Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

Cybersecurity Youth Apprenticeship Initiative (CYAI) is funded by the U.S. Department of Labor's (DOL) Employment and Training Administration (ETA) Office of Apprenticeship (OA). CYAI is administered by ICF via a five-year contract that began in 2019. ICF developed the policies related to operation of the program established in this Program Manual, which has been reviewed and approved by DOL.

The goal of this Program Manual is to provide standardized programming for Registered Apprenticeship Programs (RAP) that receive funding from CYAI.

CYAI-Funded Sites

The Executive Director or Responsible Party and the Training Director must confirm they have received, read, and agree to follow the policies and procedures outlined in the Program Manual prior to CYAI reimbursement.

Training Site Program Manual Receipt

I agree that I have received, reviewed, and will agree to abide by the policies and procedures outlined in the Program Manual. Failure to abide by these policies and procedures could indicate that my training program will forfeit any funds and or may be required to return all reimbursements to CYAI.

I understand that this Program Manual is subject to change and will be amended in the future as changes arise. This version is effective as of August 25, 2020.

The signed receipt of this manual is required prior to award of any funds.

_____ _____

Executive Director/Responsible Party Date

_____ _____

Training Director Date

Please submit all application materials to ICF at: CYAI2024@icf.com

Overview

CYAI will establish and sustain cybersecurity apprenticeships for youth by working with employers, industry and trade association executives, public officials, workforce professionals, secondary and post-secondary educators, and registered apprenticeship experts. Specific tasks include building brand awareness of youth apprenticeships, facilitating peer learning and knowledge-sharing, managing outreach and recruitment, convening apprenticeship forums, initiating new apprenticeship programs, expanding and sustaining existing youth apprenticeship programs, conducting research and evaluations, and preparing a promising practices guide. CYAI will invest $400,000[1] over a period of five years to strategically launch and sustain promising cybersecurity youth apprenticeships.

Section 1. Site Qualifications

Selected sites must either be a Registered Apprenticeship Program (RAP) or have submitted proof that they will become a RAP prior to requesting or receiving reimbursement funds from CYAI. CYAI will only reimburse programs for registration of eligible participants into a cybersecurity RAP. Pre-apprenticeship programs are eligible but funds will not be disbursed until the participant has completed the program and been placed with an employer.

Section 2. Eligible Participants

Participants must be between the ages of 16-21. Eligible students may be enrolled in high school, technical colleges, community colleges, four-year colleges, universities, career and technology education training centers, regional education service agencies, non-profit registered apprenticeship programs, YouthBuild programs, or Job Corps. This list is not exhaustive. If you feel your program serves eligible participants, contact CYAI to discuss.

Section 3. Tracking Participant Attendance

CYAI has $80,000 to disburse annually across all CYAI partner organizations. CYAI partners may receive up to $400/apprentice. Once CYAI funds have been exhausted, no additional programs will receive reimbursements. ICF will notify awardees when funds are nearly exhausted. An award does not guarantee a reimbursement of funds if the site is not successful in enrolling apprentices. Payment will be made once ICF has verified all submitted information. To receive reimbursements, partner organizations must provide the below information. Definitions of each required tracking element can be found in Appendix A.

- Apprentice Last Name
- Apprentice First Name
- Apprentice Middle Name
- Apprentice Suffice
- Employment Status
- Date of Birth
- Apprentice Registration Date
- Apprentice State Date
- Sex
- Apprentice Street Address
- Apprentice City
- Apprentice State
- Apprentice 5-Digit Zip Code
- Primary Telephone
- Ethnicity/Race
- Veteran Status
- Apprentice Education Status
- Occupation 8-digit O*NET Code
- Entry Wage
- Expected Completion Date

Section 4. Personal Identifiable Information and Documentation Retention

[1] Funding is dependent on ICF receiving annual funding from the Department of Labor.

CYAI partners will be required to comply with CYAI requirements around Personal Identifiable Information (PII). Any deviation from the guidance outlined in Appendix B will render the organization ineligible for the funds.

The partner organization will retain all participant information. All documents must be retained three years after examination. As part of the Paperwork Reduction Act[2], training sites can maintain these documents in electronic form.

