferred under these Clauses: As detailed in Exhibit A to this DPA and the Agreement.

Role: Processor

EXHIBIT D

DESCRIPTION OF TRANSFER OF CUSTOMER PERSONAL DATA

Categories of data subjects whose personal data is transferred

As outlined in Exhibit A to this DPA under "Categories of Data Subjects whose Personal Data is Processed".

Categories of personal data transferred

As outlined in Exhibit A to this DPA under "Categories of Personal Data is Processed".

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

Depending on the nature and scope of the Offerings:

- As to the Falcon Platform and usages of CrowdStrike's EU Cloud, transfers may happen on a one-off basis, e.g. for Support, Engineering, OverWatch purposes.
- As to the Falcon Platform and usages of CrowdStrike's US Cloud, transfers may happen on a continuous basis by uploading and hosting Customer Personal Data.
- As to Humio and usages of CrowdStrike Humio's EU Cloud, transfers may happen on a one-off basis, e.g. for Support and Engineering purposes.
- As to Humio and usages of CrowdStrike Humio's US Cloud, transfers may happen on a continuous basis by uploading and hosting Customer Personal Data.

Nature of the processing

Depending on the nature and scope of the Offerings, collection, storage, use, dissemination (towards Subprocessors in line with the Agreement and this DPA), erasure of Customer Personal Data.

Purpose(s) of the data transfer and further processing

As outlined in Exhibit A to this DPA under " Purpose for which the Personal Data is Processed on Behalf of Customer Group Member".

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

The duration of the Processing of the Customer Personal Data is set out in the Agreement and this DPA.

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

For Falcon, CrowdStrike maintains an up-to-date list of sub-processors incl. the subject matter, nature and duration online at https://falcon.crowdstrike.com/support/documentation/34/crowdstrike-products-and-services-third-party-subprocessors-of-personal-data).

For Humio, CrowdStrike maintains an up-to-date list of sub-processors online at https://cloud.humio.com/account/subprocessors (EU cluster), and https://cloud.us.humio.com/account/subproccesors (US cluster).

EXHIBIT E

COMPETENT SUPERVISORY AUTHORITY

Where CrowdStrike Processes Customer Personal Data originating from the EEA, the competent supervisory authority shall be determined in accordance with Clause 13 of the Exhibit B: Landesbeauftragte für Datenschutz und Informationsfreiheit, Nordrhein-Westfalen, Kavalleriestr. 2 - 4, 40102 Düsseldorf, Germany.

Where CrowdStrike Processes Customer Personal Data originating from the UK, the competent supervisory authority shall be the UK Information Commissioner's Office.

EXHIBIT F

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

The technical and organizational measures are set forth in the Agreement.

Exhibit G

LIST OF SUBPROCESSORS

The controller has authorized the use of the following sub-processors.

For Falcon, CrowdStrike maintains an up-to-date list of sub-processors online at https://falcon.crowdstrike.com/support/documentation/34/crowdstrike-products-and-services-third-party-subprocessors-of-personal-data). For Humio, CrowdStrike maintains an up-to-date list of sub-processors online at https://cloud.humio.com/ account/subprocessors (EU cluster), and https://cloud.us.humio.com/account/subprocessors (US cluster).

Exhibit H

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: CrowdStrike, Inc.

Address: 150 Mathilda Place, Suite 300, Sunnyvale, CA 94086, U.S.A.,

Tel.: fax: ; **e-mail: dpa@crowdstrike.com** (for returning the DPA and these Contractual Clauses; and privacy@crowdstrike.com (for general privacy questions)

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 Exhibit D.

Clause 1

Definitions

For the purposes of the Clauses:

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

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

(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 Exhibit D 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.

---

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

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 Exhibit F 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 Exhibit F, and a summary description of the security measures, as well as a copy of any contract for

subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

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

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Exhibit F 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

---

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

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 Exhibit F 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, namely the UK.

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, namely the UK.

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.