GLOBAL DATA PROTECTION AGREEMENT

This Data Protection Agreement ("DPA") supplements any current CrowdStrike Terms and Conditions, Master Purchase Agreement or other similar agreement (each "Agreement") made between CrowdStrike, Inc. ("CrowdStrike") and the Customer (defined below) (collectively, the "Parties"), if and to the extent: (i) this DPA is required under Applicable Laws (defined below), and (ii) CrowdStrike Processes Customer Personal Data (both defined below). 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.

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 Data Protection Agreement ("DPA") supplements any current CrowdStrike Terms and Conditions, Master Purchase Agreement or other similar agreement (each "Agreement") previously made between CrowdStrike and the Customer (defined below) (collectively, the "Parties"), if and to the extent: (i) this DPA is required under Applicable Laws (defined below), and (ii) where CrowdStrike Processes Customer Personal Data (both defined below). 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.

This DPA will become legally binding when Customer:

1. Completes the information in the signature box of this DPA;
2. Signs the DPA in the signature box;
3. Sends 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;* (the date of such receipt is the "DPA Effective Date").

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 to have the same meaning.

1.1.1 **"Adequate Country"** means a country providing an adequate level of data protection pursuant to Applicable Laws;

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

1.1.3 "**CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civil Code § 1798.100 et seq.), including, but not limited to, amendments of the CCPA or applicable regulations promulgated by the California Privacy Protection Agency. Exhibit C contains provisions governing CrowdStrike's compliance with the CCPA;

1.1.4 "**CrowdStrike Affiliate**" means an entity belonging to the CrowdStrike group of companies. The term "CrowdStrike" is inclusive of the applicable CrowdStrike Affiliate when: (i) Applicable Laws require a direct relationship between the CrowdStrike Affiliate and the Customer with respect to data protection agreements, and (ii) the CrowdStrike Affiliate Processes Customer Personal Data. CrowdStrike represents that it is duly and effectively authorized (or will be subsequently ratified) to act on the CrowdStrike Affiliate's behalf;

1.1.5 "**Customer**" means (i) the person or entity that is indicated below in the signature block, or (ii) if there is no signature block or it is not completed, then Customer is the person or entity that has entered into the Agreement with CrowdStrike. Customer also means a Customer Affiliate when: (i) Applicable Laws require a direct relationship between CrowdStrike and the Customer's Affiliate with respect to data protection agreements, (ii) Customer is duly and effectively authorized (or subsequently ratified) to act on its Affiliate's behalf, and (iii) CrowdStrike processes the Affiliate's Customer Personal Data;

1.1.6 "**Customer Personal Data**" means any Personal Data Processed by CrowdStrike or a Subprocessor on behalf of the Customer in the provision of the Offerings;

1.1.7 **"EU-U.S. Data Privacy Framework"** or **"EU-U.S. DPF"** means the transfer mechanism in terms of Art. 45 of the EU GDPR that enables participating organizations - pursuant to the European Commission's Implementing Decision C(2023) 4745 final of 10.7.2023 and the EU-U.S. Data Privacy Framework Principles[1] as set forth by the U.S. Department of Commerce - to Process Customer Personal Data originating from the European Union (EU) and the European Economic Area (EEEA) ("**EU Customer Personal Data**") in the United States (U.S.) in accordance with Chapter V of the EU GDPR;

[1] https://www.dataprivacyframework.gov/s/framework-text

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

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

1.1.10 **"Personal Data"** means information provided by Customer to CrowdStrike or collected by CrowdStrike from Customer used to distinguish or trace a natural person's identity, either alone or when combined with other personal or identifying information that is linked or linkable by CrowdStrike to a specific natural person. Personal Data also includes such other information about a specific natural person to the extent that the data protection law applicable in the jurisdictions in which such person resides define such information as Personal Data.

1.1.11 **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.1.12 "**Restricted Transfer**" means: (i) any export by Customer of Customer Personal Data from its country of origin to CrowdStrike to a jurisdiction that is not an Adequate Country.

1.1.13 "**Standard Contractual Clauses"** or **"SCCs""** means the contractual clauses or other documentation required by Applicable Laws for the transfer of Personal Data to Processors that are not established in Adequate Countries, as may be amended, superseded or replaced by Applicable Law;

1.1.14 "**Subprocessor**" means any contracted service provider (including any third party and CrowdStrike Affiliate but excluding sub-contractors unless specified in an applicable Statement of Work) Processing Customer Personal Data in the course of CrowdStrike's provisioning of the Offerings set forth in the Agreement.

