WORKSUITE INC.
DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**DPA**") is made as of the last date set forth on the signature page hereto (the "**Effective Date**") by and between Worksuite Inc., a corporation organized and existing under the laws of the State of Delaware, U.S.A. ("**Worksuite**"), and the entity or person set forth on the signature page hereto ("**Customer**"), pursuant to the Agreement (as defined below). This DPA has been pre-signed on behalf of Worksuite. This DPA will be void *ab initio*, with no force or effect, if the entity or person signing this DPA is not a party to an effective Agreement (as defined below) directly with Worksuite. Worksuite and Customer are sometimes referred to herein individually as a "**party**" or together as the "**parties**".

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data is processed by Worksuite under the Agreement.

1. Definitions

1.1 For the purposes of this DPA, the following terms shall have their respective meanings set forth below and other capitalized terms used but not defined in this DPA have the same meanings as set forth in the Agreement:

(a) "**Agreement**" means the Terms of Service or SaaS Provider Agreement, as applicable, between the parties, in each case providing for the provision by Worksuite to Customer of the services described therein.

(b) "**EEA**" means the European Economic Area (including the United Kingdom).

(c) "**EU Data Protection Legislation**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**Directive**"), including any applicable national implementations of it; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**") (as amended, replaced or superseded).

(d) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

(e) "**Processor**" means an entity which processes Personal Data on behalf of the Controller. (f)

"**Personal Data**" means any information relating to an identified or identifiable natural person.

(g) "**Privacy Shield**" means the EU-U.S. and Swiss-U.S. Privacy Shield self-certification program operated by the U.S. Department of Commerce.

(h) "**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of July 12, 2016 (as may be amended, superseded or replaced).

(i) "**Security Incident**" means accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

(j) **"Sensitive Data**" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof), (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; (f) date of birth; (g) criminal history; (h) mother's maiden name; and (i) any other information that falls within the definition of "special categories of data" under EU Data Protection Legislation or any other applicable law relating to privacy and data protection.

2. Relationship with Agreement

2.1 Except as amended by this DPA, the Agreement will remain in full force and effect. 2.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. 2.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

3. Applicability of this DPA

3.1 Part A (being Sections 4 to 6 as well as Annexes A and B of this DPA), shall apply to the processing of Personal Data under the Agreement from the Effective Date above.

3.2 Part B (being Sections 7 to 10) shall apply to the processing of Personal Data by Worksuite falling within the scope of the GDPR from and including 25 May 2018.

3.3 Part C (being Section 11) and those provisions of Part B expressly incorporated into Annex C shall apply to the processing of Personal Data by Worksuite falling within the scope of the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA") and the Virginia Consumer Data Protection Act (Va. Code §§ 59.1-575 et seq.) ("VCDPA"), in each case, as updated, amended or replaced from time to time.

3.4 With respect to the processing of Personal Data falling within the scope of Part B:

(a) the terms of Part B shall apply in addition to, and not in substitution of, the terms in Part A; and

(b) to the extent there is any conflict between the provisions in Part A and Part B, the provisions in Part B shall take priority from and including 25 May 2018.

3.5 Notwithstanding anything in this DPA, Worksuite will have the right to collect, extract, compile, synthesize and analyse aggregated, non-personally identifiable data or information (data or information that does not identify Customer or any other entity or natural person as the source thereof) resulting from Customer's use or operation of the Services ("**Service Data**") including, by way of example and without limitation, information relating to volumes, types, skills, on boarding percentages, performance ratings, or any other information regarding talent Customer, its end users generate using the Services. To the extent any Service Data is collected or generated by Worksuite, such data will be solely owned by Worksuite and may be used by Worksuite for any lawful business purpose without a duty of accounting to Customer or its recipients. For the avoidance of doubt, this DPA will not apply to Service Data.

Part A: General data protection obligations

4. Roles and responsibilities

4.1 Parties' Roles. Customer, as Controller, appoints Worksuite as a Processor to process the Personal Data described in **Annex A** on Customer's behalf.

