HUMAN

PRIOR VERSION: December 11, 2024

CUSTOMER/ HUMAN SECURITY, INC.
DATA PROCESSING ADDENDUM

"**Customer**"	As defined in the Agreement between Customer and HUMAN Notices to be provided Attn: Legal Notices of Incidents to be provided: Business Contact listed in accompanying Order Form
"**HUMAN**"	Human Security, Inc., a Delaware corporation, 841 Broadway, 2nd Floor, New York, NY 10003 Notices to be provided Attn: General Counsel Notices of Incidents to be provided: privacy@humansecurity.com and legal@humansecurity.com

This Data Processing Addendum ("**DPA**") (including its appendices) is made by and between Customer and HUMAN (each a "**Party**"; collectively the "**Parties**") and entered into as of the Effective Date of the Agreement (as defined below) for the purpose of governing the Processing by HUMAN of Personal Data (both as defined below) on behalf of Customer pursuant to the Service Agreement entered into between HUMAN and Customer (the "**Agreement**"). This DPA is incorporated into and made subject to the terms of the Agreement. In the event of a conflict between the terms of this DPA and the terms of the Agreement, the terms of the DPA shall prevail. In case of a conflict or inconsistency between the operative provisions in this DPA and the Standard Contractual Clauses in Appendix 3, if applicable, the Standard Contractual Clauses shall supersede and take precedence.

1. Definitions. Definitions applicable to the DPA are as follows:

1.1 "**Applicable Laws**" means any law or regulation concerning information privacy or security applicable to HUMAN's Processing of the Personal Information to provide Services under the Agreement, including to the extent applicable to the Processing, (i) EU GDPR, (ii) UK GDPR, and (iii) any United States privacy laws (such as Cal. Civ. Code § 1798.100 *et seq,* Va. Code § 59.1-575 *et seq*., Colorado Rev. Stat. §§ 6-1-1301 *et seq*., Connecticut Public Act No. 22-15, Iowa Code §§ 715D.1 *et seq*., and Utah Code Ann. §§ 13-61-101 *et seq*.) and all implementing regulations.

1.2 "**Authorized Employees**" means HUMAN's employees who have a need to know or otherwise access Personal Data to enable HUMAN to perform its obligations under the Agreement.

1.3 "**Authorized Persons**" means (i) Authorized Employees; and (ii) HUMAN's contractors, agents, and auditors who have a need to know or otherwise access Personal Data to enable HUMAN to perform the Services.

1.4 **"Controller"** has the meaning given to "controller", "data controller", "business" or a similar term used to define the Party that, alone or jointly with others, determines the means and purpose of the Processing of Personal Data in accordance with Applicable Laws.

1.5 **"Customer Data**" means any information Processed by HUMAN (and/or its affiliates and/or Authorized Persons) in HUMAN's role as a Processor to Customer pursuant to the Agreement, including any Personal Data.

1.6 **"Data Subject"** has the meaning given to "data subject", "consumer" or similar term used to describe the individual who is the subject of the Personal Data in accordance with Applicable Laws.

1.7 "**EEA**" means the European Economic Area.

1.8 "**EU GDPR**" means the European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), as may be amended from time to time.

1.9 "**GDPR**" means, as applicable, the EU GDPR and/or the UK GDPR.

1.10 "**Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.11 "**Personal Data**" has the same meaning as personal data, "personal information," or similar terms used in Applicable Laws to describe information that identifies or relates to an individual who can be identified directly or indirectly from the data alone or in combination with other information in HUMAN's possession or control or that HUMAN is likely to have access to. For avoidance of doubt, the term Personal Data refer to Personal Data that is provided by Customer As well as Personal Data which is collected on behalf of Customer by HUMAN, and that is Processed by HUMAN

(and/or its affiliates and/or any Authorized Persons) in HUMAN's role as a Processor to Customer pursuant to the Agreement.

1.12 "**Processing**" or "**Process**" has the meaning given in accordance with Applicable Laws or absent such a definition, any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, storage, alteration, retrieval, use, disclosure, or otherwise making available, or destruction.

1.13 "**Processor**" has the meaning given to "processor," "data processor", "service provider," "contractor," or other terms used to describe the Party that Processes the Personal Data on behalf of the Controller in accordance with Applicable Laws.

1.14 "**Regulatory Authority**" means any court, tribunal, or governmental or other entity that has jurisdiction, under Applicable Laws, over the Agreement, the Services, Customer or HUMAN, including any foreign data protection authority with jurisdiction or oversight over the Applicable Laws.

1.15 "**Share**," "**Shared**," and "**Sharing**" have the meaning defined in the California Consumer Privacy Act (CCPA).

1.16 "**Sale**" and "**Selling**" have the meaning defined in the Applicable Laws.

1.17 **"Service Order**" means a written or online ordering document by which Customer purchases Services.

1.18 "**Services**" means the services provided to Customer pursuant to the Agreement.

