Data Processing Addendum

This Data Processing Addendum ("DPA") is by and between Supplier on behalf of itself and Supplier Affiliates ("Supplier") and UKG signing entity of the Agreement, UKG Inc. and UKG Affiliates, ("UKG") and is an addendum to that certain agreement by and between Supplier and UKG, as amended or supplemented, (the "Agreement"). Supplier and UKG are referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, in the course of providing Services under the Agreement, Supplier may Process UKG Personal Data passed from UKG to Supplier, and the Parties agree to comply with the following provisions with respect to the Processing of UKG Personal Data. UKG Personal Data includes 1) the Personal Data controlled by UKG (e.g., UKG employees, contractors, job applicants, etc.) and 2) Personal Data of UKG End-User Customers Processed by UKG.

NOW THEREFORE, in consideration of the mutual covenants contained herein and for other good and valuable consideration, the respective receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. General

1.1 The above and foregoing recitals are true and correct and incorporated herein by reference.

1.2 This DPA consists of the terms and conditions set forth in this DPA and the following Schedules, which are attached hereto and incorporated herein by reference:

1.2.1 Schedule 1: Details of the Processing

1.2.2 Schedule 2: Technical and Organizational Security Measures

1.2.3 Schedule 3: Subprocessors

1.2.4 Schedule 4: Additional Applicable Privacy Provisions

2. Definitions

2.1 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.

"**Applicable Law(s)**" means any applicable provisions of all laws, codes, legislative acts, regulations, ordinances, rules, rules of court, case law, guidelines, regulatory orders and any orders which govern the Party's respective business.

"**Countries with Adequate Protection**" means third countries, territories or specified sectors within a third country, which:

- (1) for data Processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR;
- (2) for data Processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or
- (3) for data Processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.

"Cross-Border Transfer Mechanism" means applicable legally valid mechanisms required for the transfer of UKG Personal Data where applicable Data Protection Laws require a legal mechanism for cross-border transfer. Such mechanisms include, by way of example and without limitation, the Standard Contractual Clauses. The EU SCCs (Processor-to-Processor) and (Controller-to-Processor) and the UK IDTA, as applicable, are available at https://www.ukg.com/ukg-supplier-sccs, and are deemed incorporated in this DPA, in accordance with Section 11 of the DPA.

"Data Protection Laws" means (a) GDPR, and (b) any other Applicable Laws regarding protection of UKG Personal Data.

"GDPR" means EU General Data Protection Regulation 2016/679.

"Restricted Transfer" means a transfer of UKG Personal Data from UKG to a Supplier Processor, or a transfer of such data between Supplier Processors, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer

agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of a Cross-Border Transfer Mechanism.

"Services" means the services and other activities to be supplied to or carried out by or on behalf of Supplier for UKG pursuant to the Agreement.

"Standard Contractual Clauses" or **"SCCs"** means any type or module of standard contractual clauses approved by any relevant authority such as the European Commission in Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries, the British Data Protection Authority, the Swiss Data Protection Authority or the Singapore Data Protection Authority, including those executed between Supplier Affiliates (Module 3). The EU SCCs (Processor-to-Processor) and (Controller-to-Processor), as applicable, are available at https://www.ukg.com/ukg-supplier-sccs and are deemed incorporated in this DPA, in accordance with Section 11 below.

"Subprocessor" means any person (including any third party and any Supplier Affiliate) appointed by or on behalf of Supplier to Process UKG Personal Data passed from UKG to Supplier in connection with the Agreement.

"UKG Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with UKG, where control is defined as the possession, directly or indirectly, of 50% or more of the voting or equity securities, contract, voting trust or otherwise.

"UKG End-User Customers" means UKG's customers using UKG products and services.

"UKG Personal Data" means any Personal Data Processed by Supplier on UKG's behalf or sub-processed on behalf of UKG End-User Customers pursuant to or in connection with the Agreement.

"Supplier Processor" means Supplier or a Supplier Subprocessor.