4.2 Purpose Limitation. Worksuite shall process the Personal Data for the purposes described in **Annex A** and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law. The Agreement and this DPA sets out Customer's complete instructions to Worksuite in relation to the processing of the Personal Data and any processing required outside of the scope of these instructions will require prior written agreement between the parties.

4.3 Sensitive Data. For the avoidance of doubt, Sensitive Data is not required by Worksuite to use the Services. Controller is solely responsible for the amount of Personal Data collected and stored within Worksuite and represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit us, our affiliates and sub-processors, to execute their rights or perform their obligations under this DPA. We shall promptly inform you, if in our opinion, any of the instructions regarding the processing of Customer data provided by you, breach any applicable data protection laws.

4.4 Description of Processing. A description of the nature and purposes of the processing, the types of Personal Data, categories of data subjects, and the duration of the processing are set out further in **Annex A**.

4.5 Compliance. Customer shall be responsible for ensuring that:

(a) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including EU Data Protection Legislation, in its use of the Services and its own processing of Personal Data (except as otherwise required by applicable law); and

(b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Worksuite for processing in accordance with the terms of the Agreement and this DPA.

5. Security

5.1 Security. Worksuite shall implement appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

5.2 Security Exhibit. The technical and organizational security measures which Worksuite shall have in place under the Agreement are set out at **Annex B** to this DPA.

6. International transfers

6.1 International Transfers. To the extent that Worksuite processes (or causes to be processed) any Personal Data originating from the EEA in a country that has not been designated by the European Commission as providing an adequate level of protection for Personal Data, the Personal Data shall be deemed to have adequate protection (within the meaning of EU Data Protection Legislation) by virtue of Worksuite's self-certification to the Privacy Shield. Worksuite shall agree to apply the Privacy Shield Principles when processing (or causing to be processed) any EEA or Swiss Personal Data under this Agreement.

6.2 Privacy Shield Notifications. Worksuite agrees to notify Customer without undue delay if its self certification to the Privacy Shield is withdrawn, terminated, revoked, or otherwise invalidated. In such a case, the parties shall cooperate in good faith to put in place such alternative data export mechanisms as are required under EU Data Protection Legislation to ensure an adequate level of protection for the Personal Data.

Part B: GDPR Obligations from 25 May 2018

7. Additional security

7.1 Confidentiality of processing. Worksuite shall ensure that any person that it authorizes to process the Personal Data shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

7.2 Security Incidents. Upon becoming aware of a Security Incident, Worksuite shall notify Customer without undue delay and shall provide such timely information as Customer may reasonably require, including to enable Customer to fulfil any data breach reporting obligations under EU Data Protection Legislation. Worksuite shall take appropriate and commercially reasonable steps to mitigate the effects of such a Security Incident on the Personal Data under this Agreement. **8. Sub-processing**

8.1 Sub-processors. Customer agrees that Worksuite may engage Worksuite affiliates and third party sub processors (collectively, "**Sub-processors**") to process the Personal Data on Worksuite's behalf. The Sub-processors currently engaged by Worksuite and authorized by Customer are available at https://worksuite.com/sub-processors/ . Customer shall be notified by Worksuite in advance of any new Sub-processor being appointed by changes to this website.

8.2 Objection to Sub-processors. Customer may object in writing to the appointment of an additional Sub-processor within five (5) calendar days after receipt of Worksuite's notice in accordance with the mechanism set out at Section 8.1 above. In the event that Customer objects on reasonable grounds relating to the protection of the Personal Data, then the parties shall discuss commercially reasonable alternative solutions in good faith. If no resolution can be reached, Worksuite will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected Worksuite service in accordance with the termination provisions of the Agreement.

8.3 Sub-processor obligations. Where a Sub-processor is engaged by Worksuite as described in this Section 8, Worksuite shall:

(a) restrict the Sub-processor's access to Personal Data only to what is necessary to perform the subcontracted services;

(b) impose on such Sub-processors data protection terms that protect the Personal Data to the

same standard provided for by this DPA; and

(c) remain liable for any breach of the DPA caused by a Sub-processor.