1.19 "**Standard Contractual Clauses**" means, as applicable, the EEA Standard Contractual Clauses and/or the UK Standard Contractual Clauses as further defined in Appendix 3.

1.20 **Sub-Processor**" means a Processor engaged by HUMAN to carry out Processing on behalf of Customer.

1.21 "**UK GDPR**" means the United Kingdom Data Protection Act of 2018 and the United Kingdom General Data Protect Act and any successor legislation thereto.

In the event of a conflict in the meanings of defined terms in the Applicable Laws, the meaning from the law applicable to the Processing of Personal Data of the relevant Data Subject applies.

2. Standard of Care

2.1 **Limited Processing and Documented Instructions**. HUMAN shall comply with this DPA and be responsible for any authorized Processing of Personal Data while such Personal Data is under HUMAN's control or in its possession. HUMAN and Customer acknowledge and agree that for the purposes of this Agreement and Applicable Laws, Customer is either a Controller or a Processor and HUMAN is a Processor of any Personal Data. HUMAN shall Process Customer Data only on documented instructions from Customer. Customer instructs HUMAN to Process Customer Data for only the following limited and specific purposes: (i) Processing in accordance with the Agreement and applicable Service Orders (if any), including Appendix 1, and to the extent necessary to perform the Services; and (ii) Processing to comply with other documented instructions provided by Customer where such instructions are consistent with the terms of the Agreement. If Customer is a Data Processor, Customer represents and warrants that its instructions and actions with respect to the Personal Data, including appointing HUMAN as an additional Processor, have been and are authorized by the relevant Data Controller in accordance with Applicable Laws. HUMAN shall not (i) collect, use, retain, disclose, Sell, Share, rent, or otherwise make Personal Data available outside of the direct business relationship with Customer or for HUMAN's own commercial purposes or for the benefit of anyone other than Customer, except with Customer's prior written consent, (ii) Sell or Share Customer Data, (iii) retain, use, or disclose Customer Data for any purpose other than for the specific purpose of performing the services specified in Appendix 1 and this subsection 2.1, and (iv) combine Personal Data received from Customer with other Personal Data HUMAN received from or on behalf of another source, or collected from its own interactions with a Data Subject, to the extent prohibited by Applicable Laws. The Parties acknowledge and agree that the exchange of Personal Data between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this DPA. Notwithstanding the foregoing, HUMAN may use the Personal Data as follows to the extent permitted by Applicable Laws: (i) for its internal use to improve the quality of the Services provided by HUMAN, provided, however, that HUMAN does not use the Personal Data to build or modify a profile about a Data Subject or their household to use in providing services to a third-party, or cleaning or augmenting any Personal Data acquired from another source; (ii) to detect Incidents, or to protect against fraudulent or illegal activity; and (iii) as otherwise explicitly permitted under Applicable Law. The Agreement and this DPA are Customer's complete instructions to HUMAN for the Processing of Personal Data. Where HUMAN receives an instruction from Customer that, in its reasonable opinion, infringes Applicable Laws, HUMAN shall immediately inform Customer, and shall be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under Applicable Laws. In the event HUMAN is required under Applicable Laws to Process Customer Data in excess of Customer's documented instructions, HUMAN shall notify Customer of such a requirement, unless Applicable Laws prohibit such notification, in which case it will notify Customer as soon as the Applicable Laws permit it to do so.

2.2 **Responsibilities**. HUMAN shall in accordance with Customer's written instructions: (i) implement reasonable and appropriate measures appropriate to the risk of Processing the Personal Data as required by Applicable Laws, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by HUMAN ; (ii) apply the security measures set forth in Appendix 2 to the Processing of Customer Data; (iii) notify Customer if HUMAN is unable to comply with the obligations in this DPA or Applicable Laws, in which case Customer shall be entitled to suspend the Processing of Personal Data by HUMAN and/or terminate the Agreement upon written notice to HUMAN if HUMAN is unable to bring itself into compliance within a reasonable period of time, or otherwise take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data; and (iv) ensure that Authorized Persons are informed of the confidential nature of the Customer Data, have executed confidentiality agreements, and are subject to a duty of confidentiality with respect to Customer Data.

3. Mechanism for Processing.

3.1 **Compliance with Laws**. HUMAN and Authorized Persons will (i) Process Personal Data in compliance with all Applicable Laws, (ii) comply with the obligations of the Applicable Laws, (iii) provide the same level of protection for the Personal Data as is required of Customer under Applicable Laws, (iv) provide Customer with all reasonably-requested assistance to enable Customer to fulfill its own obligations under the Applicable Laws, and (v) understand and comply with this DPA. Upon the reasonable request of Customer, HUMAN shall make available to Customer all information in HUMAN's possession necessary to demonstrate HUMAN's compliance with this subsection. Customer also has the right to take reasonable and appropriate steps to ensure that HUMAN uses Customer Data consistent with Customer's obligations under Applicable Laws.