2.2 The terms, **"Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Personal Information", "Processing", "Processor",** and **"Supervisory Authority"**, will have the same meaning as in the GDPR, or the equivalent meaning as set forth in applicable Data Protection Laws, and **"Processing"** shall be interpreted to include the following as applicable **"Process"**, **"Processes"** and **"Processed"**.

2.3 The terms, **"Service Provider" "Sell", and "Share"** will have the same meaning as in the California Consumer Privacy Act as amended, modified or reenacted from time to time (**"CCPA"**).

3. Processing of UKG Personal Data

3.1 Supplier will:

3.1.1 comply with all applicable Data Protection Laws in the Processing of UKG Personal Data;

3.1.2 provide UKG with full and prompt cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that UKG is legally required to make in respect of UKG Personal Data; and

3.1.3 not Process UKG Personal Data other than for the purpose, and in accordance with, the relevant UKG instructions as documented in the Agreement and this DPA, unless Processing is required by the Data Protection Laws to which the Supplier is subject, in which case Supplier to the extent permitted by the Data Protection Laws, will inform UKG of that legal requirement before the Processing of that UKG Personal Data.

3.2 UKG hereby:

3.2.1 instructs Supplier (and authorizes Supplier to instruct each Subprocessor) to: (a) Process UKG Personal Data; and (b) in particular, transfer UKG Personal Data to any country or territory, in each case as reasonably necessary for the provision of the Services and consistent with the Agreement; and

3.2.2 agrees that it is and will at all relevant times remain duly and effectively authorized to give the instructions set out in Section 3.2.1.

3.3 Schedule 1 to this Addendum sets out certain information regarding the Supplier's Processing of UKG Personal Data as required by Article 28(3) of the GDPR (and equivalent requirements of other Data Protection Laws).

4. Supplier Personnel

Supplier will take steps to ensure that access to UKG Personal Data is limited to those individuals who: (a) need to know or access the relevant UKG Personal Data as necessary for the purposes of providing the Services under the Agreement or to comply with Data Protection Laws in the context of that individual's duties to Supplier; and (b) are subject to written confidentiality undertakings or professional or statutory obligations of confidentiality; and (c) receive regular training and awareness on privacy and data protection (including but not limited to Data Protection Laws).

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier will in relation to the UKG Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk as set forth in Schedule 2 to this DPA.

5.2 In assessing the appropriate level of security, Supplier will take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

6.1 UKG generally authorizes Supplier to appoint Subprocessors in accordance with this Section 6, including without limitation those Subprocessors set forth in Schedule 3 and any new Subprocessors.

6.2 At least thirty (30) days before any new Subprocessor carries out Processing activities on UKG Personal Data, Supplier will provide UKG with written notification of the appointment of said new Subprocessor, including material details of the Processing to be undertaken by the Subprocessor. UKG may object, on reasonable data protection grounds, to any new Subprocessor by providing notice of an objection to Supplier. In the event Supplier does not, in the reasonable discretion of UKG, cure such objection or cease to permit such Subprocessor to Process UKG Personal Data, UKG may (i) request the suspension of the Processing of UKG Personal Data and/or (ii) may terminate this DPA and the Agreement.

6.3 With respect to each Subprocessor, Supplier will:

6.3.1 verify that the arrangement between Supplier and the Subprocessor is governed by a written contract including terms which offer at least equivalent level of protection for UKG Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR; and

6.3.2 if that arrangement involves a Restricted Transfer, guarantees that the Standard Contractual Clauses, or other legally valid Cross-Border Transfer Mechanism, are at all relevant times incorporated into the relevant agreement(s) between Supplier and the Subprocessor, coupled where required with additional measures to comply with Data Protection Laws.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Supplier will assist UKG by implementing appropriate technical and organizational measures for the fulfilment of UKG's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 If Supplier receives a request from a Data Subject under any Data Protection Law in respect of UKG Personal Data ("Data Subject Request"), Supplier will:

7.2.1 without undue delay redirect the Data Subject to UKG; and

7.2.2 ensure that Supplier does not respond to that Data Subject Request except on the documented instructions of UKG or as required by Data Protection Laws to which Supplier is subject, in which case Supplier, to the extent permitted by the Data Protection Laws, shall inform UKG of that legal requirement before Supplier responds to the Data Subject request.

