United States Data Processing Agreement

This United States Data Processing Agreement ("DPA") is by and between (i) the UKG entity set forth in the Order that references the UKG Master Services Agreement, or any other currently effective agreement, (the "Agreement"), ("UKG"), and (ii) the person or entity who is named on such Order on behalf of itself as customer and Customer Affiliates based in the United States ("Customer") and sets forth the terms and conditions applicable to UKG's processing activities under the Agreement. Customer and UKG are referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, in the course of providing the Services to Customer pursuant to the Agreement, UKG may Process Personal information on behalf of Customer, and the Parties agree to comply with the following provisions with respect to the Processing of Customer Personal information.

This DPA applies to the extent Customer and/or its Affiliates are subject solely to U.S. Privacy Laws. Should Customer become subject to any other privacy laws such as the EU General Data Protection Regulation, the Parties agree the processing of Personal information will be subject to UKG's international Data Protection Addendum located at https://www.ukg.com/ukg-unified-dpa unless otherwise agreed to in writing by the Parties. UKG shall comply with all U.S. Privacy Laws applicable to it as a "Service Provider" or in its role as a processor of Personal information. Customer shall comply with all U.S. Privacy Laws applicable to it as a "Business" or the controller of Personal information. Notwithstanding, UKG is not responsible for complying with U.S. Privacy Laws applicable only to Customer or Customer's industry.

1. Definitions

1.1 In this DPA, capitalized terms will have the meanings set out below. Capitalized terms not otherwise defined below will have the meaning given to them in the Agreement.

"**Affiliates**" means, as to UKG, those entities that are directly or indirectly controlled by UKG Inc.; and as to Customer, those Customer entities that directly or indirectly control, are controlled by, or are under common control with Customer and which are doing business in the United States. "Control" (in this context) means the possession, directly or indirectly, of the power to direct or cause the direction of the management and operating policies of the entity in respect of which the determination is being made through the ownership of the majority of its voting or equity securities, contract, or otherwise.

"Applicable Laws" means any applicable provisions of all U.S. laws, codes, legislative acts, regulations, ordinances, rules of court, and court orders which govern the Party's respective business operations. UKG shall comply with all Applicable Laws applicable to UKG in its role as a Data Processor Processing Personal information. For the avoidance of doubt, UKG is not responsible for complying with Applicable Laws applicable to Customer or Customer's industry. Customer shall comply with all Applicable Laws to Customer as a Data Controller

"Core Subscription Services" means UKG Pro, UKG Pro Workforce Management, UKG Ready, and UKG Pro People Assist and UKG Pro Document Manager offerings identified in the Order.

"Data Subject" means an identified or identifiable natural person.

"**Personal Information**" means Customer Data related to a Data Subject as defined under U.S Privacy Laws, including "personal information" as defined under the California Consumer Privacy Act ("CCPA") and any similar terms, such as "personally identifiable information".

"**Processing**", "**Process**", "**Processes**" and "**Processed**" means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Schedule 1 to this DPA provides for details of the Processing.

"**Pseudonymized Data**" means the processing of Personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

"Services" means Core Services and any other UKG Products and Services.

"Subprocessor" means any person (including any third party and any UKG Affiliate) appointed by or on behalf of UKG to Process Personal information on behalf of Customer in connection with the Agreement, a list of which is available on ukg.com, and which is

incorporated herein by reference.

"UKG Processor" means UKG or a UKG Subprocessor.

"**UKG Other Products & Services**" means Professional Services and UKG products and services other than Core Subscription Services, which are subject to the specific Supplement for UKG Other Products and Services available on ukg.com.

"**U.S. Privacy Laws**" have the same meaning as in Applicable Laws and regulations concerning the privacy and security of information reasonably identifying or linked to an individual, including, without limitation, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. or its successor the California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq., and their accompanying regulations as promulgated by the California Attorney General or California Privacy Protection Agency, as then applicable (collectively the "CPRA"); the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1309 et seq. (the "CPA") the Connecticut Data Privacy Act, Public Act No. 22-15 (the "CTDPA"); the Utah Consumer Privacy Act, Utah Code § 13-61-101 et seq. (the "UCPA "); and the Virginia Consumer Data Protection Act, Virginia Code § 59.1-571 et seq. (the "VCDPA").

Where applicable, the terms, "**Service Provider"** "**Share**" and "**Sell**" will have the same meaning as in the California Consumer Privacy Act ("**CCPA**") or in US Privacy Laws.