1.1.15 **"Swiss-U.S. Data Privacy Framework Program"** or **"Swiss-U.S. DPF"** means the transfer mechanism that enables participating organizations to Process Customer Personal Data ("**Swiss Customer Personal Data**") in the United States in accordance with the Federal Act on Data Protection of 25 September 2020 as amended;

1.1.16 **"UK Extension to the EU-U.S. DPF"** means the transfer mechanism that enables participating organizations to Process Customer Personal Data originating from the United Kingdom ("**UK"**) ("**UK Customer Personal Data**") in the U.S. in accordance with Art. 45 of the UK GDPR.

1.1.17 "**UK GDPR**" means the UK Government approved and updated Data Protection Act 2018 including all the clauses from the EU-GDPR being the basis upon which Processing of Personal Data would be judged within the UK.

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

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

2. Processing of Customer Personal Data

2.1 CrowdStrike shall:

2.1.1 Process Customer Personal Data only on Customer's documented instructions, as set out in the Agreement and this DPA, including Customer providing instructions via APIs made available by CrowdStrike with the Offerings, and as required by Applicable Laws (the "**Documented Instructions**"). Any additional or alternate instructions, having an impact to the Offerings must be agreed upon by the Parties separately in writing; and

2.1.2 Unless prohibited by Applicable Law, inform the Customer if CrowdStrike determines that: (i) Customer's instructions conflict with Applicable Laws; or (ii) Applicable Laws require any Processing contrary to the Customer's instructions.

2.2 Customer shall:

2.2.1 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; and

2.2.2 Defend and indemnify CrowdStrike, CrowdStrike Affiliates, and CrowdStrike Subprocessors for any claim brought against any one or more of them arising from an allegation of Customer's breach of this Section, whether by a Data Subject or a government authority. In the event of such a claim, the Parties shall follow the process set forth in the Agreement for Customer to defend and indemnify CrowdStrike and if none, then CrowdStrike will: (a) notify Customer of such claim, (b) permit Customer to control the defense or settlement of such claim; provided, however, Customer shall not settle any claim in a manner that requires CrowdStrike to admit liability or make any changes with respect to the Offerings without CrowdStrike's prior written consent, and (c) provide Customer with reasonable assistance in connection with the defense or settlement of such claim, at Customer's cost and expense. In addition, CrowdStrike may participate in the defense of any claim, and if Customer is already defending such claim, CrowdStrike's participation will be at CrowdStrike's expense. This provision does not diminish Customer or Data Subject's rights under Applicable Laws related to CrowdStrike's adherence to its obligations under Applicable Laws.

3. CrowdStrike Personnel

CrowdStrike shall implement appropriate security controls designed to ensure that:

3.1 Access to Customer Personal Data within CrowdStrike or its Subprocessors' control is strictly limited to those individuals who need to know/access the relevant Customer Personal Data as reasonably necessary for the purposes outlined in this DPA, the Agreement or as required under Applicable Laws; and

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

4. Security

4.1 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 in Exhibit B that are designed to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in Applicable Laws.

4.2 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.

5. Sub-Processing

5.1 To the extent required under Applicable Laws, Customer specifically authorizes CrowdStrike to use those Subprocessors already engaged as of the date of this DPA and listed at: CrowdStrike Subprocessors. In addition, and subject to Section 5.3, Customer generally authorizes CrowdStrike's engagement of other third parties as Subprocessors ("**New Subprocessor(s)**").

5.2 CrowdStrike shall provide notice of a New Subprocessor to the Customer at least 30 days prior to CrowdStrike's use of the New Subprocessor to Process Customer Personal Data, through the applicable CrowdStrike Offering or platform, where Customer may elect to subscribe to such notices. Customers may also sign up for email notifications at https://www.crowdstrike.com/Subprocessor-notification/. Customer is responsible for ensuring that its notification email addresses remain current. During the notice period, Customer may object to a New Subprocessor in writing and CrowdStrike may, in its sole discretion, attempt to resolve Customer's objection, including providing the Offerings without use of the New Subprocessor. If (a) CrowdStrike provides Customer written notice that it will not pursue an alternative, or (b) such an alternative cannot be made available by CrowdStrike to Customer within 90 days of Customer providing notice of its objection, then in either case, and notwithstanding anything to the contrary in the Agreement or Order, Customer may terminate the Agreement or Order to the extent that it relates to the Offerings which require the use of the New Subprocessor.