8. Personal Data Breach

8.1 Supplier will notify UKG without undue delay and in accordance with Data Protection Laws upon Supplier or any Subprocessor

becoming aware of (a) any instruction which, in its opinion, infringes applicable law and (b) without undue delay and in any event within twenty-four (24) hours of a Personal Data Breach affecting UKG Personal Data, providing UKG with sufficient information to allow UKG to meet its obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 In the event of a Personal Data Breach, the Parties will reasonably cooperate with each other, and Supplier shall (1) investigate, mitigate and remediate any such Personal Data Breach and (2) take commercially reasonable steps to keep UKG informed as to the investigation, mitigation and remediation of any such Personal Data Breach.

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

9. Deletion or return of UKG Personal Data

9.1 Subject to Sections 9.2 and 9.3, following the later of (i) termination or expiration of the Agreement or (ii) the Processing of UKG Personal Data, (the "Cessation Date"), Supplier will, in accordance with the terms of the Agreement, without undue delay return or securely delete UKG Personal Data in accordance with the requirements of the relevant Data Protection Laws. Supplier shall provide UKG a certificate of destruction signed by a duly authorized officer.

9.2 Notwithstanding Section 9.1 above, each Supplier Processor may retain UKG Personal Data to the extent required by Data Protection Laws and only to the extent and for such period as required by Data Protection Laws, provided that (1) Supplier will ensure the confidentiality of all such UKG Personal Data, (2) ensure continued compliance with this DPA for as long as it retains UKG Personal Data in accordance with this clause 9.2 and (3) will ensure that such UKG Personal Data is only Processed as necessary for the purpose(s) specified in the Data Protection Laws requiring its storage.

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

10. Audit rights

Supplier will at the request of UKG, agree to submit its data processing facilities for audits and allow for inspections of the Processing activities covered by this DPA, which may be carried out by UKG or a regulated End-User Customer (when a government or regulatory body with binding authority ("Regulator") regulates such entity's regulated services, such as under the EBA guidelines) or any independent or impartial inspection agents or auditors selected by UKG or a regulated End-User Customer and not reasonably objected to by the Supplier, and will allow UKG to provide any audit reports to its End-User Customers where required.

11. Restricted Transfers and Cross-Border Transfer

Supplier will only operate cross-border transfers of UKG Personal Data (i) either to Countries with Adequate Protection; or (ii) based on a Cross-Border Transfer Mechanism coupled with any additional measures required by Data Protection Laws. Should UKG assess that a Cross-Border Mechanism is no longer valid, UKG shall be entitled to terminate the Agreement, without prejudice to any other available remedy.

12. Additional Assurances

12.1 Supplier shall maintain any additional safeguards to comply with the requirements of Applicable Laws, including ones listed under the UKG Supplier Code of Conduct, as incorporated into the Agreement, and the following additional safeguards with respect to UKG Personal Data:

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

12.1.2 In the event Supplier receives a Disclosure Request for disclosure of UKG Personal Data Processed under this DPA and Supplier is not legally permitted to notify UKG of the Disclosure Request, Supplier agrees to take reasonable legal actions against the disclosure of UKG Personal Data (including but not limited to challenging and redirecting such Disclosure Request and to refrain from disclosure of UKG Personal Data to the respective authorities until a court of

competent jurisdiction orders Supplier to disclose such UKG Personal Data. In such event, Supplier agrees to provide the minimum amount of information required when responding to the Disclosure Request; and

12.1.3 Supplier will encrypt UKG Personal Data when stored and while it is transmitted. Supplier limits access to and encrypts its encryption keys.

12.2 Upon request, Supplier will make available to UKG a transfer impact assessment complying with the requirements of Applicable Laws to assist UKG in carrying out its own transfer impact assessment related to UKG's use of the Services.