3.2 **Customer's Processing of Personal Data.** Customer is responsible for Processing Personal Data in accordance with the requirements of all Applicable Laws. Customer shall comply with all Applicable Laws, and Customer's instructions for the Processing of Personal Data shall comply with all Applicable Laws. Customer shall ensure that Customer has provided or shall provide any necessary notices to Data Subjects and has obtained or shall obtain all consents and rights necessary for HUMAN to Process Personal Data in accordance with this DPA and the Agreement. Customer represents and warrants that HUMAN's Processing in accordance with Customer's instructions shall not cause HUMAN to be in breach of any Applicable Laws or Customer's policies and procedures.

3.3 **Changes to Processing of Personal Data**. Appendix 1, Part B to this DPA sets out the details of HUMAN's Processing of Personal Data. Customer may amend Appendix 1, Part B on written notice to HUMAN from time to time as Customer reasonably considers necessary to meet any applicable requirements of Applicable Laws. Without limiting any rights or obligations of the Parties conferred or imposed under the Agreement, nothing in Appendix 1 (including as amended pursuant to this Section 3.3) confers any right or imposes any obligation on any Party to this DPA.

4. Actions and Access Requests

4.1 **Assistance**. Each Party shall reasonably assist the other in the event of any action by any Regulatory Authority in relation to the Services, if and to the extent that such action relates to the collection, maintenance, use, Processing or transfer of Personal Data under this DPA, at the requesting Party's cost and expense.

4.2 **Third Party Requests**. HUMAN shall assist Customer by appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to third party requests, including, but not limited to, requests of Regulatory Authorities, at Customer's cost and expense. HUMAN shall (i) promptly notify Customer if it receives a third party request related to Customer Data unless prohibited by Applicable Laws; and (ii) not respond to that third party request related to Customer Data except on the documented instructions of Customer or as required by Applicable Laws to which it is subject, in which case HUMAN shall, to the extent permitted by Applicable Laws, inform Customer of that legal requirement before it responds to the third party request. Should any Regulatory Authority to which Customer is subject require or request a security audit or review of HUMAN, HUMAN shall, with Customer's full involvement (including Customer's attendance at any related meetings with federal, state or other government officials), cooperate with any such requirement or request and provide to Customer, its authorized representatives, and/or an independent inspection body designated by Customer, on reasonable notice, (a) access to HUMAN's information processing premises and records, and (b) reasonable assistance and cooperation of Authorized Persons for the purpose of auditing HUMAN's compliance with its obligations under this DPA. For the avoidance of doubt, any additional expenses that shall arise as a result of regulatory or compliance requirements for Customer shall be covered by Customer entirely.

4.3 **Data Subject Requests**. Except as required by Applicable Laws, HUMAN shall not respond to a Data Subject who requests to exercise their data protection rights under Applicable Laws in connection with their Personal Data other than at the written instruction of the Customer. Customer shall use commercially reasonable efforts to provide any necessary data or identifiable information to assist HUMAN in responding to data access requests. HUMAN shall not be responsible for fulfilling a data request without such assistance from Customer. Where required by Applicable Laws, HUMAN shall provide commercially

reasonable assistance to Customer for the fulfillment of Customer's obligations to respond to Data Subject rights requests pursuant to the Applicable Laws. If, upon a Data Subject's request for access to their Personal Data, HUMAN is unable to produce or delete the Personal Data requested as a result of an act or omission of HUMAN in violation of its obligations under this DPA, HUMAN shall be responsible for all costs associated with or arising from its inability to produce the Personal Data.

4.4 **Data Protection Impact Assessment**. Upon Customer's request, HUMAN shall provide Customer with reasonable assistance needed to fulfil Customer's obligations under Applicable Laws to carry out a data protection impact assessment related to the Processing of Personal Data, taking into account the nature of the Processing, at Customer's cost and expense.

4.5 **Prior Consultation**. Upon Customer's request, HUMAN shall provide Customer with reasonable assistance with any prior consultations to any Regulatory Authority of Customer which are required under Applicable Laws, such as Article 36 of the GDPR, at Customer's cost and expense.

5. Security Breach Procedures

5.1 **Notice Process**. HUMAN shall notify Customer without undue delay (after any appropriate internal investigations) after becoming aware of an Incident involving Personal Data to the extent required by Applicable Laws or other unlawful Processing that would require HUMAN to notify Customer under Applicable Laws. In the event of such an Incident:

5.1.1 HUMAN shall provide Customer with: (a) the nature of the Incident; (b) the types of potentially compromised Personal Data; (c) the duration and expected consequences of the Incident; (d) the date the Incident took place, and the date on which the HUMAN discovered the Incident; and (e) the mitigation or remediation measures taken or planned in response to the Incident.