5.3 With respect to each Subprocessor, to the extent required under Applicable Laws, CrowdStrike shall:

5.3.1 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;

5.3.2 Have a written contract between CrowdStrike and Subprocessor with that obligates the Subprocessor to provide 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;

5.3.3 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;

5.3.4 Maintain copies of the agreements with Subprocessors and make these reasonably available upon Customer's written request. To the extent necessary to protect Confidential Information, CrowdStrike may redact the copies prior to sharing with Customer; and

5.3.5 Notify Customer of Subprocessor's relevant failure to comply with obligations set out by Applicable Laws and this DPA where CrowdStrike has received notice of such.

6. Data Subject Rights

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

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

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

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

6.2.3 Reasonably assist Customer through appropriate technical and organizational measures to fulfill 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.

7. Personal Data Breach

7.1 Upon CrowdStrike becoming aware of any Personal Data Breach affecting Customer Personal Data, CrowdStrike shall without undue delay notify Customer of such Personal Data Breach. To the extent known, CrowdStrike shall provide Customer with sufficient information to meet obligations under Applicable Laws to report or inform Data Subjects about the Personal Data Breach.

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

8. Obligations to Assist Customer

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

8.1 Necessary data protection impact assessments required of Customer by Applicable Laws;

8.2 Consultation with or requests of a competent data protection authority;

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

9. Deletion of Customer Personal Data

9.1 Upon termination of the Offerings to Customer and pursuant to the Agreement:

9.1.1 Customer Personal Data will be deleted within 90 days of the Offerings being deprovisioned unless the retention of Customer Personal Data is required under Applicable Laws or the Agreement.

9.1.2 Upon Customer's written request, CrowdStrike shall:

9.1.2.1 Make Customer Personal Data available for return to Customer, where such a request has been made prior to deletion by CrowdStrike, by providing Customer with a reasonable means by which Customer can retrieve Customer Personal Data from the Offerings; and

9.1.2.2 Provide written confirmation that Customer Personal Data was deleted.

10. Audit Rights

10.1 Subject to Sections 10.2 to 10.4 and upon Customer's written request, CrowdStrike shall make available to Customer information necessary to demonstrate compliance with Applicable Laws and this DPA.

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

10.3 Information and audit rights of the Customer only arise under Section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Laws.

10.4 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.

11. Cross-Border Transfers of Customer Personal Data

At the time of Order placement, Customer has the option to designate the cloud-hosting region (either the EU or US) where Customer Personal Data will be physically stored within CrowdStrike Systems. Independent of the hosting location, CrowdStrike may Process Customer Personal Data internationally where CrowdStrike and Subprocessors have operations. Whenever Customer Personal Data is a Restricted Transfer, each Party will ensure such Restricted Transfer complies with Applicable Laws.

11.1 **EU Customer Personal Data**. CrowdStrike's Processing of EU Customer Personal Data in the U.S. shall adhere to the EU-U.S. Data Privacy Framework Principles. CrowdStrike is certified under the EU-US DPF. CrowdStrike's certification status is available in the U.S. Department of Commerce's Data Privacy Framework List.

In the event that CrowdStrike is required to adopt an alternative transfer mechanism pursuant to Chapter V of the EU GDPR for Processing EU Customer Personal Data in the U.S other than the EU-U.S. DPF, then the Parties agree that SCCs as set forth in Exhibit D shall apply. Notwithstanding the foregoing, the SCCs will not apply to the Processing of EU Customer Personal Data if CrowdStrike has adopted Binding Corporate Rules for Processors, as defined by Article 47 of the EU GDPR.

11.2 **UK (and Gibraltar) Customer Personal Data**. CrowdStrike's Processing of UK (and Gibraltar) Customer Personal Data in the U.S. shall adhere to the UK Extension to the EU-U.S. DPF approved by the UK

government in its UK Adequacy Decision. CrowdStrike is certified under the UK Extension to the EU-US DPF. CrowdStrike's certification status is available in the U.S. Department of Commerce's Data Privacy Framework List.

In the event that CrowdStrike is required to adopt an alternative transfer mechanism pursuant to Chapter V of the UK GDPR for Processing UK Personal Data in the U.S. other than the UK Extension to the EU-U.S. DPF, then the Parties agree that SCCs and the UK's International Data Transfer Addendum as set forth in Exhibit D shall apply. Notwithstanding the foregoing, the SCCs or the UK International Data Transfer Addendum will not apply to the Processing of UK (and Gibraltar) Customer Personal Data if CrowdStrike has adopted Binding Corporate Rules for Processors, as defined by Article 47 of the UK GDPR.