2. Processing of Customer Personal information

2.1 UKG will only Process Personal information for the purpose, and in accordance with, the relevant Customer's instructions as documented in the Agreement and this DPA, unless Processing is required by the Applicable Laws to which the relevant UKG Processor is subject, in which case UKG to the extent permitted by the Applicable Laws, will inform Customer of that legal requirement before the Processing of that Customer Personal information.

2.2 UKG will not: (i) Sell or Share any Personal information; (ii) retain, use, or disclose such Personal information for any purpose other than performing the Services, the business purpose stated in the Agreement or as otherwise permitted by the U.S. Privacy Laws; (iii) retain, use, or disclose the Personal information for a commercial purpose other than providing the Services unless otherwise permitted under the Agreement; (iv) retain, use, or disclose Personal information outside of the direct business relationship between Customer and UKG unless otherwise permitted under the Agreement; (v) combine Personal information UKG receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons or collects from its own interaction with a consumer, provided that UKG may combine personal information to perform the Services or as set forth in the Agreement. UKG shall notify Customer if it makes a determination that it can no longer meet its obligations under U.S Privacy Laws and Customer may take reasonable and appropriate steps to stop and remediate the unauthorized Processing of Personal information. Customer may take reasonable and appropriate steps to ensure UKG uses Personal information collected pursuant to the Agreement and this DPA in a manner consistent with Customer's obligations under U.S Privacy Laws.

2.3 Customer hereby (i) instructs UKG (and authorizes UKG to instruct each Subprocessor) to (a) Process Personal information in accordance with Schedule 1; and (b) in particular, transfer Personal information to any country or territory as reasonably necessary for the provision of the Services and consistent with the Agreement, (ii) warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instructions set out in this section on behalf of each relevant Customer Affiliate; and (iii) warrants and represents that it has all necessary rights in relation to the Personal information and/or has collected all necessary consents from Data Subjects to Process Personal information to the extent required by Applicable Law.

3. UKG Personnel

UKG will take steps to ensure that access to Personal information is limited to those individuals who: (a) need to know or access the relevant Personal information as necessary for the purposes of providing the Services under the Agreement or to comply with Applicable Laws in the context of that individual's duties to UKG; and (b) are subject to written confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

UKG shall implement reasonable and appropriate safeguards to protect Personal information as set forth in Schedule 2 to this DPA and incorporated by this reference.

5. Subprocessing

5.1 Customer generally authorizes UKG to appoint Subprocessors in accordance with this Section 7, including without limitation those Subprocessors provided herein and any new Subprocessors. Subprocessors used for UKG Other Products and Services may be listed under each applicable Services Description or Order Form, in an addendum to this DPA, or in other form of communication.

5.2 UKG will provide Customer with a mechanism to obtain notification of the appointment of any new Subprocessor, including material details of the Processing to be undertaken by the Subprocessor at least thirty (30) days before said Subprocessor carries out Processing activities on Customer Personal information on behalf of Customer. Customer may object by email to privacy@ukg.com, on reasonable data protection grounds, to any new Subprocessor by providing notice of an objection to UKG within ten (10) days of Customer's receipt of notification of the addition of the new Subprocessor by UKG. In the event UKG, in its sole discretion, is unable to forego the utilization of a new Subprocessor that has been objected to for the Processing of Customer Personal information or is otherwise unable to reasonably address the Customer's objection within thirty (30) days of UKG's receipt of such objection from Customer, the Customer may terminate the impacted services upon written notice to UKG. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor, and is not a termination for cause. UKG will cease providing the impacted services thirty (30) days following the notice of termination.

5.3 With respect to each Subprocessor, UKG will verify that the arrangement between UKG and the Subprocessor is governed by a written contract including terms which offer at least equivalent level of protection for Customer Personal information as those set out in this DPA**.**

6. Data Subject Requests

6.1 If Customer receives a request from a Data Subject related to Personal information Processed by UKG, Customer can either: (a) retrieve the information necessary to fulfill the request from the Services; or (b) to the extent such information is not available to Customer through the Services, UKG will reasonably assist Customer in fulfilling the request upon written request.

6.2 If UKG receives a request from a Data Subject related to Personal information Processed by UKG , UKG will promptly redirect the Data Subject to its Customer and not respond to the request except on the documented instructions of Customer or as required by Applicable Laws to which UKG is subject, in which case UKG, to the extent permitted by the Applicable Laws, shall inform Customer of that legal requirement before UKG responds to the Data Subject request.

7. Personal information Breach

7.1 UKG will notify Customer without undue delay and in accordance with U.S. Privacy Laws upon UKG or any Subprocessor becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal information transmitted, stored or otherwise processed by UKG ("**Personal information Breach**") affecting Personal information, providing Customer with sufficient information to allow Customer to meet its obligations to report or inform Data Subjects of the Personal information Breach under the U.S. Privacy Laws.