Section 5. Technical Assistance

In addition to incentive funds, CYAI partners will receive technical assistance from CYAI, including but not limited to support related to outreach, recruitment, orientation, training, curriculum, employment placement, and retention.

Section 6. Brand Awareness, Employment Engagement, Apprenticeship Forums

To raise the visibility of the initiative, CYAI will work with the partner organization to raise brand awareness through social media as well as support various employment engagement and/or apprenticeship forums. CYAI will work with partner organizations to identify locations and interested parties for these events. Partners are expected to assist in site location, registration lists, and highlighting program innovations.

Section 7. Cybersecurity Showcases

CYAI will sponsor existing ethical hackathons and/or convene cybersecurity showcases annually. Partner organizations will support the events by encouraging and facilitating enrollment of CYAI apprentices and other interested individuals to attend the competition.

[2] https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf

Appendix A: Definitions of Required Registration Fields

Data Element Name	Data Definition and Instruction
Apprentice Last Name	Enter the last name of the apprentice.
Apprentice First Name	Enter the first name of the apprentice.
Apprentice Middle Name	Enter the middle name of the apprentice.
Apprentice Suffix	Enter the suffix to the apprentice name. Values include I, II, III, Jr., Sr. Default is Null.
Employment Status	Enter participant's employment status. Incumbent workers are defined as existing employees of the company.
Date of Birth	Record the participant's date of birth.
Apprentice Registration Date	Enter the date the apprentice was registered.
Apprentice Start Date	Enter the date that the apprentice began their apprenticeship. This date may be the same as the registration date but cannot be prior to the registration date.
Sex	Record 1 if the participant indicates that he is male. Record 2 if the participant indicate that she is female. Record 9 if the participant prefers not to say.
Apprentice Street Address	Enter the apprentice's street address.
Apprentice City	Enter the apprentice's city.
Apprentice State	Enter the apprentice's state.
Apprentice 5-Digit Zip Code	Enter the apprentice's 5-digit zip code.
Primary Telephone	Enter the area code (999) and telephone number 999-9999 of the apprentice.
Ethnicity/Race	Capture if identified as: Hispanic/Latino; American Indian/Alaskan Native; Asian Black/African American; Native Hawaiian/Other Pacific Islander; White; More than One Race.
Veteran Status	Capture if the apprentice is identified as a Veteran.
Apprentice Education Status	Enter the apprentice's education status. Default Value = 5 for unknown/not provided.
Occupation 8-digit O*NET Code	Enter the 8-digit O*NET code that best fits the apprentice occupation (www.onetonline.org). **NOTE: This code must match an occupation code registered by the program sponsor.**
Entry Wage	Enter the apprentices hourly starting wage. This wage cannot be less than the apprentice hourly entry wage for the occupation as established by the program sponsor.
Expected Completion Date	Expected date of completion. The expected completion date cannot be prior to the registration or start date.

Appendix B: Data Protection Addendum (DPA)

This Data Protection Addendum ("DPA") forms part of the Subcontract Agreement, or other written electronic agreement between Contractor and Subcontractor for the Services ("Agreement") to reflect the Parties' agreement with regard to the Processing of Personal Data. The obligations set forth in this Agreement are in addition to, and not exclusive of, any obligations provided by law. To the extent the data protection terms contained in this Agreement conflict or are inconsistent with any other agreement of the Parties or privacy statements, the terms contained in this Addendum shall control.

In all such clauses, unless the context of the clause requires otherwise, the term "**Vendor**", **"Supplier"** or "**Data Processor**" shall mean Subcontractor, the term "**ICF**", **"Client"**, "**Contractor**" or "**Data Controller**" shall mean Contractor.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. **Definitions.** Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified in Appendix 1, the terms of the Agreement shall remain in full force and effect. This DPA contains Vendor's Technical and Operational Measures, which procedures are in addition to and cumulative of the requirements of the Agreement.

2. **Roles of the Parties**.

2.1 During the Term of the Agreement, the Parties agree to comply with Data Protection Laws and Regulations directly applicable to their respective businesses.