11.3 **Swiss Customer Personal Data**. CrowdStrike is certified under the Swiss-US DPF. CrowdStrike's certification status is available in the U.S. Department of Commerce's Data Privacy Framework List.

The Parties acknowledge that as of the DPA Effective Date, however, Personal Data cannot be received from Switzerland in reliance on the Swiss-U.S. DPF until the date on which Switzerland officially recognizes the United States as an Adequate Country. Therefore, CrowdStrike and Customer agree that that SCCs as set forth in Exhibit D shall apply.

11.4 **Argentinian Customer Personal Data.** Where the Restricted Transfer concerns Customer Personal Data originating from Argentina, the standard contractual clauses approved under Resolution No. 60-E/2016 and available at https://www.crowdstrike.com/legal/scc-ar/ will be incorporated into this DPA by reference and shall apply to the extent required under Applicable Laws and where this DPA does not provide adequate safeguards.

11.5 **Other Restricted Transfers.** Customer will notify CrowdStrike in writing if a Restricted Transfer involving Customer Personal Data requires privacy provisions not already included in this DPA. The Parties will promptly enter into a written amendment to include such provisions, but only to the extent required under Applicable Law and where this DPA does not provide adequate safeguards. For the avoidance of doubt, by adding such provisions, the Parties do not intend to grant third-party beneficiary rights to Data Subjects not otherwise provided under Applicable Law.

12. General Terms

12.1 **Governing Law and Jurisdiction**. 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.

12.2 **Order of Precedence**. 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) Applicable Laws, (2) this DPA, and then (3) the Agreement. For the avoidance of doubt, provisions in this DPA that merely go beyond Applicable Laws without contradicting them shall remain valid. The same applies to conflicts between this DPA and the Agreement where this DPA shall only prevail regarding the Parties' Personal Data protection obligations.

12.3 **Severability.** 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, should this not be possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

12.4 **No Third-Party Beneficiaries**. For the avoidance of doubt, by applying the provisions of this DPA, the Parties do not intend to grant third-party beneficiary rights to Data Subjects under this DPA when those Data Subjects would not otherwise benefit from such rights under the Applicable Laws.

12.5 Unless required by Applicable Laws, Customer shall exercise any right or seek any remedy on behalf of itself, its Affiliates, and any other Controller that Customer instructs CrowdStrike to process Customer Personal Data for under this DPA (collectively, the "Customer Parties"). Customer shall exercise any such rights or seek any such remedies in a combined manner for all Customer Parties together, rather than separately for each entity individually. To the maximum extent allowed by Applicable Laws, the limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability for all Customer Parties' claims arising out of or related to this DPA, and/or the Agreement against CrowdStrike and any CrowdStrike Affiliate(s). These limitations of liability and exclusions of damages apply to all claims, whether arising under contract, tort or any other theory of liability, and any reference to the liability of CrowdStrike means the aggregate liability of CrowdStrike and all CrowdStrike Affiliates together for claims by Customer and all other Customer Parties.

12.6 To the extent required by Applicable Laws, this Section is not intended to modify or limit (i) the Parties' liability for Data Subject claims made against a Party where there is joint and several liability, or (ii) 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 DPA Effective Date.

CROWDSTRIKE, INC.

DocuSigned by:

By: Drew Bagley
42403E92E9D844B...

Name: Drew Bagley

Title: VP, Privacy

Date: 2024-05-31

Send notices to:

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

Customer: _____

By: _____

Name: _____

Title: _____

Date: _____

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 EU-U.S. DPF Supplemental Principle #10, Article 28(3) of the EU GDPR, Article 28(3) of the UK GDPR, and Supplemental Principle #10 of the Swiss-U.S. DPF.

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

The subject matter, nature and duration of the Processing of the Customer Personal Data are set out in the Customer's documented instructions, the Agreement, and this DPA, and depend on the nature and scope of the Offerings, manner of receipt, collection, storage, use, dissemination, retention and erasure of Customer Personal Data.

Purpose for which the Personal Data is Processed on behalf of the Customer

The purposes of the Processing of the Customer Personal Data are to enable CrowdStrike and CrowdStrike's Subprocessors to provision and deliver the Offerings and perform their obligations as set forth in the Agreement, this DPA, and Customer's documented instructions or as otherwise agreed by the Parties in mutually executed written form.