5.1.2 HUMAN shall provide reasonable assistance to Customer so that Customer can comply with Customer's obligations to notify a Regulatory Authority and/or Data Subjects of the Incident, taking into account the nature of Processing and the information available to HUMAN.

5.1.3 Customer is solely responsible for complying with data incident notification requirements applicable to Customer and fulfilling any third-party notification obligations related to any Incident.

5.1.4 HUMAN shall not publicly disclose any information regarding the Incident that identifies Customer without Customer's prior express written consent; provided that HUMAN may disclose the occurrence of any Incident as necessary to comply with Applicable Laws.

5.2 **Mitigation and Remedy**. HUMAN shall, in accordance with Applicable Laws, take reasonable steps as are directed by Customer to mitigate and remedy, and to assist in the investigation of, any Incident caused by HUMAN's violation of this DPA or Applicable Laws and prevent a recurrence thereof.

6. Attestations or Certifications. Upon the request of Customer, no more than once per year, HUMAN shall provide a copy of its current attestation of compliance to any industry or compliance standards maintained by HUMAN. The reports, information, attestations and certifications provided to Customer pursuant to this Section shall be HUMAN's confidential information under the Agreement.

7. Audit Rights. Customer shall have the right, upon prior written notice, to monitor HUMAN's compliance with this DPA through reasonable and appropriate steps, including an annual audit which may include manual reviews, automated scans, internal or third-party assessments, or other technical and operational testing. HUMAN shall cooperate with any such audit initiated by Customer, provided that such audit will not unreasonably interfere with the normal conduct of HUMAN's business. Unless the audit reveals a breach by HUMAN of this DPA or Applicable Laws, Customer shall bear the costs of the audit.

8. Deletion of Personal Data. At any time during the term of the Agreement, at Customer's written request or upon the termination or expiration of the Agreement for any reason, HUMAN shall, and shall instruct all Authorized Persons to, promptly and securely dispose of all copies of Personal Data unless the applicable law requires continued storage of all or portions of the Personal Data. Notwithstanding the foregoing, to the extent it is not commercially reasonable for HUMAN to remove Personal Data from archive or other backup media, HUMAN may retain Personal Data on such media in accordance with its backup or other disaster recovery procedures. In the event HUMAN retains Personal Data after the term of the Agreement, HUMAN shall continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Personal Data.

9. Data Transfers. HUMAN may, subject to this Section 9, process the relevant Client Data anywhere HUMAN or its Sub-processors maintain facilities or have a point of presence**.** With regard to Personal Data of a Data Subject in the EEA or United Kingdom, Customer authorizes HUMAN to transfer Personal Data from the EEA and/or the United Kingdom to the United

States through the protections provided by the Standard Contractual Clauses, herein incorporated by reference in accordance with Appendix 3. HUMAN will ensure that any Sub Processor agrees to comply with the appropriate Standard Contractual Clauses. Both Parties shall ensure compliance with the *Standard Contractual Clause Agreement* as set out at Appendix 3. In connection with the use of the Standard Contractual Clauses, the Parties further agree and acknowledge that: (i) sections of this DPA addressing the same or similar subject matter as the Standard Contractual Clauses may be used to satisfy the applicable requirements of the Standard Contractual Clauses; and (ii) if required, the Parties shall sign a copy of the Standard Contractual Clauses and take such further action as is required by Applicable Laws to ensure that the Standard Contractual Clauses are legally valid. Where HUMAN's Processing of Personal Data requires an onward transfer mechanism to lawfully transfer Personal Data from one jurisdiction to another, HUMAN will enter into the appropriate Standard Contractual Clauses or, at HUMAN's election, HUMAN will offer and comply with another mechanism that enables the lawful transfer of Personal Data to a third country in accordance with Article 45 or 46 of the GDPR.

10. Sub-Processors. Subject to Section 11, HUMAN may engage third-party Sub-Processors in connection with the provision of the Services provided that, before the Sub-Processor first Processes Personal Data, HUMAN: (a) enters into a written agreement with the Sub-Processor on terms at least as protective as those set out in this DPA as well as to comply with Applicable Laws, and (b) carries out adequate due diligence to ensure the Sub-Processor is capable of providing the level of protection for Personal Data required by this DPA. HUMAN shall provide Customer with a current list of the Sub-Processors that HUMAN has engaged in connection with the provision of Services upon Customer's request. HUMAN shall provide to Customer written notice of any change to the list of Sub-Processors at least thirty (30) days prior to the date the change takes effect.

11. Right to Object. Customer hereby grants HUMAN general written authorization to engage Sub-Processors in connection with the provision of the Services. HUMAN shall give Customer notice of the appointment of any new Sub-Processor through Customer's account dashboard. If Customer reasonably objects in writing to the use of a new Sub-Processor within forty-eight (48) hours of the notice date, then the Parties shall use good faith efforts to find a reasonable replacement in a mutually agreeable manner.