2.2 As between the Parties for the Processing of Client Personal Data, Client shall be the Data Controller and Vendor shall be the Data Processor. Client shall be solely responsible for determining compliance with Data Protection Laws and Regulations as the Data Controller. Vendor shall be solely responsible for determining compliance with Data Protection Laws and Regulations as the Data Processor.

2.3 In no event will either Party be required to monitor or advise the other regarding the Data Protection Laws and Regulations applicable to other Party concerning Client Personal Data.

2.4 Vendor will provide verifiable notice to Client's Users or other applicable Data Subjects through Client's applicable local country privacy statement. Such privacy statement must comply with applicable Data Protection Laws and Regulations.

2.5 Vendor will obtain Data Subject verifiable, freely given, specific and unambiguous consent to Process Client Personal Data in the Services.

3. **Processing of Personal Data.**

3.1 Client's Processing of Personal Data. Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

3.2 Details of Vendor's Processing of Personal Data. Vendor will:

3.2.1.1 Process Client Personal Data on Client's behalf and in accordance with Client's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable SOWs or related orders forms; (ii) Processing initiated by Client in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.3 The subject-matter of Processing of Personal Data by Client is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 ("Details of the Processing") to this DPA.

3.4 Confidentiality and Discloser. Vendor will:

3.4.1.1 treat Client Personal Data as Confidential Information.

3.4.1.2 ensure that its personnel engaged in the Processing of Client Personal Data are informed of the confidential nature of the Client Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

3.4.1.3 ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.4.1.4 ensure the reliability of any Vendor personnel, contractor or agent engaged in the Processing of Personal Data.

3.4.1.5 ensure that Vendor's access to Client Personal Data is limited to those individuals who need access to perform Services in the context of that individual's duties to Vendor.

3.4.1.6 not disclose or permit the disclosure of the Client Personal Data to any third party other than in accordance with Client's documented instructions.

3.4.1.7 be permitted to disclose Client Personal Data as may be required by law, regulation, judicial or administrative process or in connection with litigation pertaining thereto, provided that Vendor first gives Client prompt notice, where feasible, and a reasonable opportunity to seek an injunction to prevent the disclosure of Client Personal Data if Client believes such disclosure is not legally required.

4. **Return and Deletion of Client Personal Data.**

4.1 Vendor, within ninety (90) calendar days of the Relevant Date, will: (a) return a complete copy of all Client Personal Data to Client by secure file transfer in such format as notified by Client to Vendor; and (b) Delete and procure the Deletion of all other copies of Client Personal Data Processed by Vendor or any Authorized Subprocessor.

4.2 Subject to Section 4.3, Client may, in its discretion, notify Vendor in writing within thirty (30) days of the Relevant Date to require Vendor, at Vendor's sole expense, to Delete and procure the Deletion of all copies of Client Personal Data Processed by Vendor or any Authorized Subprocessor. Vendor shall comply with any such written request within ninety (90) days of the Relevant Date.

4.3 Vendor may retain Client Personal Data to the extent required by Applicable Laws only to the extent and for such period as required by Applicable Laws and always provided that Vendor shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

4.4 Vendor, upon Client's prior written request, shall provide written certification to Client that it has fully complied with this Section 4 within ninety (90) days of the Relevant Date.

5. **Sub-Processing.**

5.1 Vendor may:

5.1.1.1 not engage any Sub-processors (excluding its own personnel, resources or Vendor Affiliates) to Process Client Personal Data without Contractor's prior written approval, except as set out in Annex 2 ("Authorized Subprocessors") in connection with the provision of the Services.

5.1.1.2 shall implement adequate due diligence on each pre-approved Subprocessor to ensure that it is capable of providing the level of protection for Client Personal Data as is required by this DPA and enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.1.1.3 remain fully liable to Client for any failure by any Subprocessor to fulfil its obligations in relation to the Processing of any Client Personal Data.

5.2 Objection Right for New Sub-processors. If Sub-processors are used, Client may object to Vendor's use of any new Sub-processor by notifying Vendor promptly in writing within ten (10) business days after receipt of Vendor's notice in accordance with the mechanism set out in Section 5.1. In the event Client objects to a new Sub-processor, as permitted in this Section, Vendor will make available to Client a change in the Services or recommend a change to Client's configuration or use of the Services to avoid Processing of Client Personal Data by the objected-to new Sub-processor without unreasonably burdening the Client.