Categories of Personal Data Processed including sensitive Personal Data

The Customer, rather than CrowdStrike, determines which categories of Personal Data exist and will be disclosed to and Processed by CrowdStrike in the provisioning of the Offerings because (i) Customer's infrastructure (e.g., endpoint, virtual machine and cloud environments) is unique in configurations and naming conventions, (ii) CrowdStrike enables the Customer to configure settings in APIs and the Offerings, and (iii) Customer controls (such as via deployment, configuration, and submission) which Customer content is uploaded, or is collected by, the CrowdStrike Offerings or the CrowdStrike Tools.

Categories of Data Subjects whose Personal Data is Processed

The Customer, rather than CrowdStrike, determines which Data Subjects' Personal Data is Processed by CrowdStrike through the Customer content put into, or collected by, the CrowdStrike Offerings or the CrowdStrike Tools.

Period for which the Personal Data will be Retained, or Criteria Used to Determine that Period

As set out in the Agreement, this DPA and Customer's documented instructions.

Subject Matter and Nature of the Processing with respect to Subprocessors

CrowdStrike maintains an up-to-date list of Subprocessors including name, contact details, processing and address, available to registered users of the Falcon platform at: https://falcon.crowdstrike.com/support/documentation/34/crowdstrike-products-and-services-third-party-Subprocessors-of-personal-data.

EXHIBIT B

Information Security Controls for CrowdStrike Systems

Security Control Category	Description
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing CrowdStrike's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data. b. Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions.
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls. b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur. c. Document formal risk assessments. d. Review formal risk assessments by appropriate managerial personnel. e. Review cloud service agreements and complete risk assessments before engaging with cloud service providers.
3. Information Security Policies	a. Create information security policies, approved by management, published and communicated to all employees and relevant external parties. b. Review policies at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. c. Maintain policies that outline the processes that are required for the acquisition, use, and management of cloud services.
4. Human Resources Security	a. Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Data or relevant CrowdStrike Systems, subject to local law. b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization.
5. Asset Management	a. Maintain policies establishing data classification based on data criticality and sensitivity. b. Maintain policies establishing data retention and secure destruction requirements. c. Implement procedures to clearly identify assets and assign ownership.

6. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Data, relevant CrowdStrike Systems and the organization's premises. b. Maintain controls designed to limit access to Personal Data, relevant CrowdStrike Systems and the facilities hosting the CrowdStrike Systems to authorized personnel. c. Review personnel access rights on a regular and periodic basis. d. Maintain physical access controls to facilities containing CrowdStrike Systems, including by using access cards or fobs issued to CrowdStrike personnel as appropriate. e. Maintain policies requiring termination of physical and electronic access to Personal Data and CrowdStrike Systems after termination of an employee. f. Implement access controls designed to authenticate users and limit access to CrowdStrike Systems. g. Implement policies restricting access to the data center facilities hosting CrowdStrike Systems to approved data center personnel and limited and approved CrowdStrike personnel. h. Maintain dual layer access authentication processes for CrowdStrike employees with administrative access rights to CrowdStrike Systems. i. Identify security requirements or concerns involved in the use of cloud platforms.
7. Cryptography	a. Implement encryption key management procedures. b. Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest.
8. Physical Security	a. Require two factor controls to access office premises. b. Register and escort visitors on premises. c. Maintain policies to restrict physical areas such as server rooms and IT equipment rooms to unauthorized people. d. Implement appropriate surveillance systems to prevent unauthorized access to intruders to sensitive physical premises.
9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources. b. Contract with qualified independent 3rd parties to perform periodic network and application penetration testing. c. Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests. d. Implement restrictions to prevent employees from accessing external websites that may contain viruses, phishing materials, or other types of illegal information. e. Perform proactive network monitoring that seeks to prevent incidents before they happen with reactive efforts to form an end-to-end information security and incident resolution strategy. f. Monitoring is carried out in line with regulatory requirements or prevailing legislation and records are retained in accordance with company retention policy .
10. Communications Security	a. Maintain a secure boundary using firewalls and network traffic filtering. b. Require internal segmentation to isolate critical systems from general purpose networks. c. Require periodic reviews and testing of network controls.
11. System Acquisition, Development and Maintenance	a. Assign responsibility for system security, system changes and maintenance. b. Test, evaluate and authorize major system components prior to implementation.