12. **Customer Instructions.** Customer acknowledges that HUMAN is reliant on Customer for direction concerning the extent to which HUMAN may Process Personal Data on behalf of Customer in performance of the Services. HUMAN shall not be liable under the Agreement for any claim or complaint brought by a Data Subject, Consumer or Regulatory Authority arising from any action or omission by HUMAN, to the extent that such action or omission results from Customer's instructions or failure to comply with its obligations under Applicable Laws.

13. Dispute. Governing Law. The Parties hereby submit to the choice of law and choice of venue and jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; *provided, however*, that with respect to any disputes under the GDPR only, the Parties agree that this DPA shall be governed by the laws of Ireland.

14. Compelled Disclosures. Any disclosure by HUMAN or its representatives of any of the Personal Data pursuant to applicable federal, state, or local law, regulation, or valid order issued by a court or governmental agency of competent jurisdiction (a "**Legal Order**") will be subject to the terms of this paragraph. Prior to making such a disclosure, HUMAN shall, to the extent permitted under the Legal Order, provide Customer with: (a) prompt written notice of such requirement so that Customer may seek, at its sole cost and expense, a protective order or other remedy; and (b) reasonable assistance, at Customer's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If, after providing such notice and assistance as required herein, HUMAN remains subject to a Legal Order to disclose any Personal Data, HUMAN shall make reasonable efforts to disclose no more than the portion of Personal Data which such Legal Order specifically requires HUMAN to disclose.

15. Liability. The liability of each Party under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Any reference to any "limitation of liability" of a Party in the Agreement shall be interpreted to mean the aggregate liability of a Party under the Agreement and this DPA.

Appendix 1 - Details of the Parties and Processing

A. List of Parties

Data exporter(s): the Customer designated in the Agreement entered into with Human Security, Inc.

Name and Address: As indicated in the Agreement

Activities relevant to the data transferred under the SCCs and this DPA: use of the Services in accordance with the Agreement.

Signature and Date: This Appendix 1 shall be deemed executed upon execution of the DPA.

Role: Data exporter's role is set forth in Section 2.1 of the DPA.

Data importer(s):

Name: Human Security, Inc. ("HUMAN")

Address: 841 Broadway, New York, New York 10003

Contact person's name, position, and contact details: legal@humansecurity.com; privacy@humansecurity.com

Signature and Date: This Appendix 1 shall be deemed executed upon execution of the DPA.

Role: Processor

B. Description of Processing and Transfer

The categories of Data Subject to whom the Personal Data relates

Data Subjects include the identified or identifiable individuals contained in data submitted to the Services by Customer.

Categories of Personal Data Processed and transferred

HUMAN Processes the limited Personal Data HUMAN needs to perform the particular Services, as instructed and/or authorized by Customer. Dependent on the products and as advised by the Customer, HUMAN may Process IP address, geolocation, device ID, pseudo device ID, mobile ID, user ID, session ID, visitor ID, full URL, name, phone number, account registration date, email address, usernames, passwords, and other log-in credentials.

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

HUMAN does not collect "sensitive categories" of Personal Data as such term is defined by EU GDPR.

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

HUMAN will Process Personal Data to the extent necessary to perform the Services pursuant to the Agreement and as further instructed by Customer in writing and as otherwise permitted by the Agreement and the DPA.

The nature and purpose of the Processing

HUMAN will Process Personal Data to provide the Services in accordance with the Agreement and the DPA.

Purpose(s) of the data transfer and further Processing

HUMAN will Process Personal Data to provide the Services in accordance with the Agreement and the DPA.

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 Personal Data is set out in the Agreement and this DPA. Personal Data is deleted based on the terms of the Agreement and this DPA, legal requirements related to data storage and if Personal Data is no longer needed to perform the Services and there is no lawful reason to keep it.

C. Sub-Processors

Third Party Service/Vendor	Purpose	Entity Country	Website
Amazon Web Services, Inc.	Data Hosting	410 Terry Avenue North Seattle, WA 98109-5210, USA	https://aws.amazon.com/
Fastly, Inc.	Content Delivery Network	475 Brannan Street San Francisco, CA 94107, USA	https://www.fastly.com
Google LLC	Data Hosting	1600 Amphitheatre Parkway Mountain View, CA 94043, USA	https://cloud.google.com/
Snowflake Inc.	Data Housing/Cloud Storage	106 E Babcock St. Bozeman, MT 59715, USA	https://snowflake.com
Equinix, Inc. (formally Packet Host)	Data Housing	1 Lagoon Drive, Fourth Floor Foster City, CA 94065, USA	https://equinix.com
Salesforce, Inc. /Slack Technologies, LLC	Customer Support	415 Mission Street, 3rd Floor San Francisco, CA 94105, USA	https://salesforce.com
Support Advisors, LLC	Security Operations Center	1 East Benton Street Aurora, IL 60505, USA	https://supporttechs.com
Akamai Technologies, Inc.	Content Delivery Network	145 Broadway Cambridge, MA 02142, USA	https://www.akamai.com
Cloudflare, Inc.	Content Delivery Network	101 Townsend St. San Francisco, CA 94107, USA	https://www.cloudflare.com

HUMAN may update this list from time to time in accordance with the terms of the DPA; please visit https://www.humansecurity.com/subprocessors-list for the up-to-date list of Sub-Processors.