13. Liability & Indemnification

Supplier agrees to indemnify, defend, and hold harmless UKG and its officers, directors, employees, and agents ("Indemnified Party") from and against any and all losses, liabilities, judgments, awards, settlements, damages, fines, expenses and costs (including, but not limited to, reasonable attorney's fees and related court costs and expenses) (collectively, "Damages") arising from or relating to (i) Supplier's breach of its obligations under this DPA and/or (ii) Supplier's violation of Data Protection Laws. The foregoing indemnification obligations shall not be subject to any limitations on liability or exclusions of consequential damages in the Agreement. For the avoidance of doubt, nothing contained in this DPA or the Agreement shall be interpreted or attempt to reduce, exclude, or limit Supplier's liability towards a Data Subject.

14. General Terms

14.1 Governing Law. Without prejudice to clauses 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) of the Standard Contractual Clauses:

14.1.1 the Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

14.1.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

14.2 Cross-Border Transfer Mechanism Priority. In the event of any conflict or inconsistency between this DPA and the Cross-Border Transfer Mechanism, the Cross-Border Transfer Mechanism shall prevail.

14.3 DPA Priority. Nothing in this DPA reduces Supplier's obligations under the Agreement in relation to the protection of UKG Personal Data or permits Supplier to Process (or permit the Processing of) UKG Personal Data 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.

14.4 Amendment. This DPA may only be amended in a writing signed by both Parties.

14.5 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.

14.6 Survival. The obligations set forth in this DPA shall survive any termination of this DPA or the Agreement.

IN WITNESS WHEREOF, the Parties have executed this DPA as of the last day signed below by their duly authorized representatives for and on behalf of said entity.

Supplier:	**UKG** [Inc./Local Entity]**:**
_____	. _____
By: _____	By: _____

Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Privacy related contact:

UKG: privacy@ukg.com

Supplier: *(please specify)*

Schedule 1: Details of Processing of UKG Personal Data

This Schedule 1 includes certain details of the Processing of UKG Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of UKG Personal Data

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

The nature and purpose of the Processing of UKG Personal Data

Provision of the Services and purpose as set out in the Agreement and this DPA.

The types of UKG Personal Data to be Processed

All UKG Personal Data required by Supplier to provide the Services to UKG pursuant to the Agreement which may include, without limitation:

☒ UKG Employees' names and contact information, including addresses, emails, phone numbers, IP addresses, employment history, education/qualifications, transaction history, employees' dependents' names and contact information.

☒ UKG End User Customers' employee first and last name, employee ID number, department code, badge number, job title, absence information, identification and contact information of End User Customer data subjects, employment and education details of End User Customer data subjects, other information that End User Customer may collect in order to pay and manage its workforce.

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

☒ UKG current, former, prospective employees, job applicants, contractors, employee dependents

☒ End User Customer current, former, prospective employees, job applicants, contractors, employee dependents

Special categories of data (if appropriate)

The Personal Data transferred concerns the following special categories of data (please specify):

☒ None.

☐ If you are using / transferring any information about children or an individual's racial/ethnic origin; health; sexuality; political opinions; religious beliefs; criminal background or alleged offences; or trade union membership, this should be noted here: Please elaborate:

The obligations and rights of Supplier

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

Schedule 2: Technical and Organizational Measures

This Schedule 2 forms part of the DPA and summarizes the technical, organizational, and physical security measures implemented by Supplier in accordance with the DPA and the applicable Cross-Border Transfer Mechanism.

In addition to any data security requirements set forth in the Agreement as amended by the DPA, Supplier shall comply with the following, unless otherwise indicated below and approved by UKG.