	c. Establish policies that govern how configurations are implemented across the organization. d. Implement configuration management policies for both new systems and hardware, and any that are already in use. e. Maintain and store configurations, including keeping an audit trail of any amendments or new installations, in line with a published change management process. f. Secure software principles should be followed both for coding projects and for software reuse operations. g. Monitor evolving real-world security threats and with the most recent information on known or potential software security vulnerabilities. h. Implement and configure software development tools to ensure the security of all code created.
12. Supplier Relationships	Periodically review available security assessment reports of vendors hosting the CrowdStrike Systems to assess their security controls and analyze any exceptions set forth in such reports.
13. Information Security Breach Management	a. Monitor the access, availability, capacity and performance of the CrowdStrike Systems, and related system logs and network traffic using various monitoring software and services. b. Maintain incident response procedures for identifying, reporting, and acting on Security Breaches. c. Perform incident response table-top exercises with executives and representatives from across various business units. d. Implement plan to address gaps discovered during exercises. e. Establish a cross-disciplinary Security Breach response team.
14. Business Continuity Management	a. Design business continuity with goal of 99.9% uptime SLA. b. Conduct scenario based testing annually. c. Maintain policies to maintain business continuity following disruption or a critical event. d. Maintain policies requiring Recovery Time Objectives (RTO) and overall business impact analysis (BIA). e. Maintain a BIA that specifies what ICT services and functions are required to achieve recovery, including individual performance and capacity requirements. f. Implement processes and plans to ensure ICT services are resilient and adequate to contribute towards recovery of critical processes and systems, before, during and after disruption.
15. Compliance	a. Establish procedures designed to ensure all applicable statutory, regulatory and contractual requirements are met.
16. Threat Intelligence	a. Maintain awareness of the threat environment so that mechanisms to collect and analyze these threats and determine the proper actions that can be taken to protect information security. b. Implement procedures to be able to respond and recover appropriately if something adverse were to happen; and that the security posture is appropriate for the threat environment. c. Conduct periodic reviews of the threat environment by reviewing reports from government agencies, other organizations and/or industry associations. d. Identify relevant threat sources (e.g., insiders, competitors, criminals, terrorist groups).

	e. Analyze current events and past events to determine possible new attack vectors and trends. f. Create defenses that can be used to mitigate the effect of threat to information security. g. Consider strategic, tactical and operational threat intelligence.
17. Information Deletion/Data Masking and Data Leakage Prevention	a. Configure internal systems to delete data and information in accordance with retention policy. b. Maintain specialized deletion utility applications, verifiable deletion specialists and third party service providers. c. Implement data masking techniques that reveal the minimum amount of data to anyone that uses it. d. Maintain policies that protect Personal Data and safeguard the identity of the individuals about whom it holds data. e. Classify data in line with recognized industry standards in order to assign varying levels of risk levels across the board. f. Monitor information that is accessed, transferred or extracted by unauthorized internal and external personnel and systems, or malicious sources. g. Implement Data leakage prevention tools in accordance with regulatory requirements and legislation that deals with user privacy.

EXHIBIT C
California Personal Information Processing Exhibit

This California Personal Information Processing Exhibit ("**CA Exhibit**") applies to the extent that CrowdStrike is Processing Customer's California Consumer Personal Information.

1. Definitions

1.1 In this CA Exhibit, "**Regulations**" means applicable regulations promulgated by the California Privacy Protection Agency, as amended.

1.2 The terms "**Business**," "**Business Purpose**," "**Collects**," "**Consumer**," "**Contractor**," "**Person**," "**Personal Information**," "**Sell,**" "**Service Provider**," and "**Share**," shall have the meaning set forth in the CCPA.

2. Terms

2.1 The Agreement documents the Business Purpose for which CrowdStrike is processing the Personal Information. Customer discloses Personal Information to CrowdStrike only for such limited and specified Business Purpose.

2.2 The Parties agree that Customer is a Business and CrowdStrike is a Service Provider.

3. Service Provider and/or Contractor Obligations and Restrictions

3.1 In respect of the Personal Information Processed in the course of fulfilling the Business Purpose to Customer, CrowdStrike:

3.1.1 shall not sell or share Personal Information it collects pursuant to the Agreement;

3.1.2 shall not retain, use or disclose the Personal Information it collects pursuant to the Agreement for any purpose other than the Business Purpose, or as otherwise permitted by the CCPA and the Regulations;

3.1.3 shall not retain, use or disclose the Personal Information it collects pursuant to the Agreement for any commercial purpose other than the Business Purpose, unless expressly permitted by the CCPA or the Regulations;

3.1.4 shall not retain, use or disclose the Personal Information it collects pursuant to the Agreement outside the direct business relationship between Customer and CrowdStrike, unless expressly permitted by the CCPA or the Regulations. Specifically, CrowdStrike shall not combine or update Personal Information with Personal Information it has received from another source or collected from its own interaction with the Consumer, unless expressly permitted by the CCPA or these Regulations.