9. Cooperation

9.1 Cooperation and data subjects' rights. Worksuite shall, taking into account the nature of the processing, provide reasonable assistance to Customer insofar as this is possible, to enable Customer to respond to requests from a data subject seeking to exercise their rights under EU Data Protection Legislation. In the event that such request is made directly to Worksuite, Worksuite shall promptly inform Customer of the same.

9.2 Data Protection Impact Assessments. Worksuite shall, to the extent required by EU Data Protection Legislation and at Customer's expense, taking into account the nature of the processing and the information available to Worksuite, provide Customer with commercially reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under EU Data Protection Legislation.

10. Deletion / return of data

10.1 Deletion or return of data: Upon termination or expiry of the Agreement, Worksuite shall at Customer's election, delete or return to Customer the Personal Data (including copies) in Worksuite's possession, save to the extent that Worksuite is required by any applicable law to retain some or all of the Personal Data.

Part C: CCPA and VCDPA Obligations

11. The Parties acknowledge and agree that the processing of personal information or personal data that is subject to the CCPA or VCDPA shall be carried out in accordance with the terms set forth in Annex C.

[Signatures on Following Page]

SIGNED by the parties or their duly authorized representatives:

Customer Execution:

Customer Legal Name: _____ Worksuite Tenant URL: _____

Signed: _____

Name: _____

Title: _____

Date: _____

Worksuite Execution:

Signed: _____

Name: _____

Title: _____

Date: _____

ANNEX A
DESCRIPTION OF PROCESSING

Nature and purposes of processing

Worksuite is a US headquartered provider of cloud-based talent management tools and related services. These services will consist primarily of allowing the Customer to onboard and manage its talent, collecting information in talent profiles containing such content as are determined by the Customer in its sole discretion.

Otherwise, the data processing will involve any such processing that is necessary for the purposes set out in the Agreement, the DPA, or as otherwise agreed between the parties

Categories of data subjects

The personal data transferred concern any data subject who is a talent which the Customer instructs Worksuite to deliver and manage.

Categories of data

The personal data transferred concern the following categories of data for the data subjects:

- Talent identification information (first and last name), contact information (address, telephone number (fixed and mobile), e-mail address, fax number), employment information (job title); and
- Any other personal data that the Customer chooses to include within the talent profile using Worksuite's services.

The extent of personal data transferred to Worksuite for processing is determined and controlled by the Customer in its sole discretion. As such, Worksuite has no control over the volume and sensitivity of personal data processed through its service by the Customer.

Duration of processing

The personal data will be processed for the term of the Agreement, or as otherwise required by law or agreed between the parties.

ANNEX B
WORKSUITE SECURITY MEASURES

1. Network-Level Controls

(a) Worksuite or its hosting provider will use host-based firewall(s) to protect hosts/infrastructure handling Personal Data.
(b) Worksuite or its hosting provider will have network-based security monitoring for the segment(s) on which hosts handling Personal Data are logically located.
(c) Worksuite or its hosting provider will assess network-level vulnerabilities and address critical vulnerabilities within 30 days.
(d) Worksuite or its hosting provider will employ change management standards for network/infrastructure components handling Personal Data.

2. Hosting Level Controls

(a) Worksuite or its hosting provider will implement operating system hardening for hosts/infrastructure

handling Personal Data. Operating system hardening includes, but is not limited to, the following configurations: strong password authentication/use of keys, inactivity time-out, disabling or removal of unused or expired accounts and services, turning off unused ports, and log management. In addition, Worksuite will implement access control processes and restrict access to operating system configurations based on the least privilege principle.

(b) Worksuite or its hosting provider will perform patch management on systems that host or handle Personal Data. Worksuite will implement critical patches within vendor recommended timeframes on systems that host or handle Personal Data, not to exceed 30 days after the patch is identified.

(c) Worksuite or its hosting provider will implement specific controls to log activities of users with elevated access to systems that host or handle Personal Data.

(d) Worksuite or its hosting provider will, at a minimum, assess system-level vulnerabilities on a monthly basis and address critical vulnerabilities within 30 days.

(e) Worksuite or its hosting provider will employ a comprehensive antivirus or endpoint security solution for endpoints which handle Personal Data.