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and this DPA.

D. Competent Supervisory Authority

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

For the EEA Standard Contractual Clauses, the competent supervisory authority is determined in accordance with Clause 13 of the EEA SCCs.

For the UK Standard Contractual Clauses, the competent supervisory authority is the UK Information Commissioner's Office.

Appendix 2 – Technical and Operational Measures
DATA SECURITY

This Data Security Appendix is made a part of the attached DPA between Customer and HUMAN. The Agreement and DPA, including without limitation this Data Security Appendix, reflects the Parties' agreement with regard to the Processing and safeguarding of Personal Data.

Implementation of the provisions of this Appendix by HUMAN shall be consistent with industry standards, where applicable. Unless otherwise stated, capitalized terms in this Appendix shall have the meanings set forth in the Agreement or DPA.

1. **Organizational Security Measures.**

1.1. Point of Contact. HUMAN shall appoint a representative to act as a point of contact for the Customer with respect to this Data Security Appendix. The representative shall be responsible for ensuring HUMAN's compliance with this Data Security Appendix.

1.2. Security Program. HUMAN has developed and implemented, and will regularly update and maintain as appropriate and needed: (a) a written and comprehensive information security program in compliance with Applicable Laws; and (b) reasonable policies and procedures designed to detect, prevent, and mitigate the risk of data security breaches or identify theft ("Security Program"). Specifically, such Security Program shall include, at a minimum and in addition to the items contained in Section 2 below:

1.2.1. A disaster recovery/business continuity plan that addresses ongoing access, maintenance and storage of Personal Data as well as security needs for backup sites and alternate communication networks.

1.2.2. Secure transmission and storage of Personal Data.

1.2.3. Personnel security and integrity, including background checks where consistent with applicable law.

1.2.4. Annual training to HUMAN's employees on how to comply with the HUMAN's physical, technical, and administrative information security safeguards and confidentiality obligations under Applicable Laws.

1.2.5. Quarterly review of authentication and access control mechanisms over Personal Data, media, applications, operating systems and equipment.

1.2.6. Data retention and destruction procedures in accordance with Section 8 of the DPA.

1.3. Training. HUMAN shall provide training to its Authorized Persons to ensure their treatment of the Personal Data is in accordance with the DPA, including this Data Security Appendix. HUMAN shall provide such training to Authorized Persons before they are allowed access to Personal Data and no less than annually thereafter. Such training shall be consistent with industry standards. Upon reasonable notice from Customer, HUMAN will provide Customer with summaries or copies of HUMAN's relevant training program.

1.4. Access. HUMAN shall limit disclosure of and access to Personal Data to only those Authorized Persons who have a business need to access such Personal Data in order to provide the Services to Customer and/or to fulfill the purposes of the Agreement. HUMAN shall establish, maintain, and enforce the security principles of "segregation of duties" and "least privileged access" with respect to all Personal Data. HUMAN shall reasonably update all access rights based on personnel or computer system changes, and shall periodically review all access rights at an appropriate frequency to ensure current access rights to Personal Data are appropriate and no greater than are required for an individual to perform his or her functions necessary to deliver the Services to Customer and/or to fulfill the purposes of the Agreement. HUMAN shall verify all access rights through effective authentication methods.

1.5. Background Investigations of Personnel. As permitted by law, HUMAN agrees that any employees of HUMAN or of any subcontractor who either are directly providing the Services under the Agreement and/or who have access to Personal Data

shall have passed a background check. Each background check shall include the following minimum review: identity verification (utilizing Social Security numbers or other state/national ID number) and a criminal history check. Background checks must be performed by a member of the National Association of Professional Background Screeners or a competent industry recognized Customer with the same level of professionalism within HUMAN's jurisdiction.

2. **Physical and Technical Security Measures.**

2.1. Server Location. During the term of the Agreement, Personal Data shall at all times be hosted on servers that are physically located in the United States, unless otherwise agreed in writing by the Parties. HUMAN shall comply with and provide Customer with commercially reasonable assistance to comply with Applicable Laws in the country to which and from which Personal Data will be transferred.