3.1.5 shall comply with all applicable sections of the CCPA and the Regulations, including - with respect to the Personal Information that it collects pursuant to the Agreement - provision of the same level of privacy protection as required of Businesses by the CCPA and the Regulations;

3.1.6 shall notify Customer if CrowdStrike determines that it can no longer fulfill its obligations under the CCPA or the Regulations;

3.1.7 may, subject to the Agreement, engage another Person to assist CrowdStrike to fulfill the Business Purpose; provided, however, that CrowdStrike must enter into a written agreement with a Person that complies with this CA Exhibit, the CCPA and the Regulations, including Section 7051(a); and

3.1.8 shall inform Customer of any Consumer request made to CrowdStrike regarding Personal Information with which Customer must comply, and at Customer's request and cost, assist Customer with its obligation to respond to verifiable requests from Consumers.

3.2 In respect of the Personal Information that Customer provides to CrowdStrike to fulfill the Business Purpose, Customer has the right, upon advance written notice, to take reasonable and appropriate steps to ensure that CrowdStrike uses the Personal Information in a manner consistent with the Business's obligations under the CCPA and the Regulations.

3.3 If, after completing the assessment described in Section 3.2, Customer determines that CrowdStrike may be in violation of its obligations in this CA Exhibit, the CCPA or the Regulations, then upon advance written notice, Customer has the right to take reasonable and appropriate steps to stop and remediate CrowdStrike's unauthorized use of Personal Information.

4. Changes in the CCPA

4.1 In the event of a change to the CCPA whereby the provisions of this CA Exhibit are materially affected or compliance with the terms of this CA Exhibit becomes impractical, the Parties shall negotiate in good faith to agree to an updated CA Exhibit.

4.2 Any conflict between the terms of this CA Exhibit, the DPA, or the Agreement related to the processing of Customer Personal Data are resolved in the following order of priority: (1) the CCPA, (2) this CA Exhibit, (3) the DPA, and then (4) the Agreement. For the avoidance of doubt, provisions in this CA Exhibit that merely go beyond the CCPA without contradicting them shall remain valid. The same applies to conflicts between this CA Exhibit, the DPA and the Agreement, where this Exhibit shall only prevail regarding the Parties' Personal Information protection obligations.

EXHIBIT D
EU STANDARD CONTRACTUAL CLAUSES

In the event that Applicable Laws require CrowdStrike to adopt an alternative transfer mechanism to replace either the EU-U.S. DPF or the UK Extension to the EU DPF, then the Parties agree to incorporate by reference into this DPA the Standard Contractual Clauses available at https://www.crowdstrike.com/legal/scc-eu/ and as detailed below, to govern the transfer of Customer Personal Data from the EU/EEA and/or the UK to the U.S.

In addition, the Parties agree that such SCCs, as detailed below, shall govern the transfer of Customer Personal Data from Switzerland to the U.S as of the DPA Effective Date.

The terms **"Data Exporter"** and **"Data Importer"** shall have the same meaning as in the standard contractual clauses.

The Parties acknowledge and agree:

1. CrowdStrike will be a Data Importer acting as Processor of Customer Personal Data (or Subprocessor, as the context below requires) to a Restricted Transfer.

2. Where Customer will be a Data Exporter acting as Controller, Module 2 (Controller to Processor) will apply to a Restricted Transfer.

3. Where Customer will be a Data Exporter acting as a Processor, Module 3 (Processor to Processor) will apply to a Restricted Transfer. Taking into account the nature of the Processing, Customer agrees that it is unlikely that CrowdStrike will know the identity of Customer's Controllers because CrowdStrike has no direct relationship with Customer's Controllers and therefore, Customer will fulfill CrowdStrike's obligations to Customer's Controllers under the Module 3 (Processor to Processor) Clauses.

4. Where CrowdStrike will be the Data Importer Processing Customer Personal Data in its own discretion as Controller in the provisioning of the Offerings agreed, e.g., for administering the Agreement, Module 1 (Controller to Controller) will apply to the relationship between Customer (Data Exporter) and CrowdStrike (Data Importer).