5.3 Liability. Vendor shall be liable for the acts and omissions of its Sub-processors to the same extent Vendor would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. **International Transfers of Customer Personal Data.**

6.1 If Vendor Processes Personal Data of EEA citizens or residents, it will either: (i) obtain certification for, and comply with, EU-U.S. and Swiss-U.S. Privacy Shield or its successor, a link with may be found at: https://www.privacyshield.gov/welcome and notify the Client in writing within five (5) days, upon either the renewal of Vendor's certification or the lapse of same; or (ii) Process, at the Client's sole discretion, such Personal Data under EU-approved SCCs and shall abide by all provisions in such SCCs applicable to "Sub-processors" as defined therein immediately upon Client providing Vendor with a copy of such SCCs or similar clauses to ensure the adequate protection of the transferred Client Personal Data.

7. **Data Protection Impact Assessment and Prior Consultation.**

7.1 Upon Client's prior written request and solely in relation to Vendor's Processing of Client Personal Data, Vendor shall provide Client with reasonable cooperation and assistance needed to help Client:

7.1.1.1 fulfil Client's obligation under the applicable Data Protection Laws and Regulations to implement a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information.

7.1.1.2 in the cooperation or prior consultation with the Supervisory Authority of Client in the performance of its tasks relating to this of the DPA, to the extent required under applicable Data Protection Laws and Regulations.

8. **Data Subject Rights.**

8.1 Taking into account the nature of the Processing, Vendor, to the extent legally permitted, will:

8.1.1.1 promptly notify Client if Vendor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure/right to be forgotten, data portability, object to the Processing, right not to be subject to an automated individual decision making ("Data Subject Request").

8.1.1.2 assist Client to facilitate the fulfilment of Client's obligation to respond to a Data Subject Request to exercise their rights under Data Protection Laws and Regulations.

8.1.1.3 assist Client in responding to Data Subject Requests, to the extent the response to such Data Subject Request is required under Data Protection Laws and Regulations.

9. **Security Controls and Safeguards.**

9.1 Vendor will maintain appropriate administrational, organizational technical and security measures designed to protect the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Personal Data), confidentiality and integrity of Client Personal Data during the Agreement Term and as long as Client Personal Data is in Vendor's possession or under Vendor's control. Vendor will regularly monitor network and production systems and implements and maintains security controls and procedures designed to prevent, detect and respond to identified threats and risks to reasonably calculate and prevent unauthorized access to or unauthorized use of Client Personal Data, and upgrading information safeguards as necessary to limit risks. Such controls include, but are not limited to:

9.1.1 Data Protection Security Awareness and Training. Vendor requires and will continue to require annual security and privacy training for all personnel with access to Client Personal Data.

9.1.2 Background Checks. Vendor shall perform a criminal background check on any employee performing Vendor Services under the Agreement.

9.1.3 Access Limitations. Vendor will i) limit access to its information systems and the facilities in which they are housed to authorized persons under the Agreement and to those persons who are reasonably required to know such information to perform the Services; ii) subject such authorized persons to user authentication and log on processes when they need access to Client Personal Data. Such access shall be accompanied by, at a minimum, a written procedure that sets forth the manner in which access to Client Personal Data is restricted, and storage of the Client Personal Data in locked facilities, storage areas or containers; iii) accompany such access with a written procedure that sets forth the manner in which Supplier restricts access to Customer Personal Data; iv) store the Customer Personal Data in locked facilities, storage areas or containers; and v) remove Supplier personnel access to Customer Personal Data upon employment termination or a change in job status that results in the personnel no longer requiring access to Customer Personal Data.

9.1.4 Password Protection. Vendor will not log passwords. Vendor will i) require strong password standards (8 characters minimum), which include length, complexity and expiration and ii) block access after a ten (10) account attempt lockout threshold at a maximum is met.