(f) Worksuite or its hosting provider will ensure physical servers will be protected with appropriate physical security mechanisms, including but not limited to badged access, locked cages, secure perimeter, cameras, alarms, and enforced user provisioning controls.

3. Application-Level Controls

(a) Worksuite will maintain documentation on overall application architecture, process flows, and security features for applications handling Personal Data.

(b) Worksuite will regularly perform patch management on applications that host or handle Personal Data. Worksuite will implement critical patches within vendor recommended timeframes on all applications that host or handle Personal Data, not to exceed 30 days.

(c) Worksuite will, at a minimum, assess application-level vulnerabilities on a monthly basis and address critical vulnerabilities within 30 days.

(d) Worksuite will perform code reviews for applications that host or handle Personal Data. (e) Worksuite will employ change management standards for applications hosting or handling Personal Data.

4. Compliance Controls

(a) Worksuite will make a good faith effort to operate within the parameters of Worksuite's then-current Information Security Policy.

(b) Notwithstanding any of the foregoing, Worksuite will adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to, building access control, employee education and personnel security measures.

Annex C
United States Privacy Law Annex

This United States Privacy Law Annex ("Annex") supplements the DPA and includes additional information required by the CCPA and the VCDPA, in each case, as updated, amended or replaced from time to time. Any terms not defined in this Annex shall have the meanings set forth in the DPA and/or the Agreement.

A. CALIFORNIA

1. Definitions

1.1 For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.

1.2 All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer," respectively, as defined in the CCPA.

2. Obligations

2.1 The Parties acknowledge and agree that Worksuite is a Service Provider for the purposes of the CCPA (to the extent it applies) and Worksuite is receiving Personal Information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

2.2 Customer is only disclosing Personal Information to Worksuite for the limited and specified purposes described in Annex A to this DPA.

2.3 Worksuite shall not Sell or Share Personal Information provided by Customer under the Agreement.

2.4 Worksuite shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services to Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.

2.5 Worksuite shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between Customer and Worksuite.

2.6 Worksuite shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.

2.7 Worksuite will not combine Personal Information received from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.8 Worksuite shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by CCPA.

2.9 Worksuite shall only engage a new subcontractor to assist Worksuite in providing the Services to Customer under the Agreement in accordance with Section 8.1 of the DPA, including, without limitation, by entering into a written contract with the subcontractor that requires such subcontractor to observe all of the applicable requirements set forth in the CCPA.

3. Consumer Rights

3.1 Worksuite shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's

rights under the CCPA as set forth in Section 9 of the DPA.

4. Audit Rights

4.1 Worksuite shall allow Customer to conduct inspections or audits to the extent permitted by applicable laws.

B. VIRGINIA

1. Definitions

1.1 For purposes of this Section B, the terms “Consumer,” “Controller,” “Personal Data,” “Processing,” and “Processor” shall have the meanings set forth in the VCDPA.

1.2 All references to “Data Subject” in this DPA shall be deemed to be references to “Consumer” as defined in the VCDPA.

2. Obligations

2.1 The Parties acknowledge and agree Worksuite is a Processor for the purposes of the VCDPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Annex A to this DPA.

2.3 Worksuite shall adhere to Customer’s instructions with respect to the Processing of Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

2.3.1 Assisting Customer in responding to Consumer rights requests under the VCDPA as set forth in Section 9 of the DPA;

2.3.1 Complying with Annex B of the DPA with respect to Personal Data provided by Customer;

2.3.2 In the event of a Security Incident, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2-186.6; and

2.3.3 Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

2.4 Worksuite shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

2.5 Upon Customer’s written request, Worksuite shall delete or return all Personal Data provided by Customer in accordance with Section 10 of the DPA.

2.6 Worksuite shall only engage a new subcontractor to assist Worksuite in providing the Services to Customer under the Agreement in accordance with Section 8.1 of the DPA, including, without limitation, by entering into a written contract with the subcontractor that requires such subcontractor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

3. Audit Rights

Upon Customer’s written request at reasonable intervals, Worksuite shall (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Worksuite’s compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.