2.2. Network Configuration, Access Control and Limiting Remote Access. HUMAN shall secure its computer networks by using and maintaining appropriate firewall and security screening technology that is designed to prevent unauthorized access. HUMAN ensures that the following network security controls are in place: (a) firewall platforms are hardened and have real time logging and alerting capabilities, (b) intrusion detection and prevention systems are in place and maintained at the perimeter and critical server systems, (c) access lists are implemented on network routers to restrict access to sensitive internal networks or servers, (d) remote access requires two factor authentication and occurs over an encrypted tunnel e.g. IPSec, SSLVPN, and (e) systems servicing Customer are segregated from other network zones logically and physically including DMZ, production databases, back office, and software development areas. HUMAN shall secure access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or by tightly controlling access through management approvals, robust controls, logging, and monitoring access events and subsequent audits. HUMAN shall identify computer systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyze log files. HUMAN ensures that privileged accounts (administrator, super user, etc.) will be controlled and reviewed on at least an annual basis. HUMAN enforces a process to control and manage user accounts upon termination of employment or change in role within 24 hours of such termination or change.

2.3. Encryption. HUMAN shall use best efforts to encrypt all Personal Data in its possession, custody or control while at rest and in transit. For the avoidance of doubt, "encryption" shall be deployed using PGP or other industry best practice for key based encryption protocol. HUMAN will work with Customer to test HUMAN's ability to deliver the data in an encrypted form to Customer.

2.4. ThirdParty Data Centers. Where applicable, HUMAN using a third party data center to host the Services shall ensure that (a) all application and database servers are physically isolated within the data center and secured from unauthorized physical access, (b) physical and network access is limited to HUMAN's Authorized Persons, and (c) Personal Data remains logically segregated from other data stored in any shared environment at all times and that use of any shared environment does not compromise the security, integrity, or confidentiality of Personal Data.

2.5. Security Patches. HUMAN shall use commercially reasonable efforts to deploy all applicable and necessary system security patches to all software and systems that process, store, or otherwise support the Services, including operating system, application software, database software, web server software within industry best practices and in accordance with its information security policies.

2.6. Protection Against Malicious Software. HUMAN shall use commercially reasonable efforts to protect its own information technology against malicious code and ensure that its connection to the Internet and for any other platform or network running the Services is secure, and shall in accordance with industry standards and its own information security practices, acquire and implement new technology, including monitoring hardware and software, as the technology becomes available and is proven stable, in HUMAN's reasonable discretion, to ensure a secure and stable environment.

2.7. Vulnerability Testing. Prior to providing any code, hosting services, or network connectivity to Customer, HUMAN must perform and be able to show proof that external penetration testing has been completed and that any reported vulnerabilities have been remediated. Proof includes the external pen test report or cover letter. For software, this includes tests for security vulnerabilities that are a part of the OWASP Top 10 or SANs Top 25. HUMAN will promptly address, prioritize and correct security vulnerabilities identified in a vulnerability test or report.

2.8. Life Cycle Development. HUMAN shall implement and maintain a secure software development life cycle for all applications

which integrate with Customer's environment or are developed on Customer's behalf. HUMAN will observe all industry standard application security guidelines, such as the Open Web Application Security Project (OWASP). HUMAN will ensure that (a) regular reviews of application source code occur, (b) developers receive detailed coding and design training in application security, (c) development, testing, production and operational facilities are separated to reduce the risk of unauthorized access or changes to the production and operational systems and Personal Data, (d) software developers are restricted from accessing production environment unless a particular access request is reviewed and approved, and (e) data masking functionality is implemented in relation to software processing any financial related Personal Data (including payment card and banking information).

2.9. System Change Control. HUMAN will use commercially reasonable efforts to ensure that change control procedures are documented and maintained and detail why the change was required, how and why changes were executed and include an emergency change process. The change control process includes considering security control requirements, implementing them where necessary and testing these changes prior to implementation. HUMAN will notify the Customer of any upgrades or configuration changes which may impact the security of Personal Data.

3. **Security Reviews by Customer.**

3.1. Internal Audits. Upon Customer's written request, HUMAN shall provide Customer, at HUMAN's expense, with the results of the most recent data security compliance reports or any audit performed by or on behalf of HUMAN that assesses the effectiveness of HUMAN's, and any relevant third parties performing services on HUMAN's behalf, information security program, system(s), internal controls, and procedures relating to the Services (i.e., SSAE16 SOC1 or other) as relevant to the security and confidentiality of Personal Data, including any report summarizing any control issues and associated corrective action plans and any management responses. Such reports shall be of sufficient scope and in sufficient detail as may reasonably be required by Customer to provide reasonable assurance that any material inadequacies would be disclosed by such examination, and, if there are no such inadequacies, the reports shall so state.

4. **Noncompliance**.

HUMAN will not knowingly materially lessen the security of any system used to collect, use, disclose, store, retain or otherwise Process Personal Data during the term of the Agreement. In the event that HUMAN determines it is unable to comply with the obligations stated in the DPA or this Data Security Appendix, HUMAN shall promptly notify Customer, and Customer may take any one or more of the following actions: (a) suspend the transfer of Personal Data to HUMAN; (b) require HUMAN to cease Processing Personal Data; (c) demand the return or destruction of Personal Data; or (d) immediately terminate this Agreement.