7.2 In the event of a Personal information Breach, the Parties will reasonably cooperate with each other, and UKG shall take commercially reasonable steps to keep Customer informed as to the investigation, mitigation, and remediation of any such Personal information Breach.

7.3 Except as may be required by Applicable Laws, UKG will not notify Customer's affected Data Subjects about a Personal information Breach without Customer's prior written consent.

8. Deletion or Return of Customer Personal information

8.1 Subject to Sections 9.2 and 9.3, following the latter of either (i) termination or expiration of the Agreement or (ii) cessation of the Processing of Customer Personal information, (the "Cessation Date"), UKG will, in accordance with the terms of the Agreement, promptly return or delete Customer Personal information that can be reasonably identified and extracted in accordance with the requirements of the relevant Applicable Laws.

8.2 Notwithstanding Section 9.1 above, each UKG Processor may retain Personal information to the extent and for such period as required by Applicable Laws, provided that UKG will ensure the confidentiality of all such Personal information and will ensure that such Personal information is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage.

8.3 Upon receipt of written request from Customer, UKG will provide written certification to Customer that it has complied with this Section 9.

9. Audit rights

UKG shall demonstrate appropriate technical and organizational measures to Customer throughout the term. Customer may exercise such audit right either personally or by appointing a third party, so long as said third party is acceptable to UKG and bound to confidentiality and non-disclosure obligations at least as stringent as Customer's obligations with respect to UKG Confidential Information as set forth in the Agreement. Customer is responsible and liable for any and all acts or omissions of any such third

party. Customer may exercise such audit right either personally or by appointing a third party that is bound by appropriate obligations of confidentiality and acceptable to UKG. Customer may exercise such audit right on an annual basis with reasonable notice. Any such audits shall be limited to a robust customer due diligence package consisting of details on UKG' information security/risk practices, examination of the results of the annual AICPA SSAE 18 SOC 1 and SOC 2 Type II audits conducted by an independent third party, executive summaries of the annual penetration test results or verification of such testing through the SOC 2 report for Core Subscription Services, and reasonable access to knowledgeable personnel to discuss the controls in place, including a meeting at UKG corporate headquarters. In the event Customer requests support or information beyond the content described above, then, upon customer's audit request, the Parties will mutually agree on the terms of the audit plan, which shall include details regarding the scope, duration, fees, and scheduling of the audit. In no event shall Customer or its designees be permitted to access UKG systems, network servers, scan summaries or activities logs.

10. Law Enforcement Requests

UKG agrees to notify Customer of any request from law enforcement authority or other governmental authority with competent authority and jurisdiction over UKG for disclosure of Customer Personal information processed under this DPA ("Disclosure Request") to the extent permitted by applicable law. UKG shall not respond to Disclosure Requests without notifying Customer and receiving written authorization from Customer to respond to such Disclosure Request, except as required under Applicable Laws or order of court or governmental authority with competent authority and jurisdiction over same.

11. General Terms

11.1 DPA Priority. Nothing in this DPA reduces UKG's obligations under the Agreement in relation to the protection of Personal information or permits UKG to Process (or permit the Processing of) Personal information in a manner which is prohibited by the Agreement. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA will prevail.

11.2 Claims. Any claims brought under this DPA shall be subject to the terms and conditions of the Agreement, including but not limited to, the exclusions and limitations set forth in the Agreement.

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

11.4 This DPA supersedes all prior and contemporaneous representations, negotiations, and communications between the Parties relating to processing Customer Personal Data, including without limitation, any terms that may be imposed upon UKG by means of any "click-through", forms, applications, or any other terms and conditions which are presented to UKG in the course of UKG's engagement with Customer.

Schedule 1: Details of Processing of Customer Personal Data

This Schedule 1 includes certain details of the Processing of Customer Personal Data.

Subject matter and duration of the Processing of Customer Personal Data

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

The nature and purpose of the Processing of Customer Personal Data

Provision of the Services are set out in the Agreement and this DPA, where UKG acts as a data processor, and for business operations, as an independent controller. UKG will use and otherwise process Customer Data only as described and subject to the limitations provided below (a) to provide Customer the Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Services to Customer.

Processing to Provide Customer the Services

For purposes of this DPA, "to provide" a Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Keeping Services up to date and operational, and enhancing user productivity, reliability, efficacy, quality, and security.

When providing Services, UKG will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar business purposes, or (c) sell or share Personal Data.

Processing for Business Operations Incident to Providing the Services to Customer

For purposes of this DPA, "business operations" means the processing operations authorized by Customer in this section.