9.1.5 Encryption. Vendor, at a minimum and where Vendor transmits Client Personal Data and communication, will use i) industry-accepted encryption products, including 128-bit TLS Certificates 2048-bit RSA public keys at a minimum to protect Client Personal Data and communications during transmissions between a Client's and Vendors network and ii) AES-256 encryption for all data, including Client Personal Data, transmitted between data centers for replication purposes across a dedicated, encrypted link.

9.1.6 Monitoring, Testing and Detection. Vendor will: i) employ an industry standard network intrusion detection system and firewalls to monitor and block suspicious network traffic; ii) reviews access logs on servers and security events and retaining network security logs for 180 days; iii) review privileged access to production systems; iv) perform network vulnerability assessments on a regular basis; v) perform scans using commercially available scanning tools that identify application and operating system vulnerabilities; vi) maintain a vulnerability remediation program; vii) ensure all endpoints run an anti-virus solution and applies timely signature updates; viii) patch all critical, exploitable vulnerabilities in a commercially reasonable time frame; ix) engage upon Client's prior written request, third parties to perform network penetration testing on at least an annual basis**;** and x) any software or system design, develop, configure or implement under the Agreement will be in accordance with applicable security standards and commercial industry practices.

9.1.7 PCI-DSS Compliance. If and where applicable, Vendor shall comply, where applicable and relevant to performing Services, with the appropriate Payment Card Industry Data Security Standards and shall not retain credit card information of Users (except last four digit identifiers for transaction verification) after transmission of transactions to the credit card issuers.

9.1.8 Access To Contractor Systems. Where Vendor will access Client's systems, Vendor will comply with either Client's standards for third party access to Contractor systems or equivalent program standards, and Vendor will provide Client with written documentation of such program, which will be incorporated herein by reference. Vendor's access to such systems, if applicable, shall be limited to: (i) Vendor personnel who require access in order to perform Services under this Agreement; (ii) the Term of the Agreement or such other time as Client may determine in its sole discretion; and (iii) Client systems identified by Client as critical to the performance of this Agreement.

9.1.9 Remediation and Response. Vendor: i) documents responsive actions taken regarding any data protection incident and implements mandatory post-incident review of events and actions taken, if any, to change business practices relating to protection of Client Personal Data.

9.1.10 Business Continuity and Disaster Recovery. Vendor will i) design or has designed its production data centers to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance.; ii) utilize secondary facilities that are geographically diverse from their primary data centers, along

with required hardware, software, and Internet connectivity, in the event Vendor production facilities at the primary data centers were to be rendered unavailable; and iii) ensure disaster recovery plans are in place and test them at least once per year to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation. Vendor's disaster recovery plans currently have the following target recovery objectives: maximum Client Personal Data loss (recovery point objective) of 4 hours.

9.1.11 Backup and Reliability. Vendor will: i) configure all networking components, network accelerators, load balancers, Web servers and application servers in a redundant configuration; ii) store all Client Personal Data on a primary database server with multiple active clusters for higher availability; iii) store all Client Personal Data on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance; and iv) automatically replicate Client Personal Data on a near real-time basis to the secondary site and is back it up on a regular basis and stored on backup media for an additional 90 days in production environments and 30 days in Sandbox environments, after which it is securely overwritten or deleted (Any backups are verified for integrity and stored in the same data centers as their instance).

10. **Audit.**

10.1 Upon Client's thirty (30) days' prior written request and at commercially reasonable intervals, and subject to confidentiality obligations set forth in the Agreement, Vendor shall make available to Client, that is not Vendor's competitor (or to Client's independent, third party auditor that is not Vendor's competitor), a copy of Vendor's then most recent third-party audits, attestations, or certifications, as applicable.

10.2 If the copy under Section 10.1 is not acceptable for Client's audit purposes, Vendor shall provide reasonable assistance by allowing inspection, on Vendor's premises, of relevant documents or records, to the extent such information directly relates to the transaction records for the Services provided by Vendor to the Client under the Agreement. The audit shall be conducted at a mutually agreed upon time and Client will provide Vendor with no less than ten (10) business days' advanced written notice of any requested audit. Vendor will provide appropriate management personnel to engage with Client and supervise any audit. The onsite part of the audit shall last no longer than three (3) business days, unless the auditor requests a longer onsite inspection period.