5. Specific Clauses of the SCCs

5.1 SCC Clause 8.1 (Instructions). The Parties acknowledge that Customer's instructions may not conflict with the Offerings. Any additional or alternate instructions, having impact to the Offerings, must be agreed upon separately between the Parties. The following is a mutually agreed instruction: (a) Processing of Customer Personal Data 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 (e.g., via email) where such instructions are consistent with the terms of the Agreement.

5.2 SCC Clause 8.5 (Duration of processing and erasure or return of data). Customer acknowledges and expressly agrees that the process described in Section 9 of this DPA shall govern the fulfillment of requirements related to data erasure and return of Customer Personal Data.

5.3 SCC Clause 8.9(c, d) (Audit). The Parties agree the audits described in Clause 8.9(c, d) shall be carried out in accordance with Section 10 of this DPA. To the extent Clause 8.9(c, d) additionally requires CrowdStrike's facilities be submitted for physical inspection, Customer may contact CrowdStrike through prior written notice to request an on-site audit of the procedures relevant to the protection of Customer Personal Data. Before the commencement of any such on-site audit, Customer 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 shall promptly notify CrowdStrike with information regarding any non-compliance discovered during the course of an audit. In order to align efforts and to keep actions consistent, Customer shall be the relevant body carrying out audits towards CrowdStrike for itself and Controllers, where Customer acts as a Processor under the instruction of a Controller with which CrowdStrike has no direct relationship.

5.4 SCC Clause 9 (Use of Subprocessors). The Parties agree to and choose option 2 (general written authorization) and specify the time period for notices as set forth in Section 5 of this DPA. Where Customer is a Processor to Customer Personal Data, Customer agrees and warrants to be duly authorized to receive and pass on information about CrowdStrike's New Subprocessor(s) to Controllers with whom CrowdStrike has no direct relationship, assisting CrowdStrike to meet its obligation under Clause 9 towards the Controllers.

5.5 SCC Clause 11(a) (Redress). The Parties agree that the option provided shall not apply.

5.6 SCC Clause 13 (Supervision). The Parties agree that the options in Clause 13 will be selected in line with the Customer's main establishment in accordance with the GDPR.

5.7 SCC Clause 17 (Governing Law). The Parties agree to and choose Option 2; where such law does not allow for third-party beneficiary rights, the Parties agree that this shall be the law of the Netherlands.

5.8 The Exhibits A and B of this DPA substitutes the Annexes I to III required under the Standard Contractual Clauses providing the mandatory information under Applicable Laws.

6. Transfers from Switzerland

6.1 Where the Restricted Transfer concerns Customer Personal Data originating from Switzerland, in line with the Swiss Federal Data Protection and Information Commissioner's statement as of August, 27, 2021, the following additional requirements shall apply to the extent the Customer Personal Data transferred is exclusively subject to the Swiss Data Protection Act (FADP) or 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 SCC Clause 18 (c); (ii) Insofar as the data transfers are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP; and (iii) Insofar as the data transfers 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.

7. Transfers from the UK (and Gibraltar)

7.1 Where the Restricted Transfer concerns Customer Personal Data originating from the UK or Gibraltar, the Standard Contractual Clauses will apply subject to the conditions set out by the UK Information Commissioner Office's ("ICO") International Data Transfer Addendum to the Standard Contractual Clauses ("IDTA") that shall be incorporated herein by reference. The Parties acknowledge and agree that:

7.1.1 Table 1 of the IDTA. The Parties' details and contact information in Table 1 of the IDTA shall be the same as the information included in Annex I of the SCCs. The start date shall be the same as that set forth in the SCCs.

7.1.2 Table 2 of the IDTA. The Standard Contractual Clauses agreed to in this Exhibit D include the IDTA's selected modules, clauses, optional provisions and Appendix Information.

7.1.3 Table 3 of the IDTA. "Appendix Information" means the information which must be provided for the selected modules of the UK Addendum is set as follows:

I. Exhibit A (Description of Processing and Transfer);
II. Exhibit B (List of Parties);
III. Exhibit C (Competent Supervisory Authority);
IV. Exhibit D (Technical and Organizational Measures); and
V. Exhibit E (List of Subprocessors, if any).

7.1.4 Table 4 of the IDTA. The Parties agree that neither the Data Importer nor the Data Exporter may end the UK Addendum as set out in Section 19 of the IDTA.

8. Notwithstanding anything to the contrary in the Agreement, this DPA or this Exhibit D, the SCCs and/or the IDTA will not apply to the Processing of Customer Personal Data if CrowdStrike has adopted Binding Corporate Rules for Processors, as defined by Applicable Laws.