5. **External Communication of Internal Controls**.

HUMAN communicates its security and availability commitments regarding its products and Services to external users via its Terms of Use and Privacy Policy, which are posted on its website. Customer usage and external roles and responsibilities are communicated via several mediums, including the Terms of Use and Privacy Policy. Support contact information is readily available to customers through HUMAN's website and other customer provided documentation. Customers and users are encouraged to contact appropriate personnel if they become aware of items such as operational or security failures, Incidents, systems problems, concerns or other complaints.

Appendix 3 - Cross Border Transfer Mechanism

1. Definitions. Capitalized terms not defined in this Appendix shall have the meaning set forth in the DPA.

1.1 "Standard Contractual Clauses" means, as applicable to a particular transfer, one of the following:

1.1.1 EEA SCCs

1.1.2 UK SCCs

1.2 "EEA SCCs" or **"EEA Standard Contractual Clauses"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.3 "UK SCCs" or **"UK Standard Contractual Clauses"** means the "UK Addendum to the EU Standard Contractual Clauses" issued by the UK ICO under s.119(A)(1) of the Data Protection Act of 2018 ("UK Addendum").

2. The Standard Contractual Clauses will apply to any Processing of Personal Data by HUMAN where Personal Data is exported by Customer from the European Economic Area ("**EEA**"), the United Kingdom and/or Switzerland to HUMAN outside the EEA, the United Kingdom and/or Switzerland, either directly or via onward transfer, to any country: (a) not recognized by the European Commission, United Kingdom, or Switzerland (as applicable) as providing an adequate level of protection Personal Data (within the meaning of Applicable Laws); and (b) to the extent the transfer is not covered by an alternative mechanism of transfer (e.g., binding corporate rules) recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

3. Application of the EEA Standard Contractual Clauses. If Customer exports Personal Data from the EEA or Switzerland to HUMAN, then the EEA SCCs will apply as follows:

3.1 Module 2 (Controller to Processor) will apply where Customer is a Controller of Personal Data and Vendor is a Processor of Personal Data;

3.2 Module 3 (Processor to Processor) will apply where Customer is a Processor of Personal Data and Vendor is a Processor of Personal Data;

3.3 For each Module, where applicable:

3.3.1 in Clause 7, the option docking clause will not apply.

3.3.2 in Clause 9, Option 2 will apply, and the time period for prior notice of a sub-processor will be as set forth in Section 10 of the DPA.

3.3.3 in Clause 11, the option will apply.

3.3.4 in Clause 17 (Governing Law) (Option 1), the law of Ireland will apply.

3.3.5 In Clause 18(b), disputes will be resolved before the courts of Ireland.

3.4 Annex I of the SCCs shall be deemed completed with the information in Appendix 1 of this DPA.

3.5 Annex II of the SCCs shall be deemed completed with the information in Appendix 2 of this DPA.

3.6 Annex III of the SCCs shall be deemed completed with the sub-processor information in Appendix 1 of this DPA.

3.7 If Customer exports Personal Data from Switzerland to HUMAN:

3.7.1 The supervisory authority with respect to such Personal Data is the Swiss Federal Data Protection and Information Commissioner.

3.7.2 References to a "Member State" shall be interpreted to refer to Switzerland.

3.7.3 Data subjects located in Switzerland shall be able to enforce their rights in Switzerland.

3.7.4 References to the EU GDPR shall be understood to refer to the Swiss Federal Act on Data Protection (as amended or replaced).

3.7.5 In Clause 17 (Governing Law) (Option 1), the law of Ireland will apply.

3.7.6 In Clause 18(b), disputes will be resolved in the courts of Ireland.

4. **Application of the UK Standard Contractual Clauses.** If Customer exports Personal Data from the UK to HUMAN, then the Parties are permitted to rely on the EEA Standard Contractual Clauses for transfers of Personal Data, as amended by and subject to completion of a UK Addendum. Accordingly: (i) the EEA SCCs shall apply as amended by the UK Addendum, as modified and specified by Sections 3.1 through 3.6 of this Appendix; and (ii) the UK Addendum shall be deemed executed between HUMAN and Customer. Table 3 of the UK Addendum shall be completed as follows:

    4.1.1 Annex I shall be deemed completed with the information in Appendix 1 of this DPA.

    4.1.2 Annex II shall be deemed completed with the information in Appendix 2 of this DPA.

    4.1.3 Annex III shall be deemed completed with the sub-processor information in Appendix 1 of this DPA.

5. If a Regulatory Authority issues new Standard Contractual Clauses, such new Standard Contractual Clauses will be incorporated into this DPA when in effect without any further action of the Parties. Information contained within this DPA, including the information from Appendix 1 and Appendix 2, shall be deemed incorporated into such new Standard Contractual Clauses as applicable.

PRIOR VERSIONS

April 30, 2024