11. **Client Personal Data Breach Management, Notification and Related Process.**

11.1 Notification and Updates. Vendor shall notify Client within twenty-four (24) hours of Vendor becoming aware of a Client Personal Data Breach ("Client Personal Data Breach Notice").

11.2 Client Personal Data Breach Notice. Such notification, at minimum, contain, will: (i) describe the nature of the Client Personal Data Breach, including the date of the Client Personal Data Breach and the date of the discovery; (ii) describe the types of Client Personal Data involved, including the number and categories or identities of Data Subject involved; (iii) communicate the name and contact details of Vendor's data protection officer, chief information security officer or other relevant contact from whom more information may be obtained; (iv) describe the measures Vendor has taken, is taking, and intends to take to mitigate harm or remediate the Client Personal Data Breach; and (v) recommended steps that the Client Personal Data should take to protect any affected individuals from harm. Vendor will timely update information provided in the Client Personal Data Breach Notice to Client.

11.3 Investigation and Cooperation. Vendor shall cooperate with Client to identify the cause of such Client Personal Data Incident and take those steps as Client deems necessary and reasonable to investigate and remediate the cause of such a Client Personal Data Incident.

11.4 In the event of a Client Personal Data Incident, Vendor shall not inform any third party without first obtaining Client's prior written consent, unless notification is required by Data Protection Laws and Regulations or any other law to which Vendor is subject, in which case Vendor shall to the extent permitted by such law inform Client of that legal requirement, provide a copy of the proposed notification and consider any comments made by Client before notifying the Client Personal Data Incident.

12. **Data Protection Indemnity.**

12.1 Vendor shall indemnify and hold harmless Contractor and each Contractor Affiliate against all losses, fines and sanctions arising from any claim by a third party or Supervisory Authority arising from any breach of this Addendum.

13. **Data Protection Liability.**

13.1 Notwithstanding anything to the contrary in the Agreement, Vendor's liability for any breach of this Addendum shall be unlimited.

14. **General Terms**.

14.1 Termination. Subject to Section 14.2, this DPA shall terminate automatically upon (i) termination of the Agreement; or (ii) expiry or termination of all service contracts, SOWs, work orders or similar contract documents entered into by Client with Client and/or Client Affiliates pursuant to the Agreement, whichever is later.
Any obligation imposed on Client under this DPA in relation to the Processing of Client Personal Data shall survive any termination or expiration of this DPA.

14.2 Governing law of this DPA. This DPA shall be governed by the:

14.2.1 governing law of the Agreement for so long as that governing law is the law of a Member State of the European Union; or

14.2.2 laws of England for so long as the United Kingdom is a Member State of the European Union where Section 14.2.1 does not apply, or

14.2.3 governing law of the Agreement where Sections 14.2.1 and 14.2.2 both do not apply and to the extent that EEA Data Protection Laws and Regulations do not apply to the Processing of Client Personal Data.

14.3 Choice of jurisdiction. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in this DPA with respect to any disputes or claims howsoever arising under this DPA.

14.4 Order of precedence. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including but not limited to the Agreement, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations for Client Personal Data of a Data Subject from a Member State of the European Union.

14.5 Costs of compliance. Compliance by Client with the provisions of this DPA will be borne by Client.

14.6 Third party rights.

14.6.1 Except to the extent set forth in Section 14.2.2 and in the SCCs, a person who is not a party to this DPA shall have no right to enforce any term of this DPA.

14.6.2 A Client Affiliate may enforce any term of this DPA which is expressly or implicitly intended to benefit it. The rights of the Parties to rescind or vary this DPA are not subject to the consent of any other person.

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

Appendix C: Data Protection Addendum Definitions

1. Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1 "Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 "Applicable Laws" means (a) European Union or Member State laws with respect to any Client Personal Data in respect of which Client or any Client Affiliate is a Data Controller or a Data Processor under EEA Data Protection Laws and Regulations; and (b) any other applicable law with respect to any Client Personal Data in respect of which Client or any Client Affiliate is a Data Controller or a Data Processor under any other Data Protection Laws and Regulations.