Customer authorizes UKG:

- to create aggregated statistical, non-personal data from data containing Pseudonymized identifiers (such as usage logs containing unique, Pseudonymized identifiers);
- to calculate statistics related to Customer Data; and
- to de-identify Customer Data to enhance and create new functionalities.

in each case limited to to providing the Services, such as billing and account management; internal reporting and business modeling, and product strategy; and enhancing Customer's experience.

When processing for these incident business operations, UKG will apply principles of data minimization, confidentiality and will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, (c) any other purpose, other than for the purposes set out in this section or (d) Sell or Share Personal Data.

The types of Customer Personal Data to be Processed

All Customer Personal Data required by UKG to correctly provide the Services to Customer pursuant to the Agreement which may include, without limitation: employee first and last name, employee ID number, department code, badge number, job title, absence information, identification and contact information of Customer data subjects, employment and education details of Customer data subjects, other information that Customer may collect in order to pay and manage its workforce.

The categories of Data Subject to whom the Customer Personal Data relates

Customer's employees, contractors, and job applicants.

Special categories of Customer Personal Data to be Processed

None unless otherwise specified or unless special categories of personal data including without limitation biometric data collection is enabled by Customer on given UKG offerings.

The obligations and rights of Customer

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

Privacy related contact:

UKG: privacy@ukg.com

Customer: As specified in this DPA, in the Order Form or in the Statement of Work.

Schedule 2: Technical and Organizational Measures

The following Technical and Organizational Measures are applicable to UKG Core Subscription Services. The specific Supplement for UKG Other Products and Services to this DPA is applicable to any UKG Other Products & Services.

1. ISAE3402 /SSAE 18 (SOC 2) Audit: UKG shall ensure compliance with ISAE3402/SSAE 18 AICPA Trust Principles for Security, Confidentiality, and Availability (and, where in scope, Privacy and Processing Integrity), and will undergo an audit each year for the purposes of examining the relevant controls with respect to the Services. Such audits shall be carried out by an independent, certified third party and the resulting reports shall be provided to Customer upon request. UKG shall ensure the data center carries out its own SOC 2 audits and provide such reports to Customer upon request.

2. ISO 27000 Series Audits: UKG shall ensure compliance with ISO 27001, 27017, and 27018, where in scope for the UKG Services. UKG shall also ensure the datacenter used to provide the Services will continue to have its IT security management certified according to ISO 27001 or comparable industry standard security framework. The audits shall be carried out by an independent, certified third party, and upon request, UKG shall provide the certificates to Customer.

3. Entity Controls: Consistent with UKG's obligation to maintain its compliance programs as described above, UKG shall continuously carry out the following security measures:

a) Security Policy: UKG shall maintain an information security policy that is reviewed annually by UKG and published and communicated to all UKG employees. UKG shall maintain a dedicated security and compliance function to maintain and monitor security controls across UKG.

b) Employee Onboarding: All UKG personnel shall be subject to a comprehensive background check and agree to accept UKG's Code of Conduct upon hire.

c) Employee Termination: UKG shall terminate all credentials and access to the Services of a UKG employee in the event of termination of his or her employment within a reasonably timely manner.

d) Access Controls by UKG Personnel: Access to all UKG owned or licensed network components, servers, databases, computers, and software programs by UKG personnel shall be protected by an authentication procedure that requires giving at least a unique username and complex password. UKG shall implement technical controls to enforce a password policy consisting of a minimum number of characters and complexity, including requirements of alpha, numeric, upper case, lower case and/or special characters. Lockout periods shall be in effect for inactivity and unsuccessful password attempts. Passwords shall expire after a fixed amount of time.

e) Security Awareness Training: UKG employees shall participate in security awareness and privacy training, upon hire and annually thereafter.

f) Change Management: UKG shall employ a change management process based on industry accepted standards for change management in configurations, software, and hardware.

4. Application and Network Controls:

a) Privileged Access by UKG Personnel: Privileged access to UKG owned or licensed network components, servers, databases, computers, and software programs by UKG personnel that are used in the provision of the Services shall be secured by means of a two-factor authentication and shall be defined by UKG in such a manner as to ensure that the access authorizations are granted only to the extent necessary to perform the assigned role. Any access to UKG's systems used in the provision of the Services shall be monitored.

b) Infrastructure of the Data Center: UKG and/or its sub-processor(s) shall monitor the infrastructure in order to identify any security vulnerabilities.

c) Anti-Virus and Malware Scanning: UKG uses commercially available malicious code detection software, including virus detection and malware detectors, on UKG systems. Anti-virus definition files shall be updated regularly, on a scheduled basis, following the availability of such updates by the software provider.