1.3 "Authorized Subprocessors" means (a) those Subprocessors set out in Annex 2 ("Authorized Subprocessor(s)); and (b) any additional Subprocessors consented to in writing by Client in accordance with Section 5 ("Subprocessing").

1.4 "Client" means the client or client Affiliates, employees, representatives, Users.

1.5 "Client Personal Data" means the data described in Annex 1 ("Details of Processing of Personal Data) and any other Personal Data Processed by Client or any Client Affiliate on behalf of Client or any Client Affiliate pursuant to or in connection with the Agreement.

1.6 "Data Controller" shall have the same meaning as in the Data Protection Laws and Regulations, and shall be interpreted as in accordance with the terms "Data Controller" and "Data Processor".

1.7 "Data Processor" shall have the same meaning as in the Data Protection Laws and Regulations, and shall be interpreted as in accordance with the terms "Data Controller" and "Data Processor".

1.8 "Data Protection Laws" or "Data Protection Laws and Regulations" means any applicable data privacy or data security laws or electronic privacy laws, including but not limited to, means all laws and regulations, of the European Union, the EEA and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

1.9 "Data Subject", shall have the same meaning as in the Data Protection Laws and Regulations.

1.10 "Delete" means the removal or obliteration of Personal Data such that it cannot be recovered or reconstructed.

1.11 "EEA" means the European Economic Area.

1.12 "GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.13 "Personal Data" shall have the same meaning as in the Data Protection Laws and Regulations, including but not limited to any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations).

1.14 "Personal Data Breach" means a suspected or actual data privacy violation and/or data security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, misuse, or access to, Client Personal Data transmitted, stored or otherwise Processed, as well as any breach of Section 9 ("Security Controls and Safeguards") of this DPA, or of the data protection, confidentiality or security provisions of the Agreement.

1.15 "Process/Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, Processing of or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.16 "Relevant Date" means the date falling on the earlier of (i) the cessation of Processing of Client Personal Data by Client of Client Affiliates; or (ii) termination of the Agreement.

1.17 "Restricted Transfer" means either (i) a transfer of Personal Data from Client or any Client Affiliate ("Transferor") to Client or any Client Affiliate ("Transferee"); or (ii) an onward transfer from a Client to a Subprocessor (also a "Transferee"), in each case where such transfer would be prohibited by Data Protection Laws and Regulations in the absence of the SCCs to be established under Section 6 (“Transfer Mechanisms for Restricted Transfers of Personal Data”). For the avoidance of doubt: (a) without limitation to the generality of the foregoing, the Parties to this DPA intend that transfers of Personal Data from the UK to the European Union or from the European Union to the UK, following any exit by the UK from the European Union shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by UK Data Protection Laws and Regulations or EEA Data Protection Laws and Regulations (as the case may be) in the absence of the SCCs to be established under Sections 5 (“Subprocessing”) or 6 (“Transfer Mechanisms for Restricted Transfers of Personal Data”); and (b) where a transfer of Personal Data from one country to another country is of a type authorized by Data Protection Laws and Regulations in the exporting country for example in the case of transfers from within the European Union to a country or scheme (such as the EU - US Privacy Shield) which is approved by the European Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer for the purposes of this DPA.

1.18 "Services" means the Services supplied under the Agreement.

1.19 "Special Categories of Personal Data" shall have the same meaning as in the Data Protection Laws and Regulations.

1.20 "Standard Contractual Clauses" or “SCCs” means (i) the standard contractual clauses for the transfer of Personal Data to Data Processors established in third countries, which do not ensure an adequate level of protection as set out in Commission Decision C(2010) 593, as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a Supervisory Authority for use with respect to any specific Restricted Transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by applicable Data Protection Laws and Regulations for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Regulatory Authority or applicable Data Protection Laws and Regulations.

1.21 "Subprocessor" means any subcontracting Data Processor appointed by Data Processor to Process Client Personal Data on behalf of Client or any Client Affiliate;

1.22 "Supervisory Authority" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws and Regulations;

1.23 "Third Country" means a country which is not a Member State of the EEA.

1.24 “Users” mean customers, consumers, or users of Client services.