d) Secure Coding Practices: UKG developers shall be trained on secure development. Applications should be written in a secure manner to implement industry practices, such as input validation, session management, SQL injection, and cross site scripting mitigation. These practices shall be tested as part of the annual penetration testing described below.

e) Patch Management: UKG shall review all patches, updates, and upgrades of operating systems, middleware, or applications to all relevant components of the Services after they have been released by the manufacturer and tested by UKG. UKG shall manage the patching process prudently to assure that critical patches are applied in a timely manner consistent with the associated risk.

f) Segregation of Customer Data: UKG shall provide appropriate security controls and segmentation methods to protect and isolate Customer Data from other tenants.

g) Encrypted Data Transfers: Customer Data input into the Services shall be secured using an industry standard protocol, such as Transport Layer Security (TLS).

h) Encrypted Data Storage: UKG shall encrypt Customer Data using industry standard technology, such as AES-256 encryption standard for data at rest.

i) Firewalls: Connections to the Services networks, shall be protected with industry standard firewalls. UKG shall update its firewall software regularly, on a scheduled basis, following the availability of updates by the software provider.
j) Intrusion Detection: UKG shall implement and maintain an intrusion detection monitoring process at the network and/or host level to protect the Services and detect unwanted or hostile network traffic. UKG shall update its intrusion detection software regularly, on a scheduled basis, following the availability of updates by the software provider or a heuristic analysis shall be used.
k) Systems Hardening and Secure Configuration: UKG shall follow industry standards for platform hardening and secure configuration. UKG shall remove or disable unnecessary utilities from operating system configurations and restrict access rights to least privilege.
l) Penetration Testing: UKG shall contract, as part of its security program and on at least an annual basis, with an independent third party to conduct a network and application penetration test. The penetration test will include, but is not limited to, the potential for unauthorized internet access, compromise of roles, and escalation of privileges for the Services. Upon request, UKG will provide an executive summary of said penetration test including the scope and methodology of the test and confirmation that critical and high-risk findings have been remediated or provide an independent third-party audit report attesting to such testing and remediation. Penetration testing includes the web application vulnerabilities defined by the Open Web Application Security Project (OWASP) Top 10 and those listed in the SANS 25 (as applicable) or its successor current at the time of the test.
m) Vulnerability Management: UKG shall implement commercially reasonable processes designed to protect Customer Data from system vulnerabilities. UKG shall perform scanning of the infrastructure using an industry recognized automated scanning tool designed to detect security flaws and security vulnerabilities within the operating systems. UKG shall assess scan results and remediate relevant security vulnerabilities within a reasonable amount of time based on the risk to the Services.
n) Audit Logging: UKG shall log UKG personnel's access to the Services to maintain an audit trail that includes, but is not limited to, web server logs, system logs, and network event logs.

5. Physical Access Control: UKG shall ensure that its data center sub-processor uses industry standard technology to ensure that only the appropriately authorized staff have access to those systems of UKG that are used to provide the Services. This shall include at least the following measures: visitor sign-ins, role-based access controls, limited access to the server rooms and to the alarm systems which report any unauthorized access.

6. Security Monitoring: UKG may monitor and analyze the use of its Subscription Services, which may record information concerning security controls and compliant use of the application, the events that occur within the application, aggregated usage, performance data, and access locations. The Subscription Services will collect usage statistics, telemetry, and other data from Customer, such as mobile number, email address, IP address, and other unique verification identifier, for the purposes of enabling multifactor authentication; benchmarking, modelling, and training; providing, operating, maintaining, customizing, and improving the Subscription Services and its security, including by developing new or different functionalities for such purposes.

7. Incident Response and Notification:
a) UKG shall maintain security incident management policies and procedures, including security incident escalation procedures. In the event UKG confirms unauthorized access or acquisition, disclosure or use of Customer's Personal information has occurred, UKG agrees to notify Customer, in accordance with the terms of the Agreement or per Applicable Laws.
b) UKG shall (i) investigate such information security incident and perform a root cause analysis; (ii) remediate the effects of such information security incident; and (iii) provide Customer with assurances that such information security incident is not likely to recur.

8. Disaster Recovery: UKG shall maintain a Disaster Recovery plan and present verification of this plan (via the SOC 2 reporting) at the request of Customer. UKG shall test this plan once a year and verify that the planned measures are effective, reviewed by management and updated as necessary.

9. Business Continuity: UKG shall maintain a plan for returning to operation in the event of a disaster and present a summary of this plan at the request of Customer. Upon UKG's declaration of disaster, UKG shall implement said plan to return the Services to operation. UKG shall annually test and review its business continuity plan and update as necessary.