1. **Risk Management**

1.1 Supplier will maintain and comply with a data security program, which at all times (i) complies with an appropriate industry standard framework, such as ISO/IEC 27001 or NIST, (ii) complies with all applicable laws, rules, and regulations; (iii) identifies, assesses, and manages risks to UKG Personal Data and Supplier's systems supporting the Services and (iv) includes appropriate administrative, technical, physical, organizational, and operational safeguards and other security and privacy measures and controls that establish minimum required standards related to the safeguarding of UKG Personal Data and which will protect the security and confidentiality of UKG Personal Data (collectively, the "**Data Security Program**") from a Personal Data Breach. The Supplier will regularly review and update the Data Security Program. Upon UKG's request, Supplier will provide UKG with a copy of the Data Security Program. Supplier will have a dedicated individual who is responsible for the information security controls and processes of Supplier.

1.2 Supplier will conduct an information security risk assessment at least once annually and manage risks related to UKG Personal Data and Supplier's systems supporting the Services in accordance with documented risk management procedures.

1.3 Supplier will conduct internal and external vulnerability scans against Supplier's infrastructure and applications at least one time per year in accordance with their risk to UKG, to help identify vulnerabilities and promptly remediate any security vulnerabilities and misconfiguration.

1.4 At least once per year, Supplier will conduct penetration testing (using independent testing professionals) of all of Supplier's external network and Supplier's applications and systems used to Process UKG Personal Data, and Supplier will promptly remediate any identified vulnerabilities. Upon UKG's request, Supplier will provide UKG a copy of the results of the penetration test(s).

2. **Human Resources Security**

2.1 Supplier will ensure that Supplier's personnel have received a background check upon hiring, in accordance with Supplier's internal policies.

2.2 Supplier will ensure that Supplier's personnel complete information security awareness training on an annual basis, or more frequently as needed, with regards to information security and the handling of UKG Personal Data.

2.3 Supplier will require all of Supplier's personnel to keep all UKG Personal Data confidential in accordance with the terms of the Agreement and will use UKG Personal Data solely as necessary to perform the Services to UKG.

3. **Asset and Information Management**

3.1 Supplier will maintain an inventory of IT assets supporting the Services including internal and external systems.

3.2 Supplier will apply and maintain industry standard-based security or prevention measures (e.g., anti-tampering, air gapping, etc.).

4. **Access Control**

4.1 Supplier will ensure that requests to grant access to UKG Personal Data or systems follow approved, formal processes, and that access to UKG Personal Data is limited to only those individuals whose job requires such access, i.e., least privileged access principle.

4.2 Supplier will approve and document all new access to network, systems, and data.

4.3 Supplier will assign to each of Supplier's personnel unique authentication credentials, by utilizing usernames and passwords, and as needed, digital certificates, tokens, and smartcards.

4.4 Supplier will implement identity and access management processes to control access and authenticate users prior to granting access.

4.5 Supplier will use multi-factor authentication for internet facing or external access to systems containing UKG Personal Data.

4.6 Supplier will immediately (and in any event no less than 24 hours) revoke access to UKG Personal Data for Supplier's personnel no longer working on the Services or those that no longer require access.

4.7 On a quarterly basis, Supplier will review user accounts and their privileges, to verify that access to its systems supporting the Services is correct.

4.8 Supplier will enforce the use of password complexity, minimum length of 12 characters and lockout after 5 unsuccessful login attempts. All passwords will be changed at least every 90 days.

4.9 Supplier will ensure that remote access to its systems and networks supporting the Services is restricted to only authorized individuals using secure entry-points and approved devices.

5. **Physical and Environmental Security**

5.1 If data centers used by Supplier use a card-key access control system, Supplier will ensure that only appropriate personnel are issued card keys.

5.2 Supplier will ensure that all visitors to its data center are required to sign a log and visitors are escorted by data center personnel.

5.3 Supplier will ensure that its data centers employ security surveillance cameras which record all activity at the data center.

6. **Data Security**

6.1 Supplier will maintain procedures and controls to protect the security of UKG Personal Data at every stage of its lifecycle, from creation through Processing, storage, and disposal.

6.2 Supplier will logically segregate all UKG Personal Data from the data of Supplier's other customers.

6.3 Supplier will use full-disk encryption for all UKG Personal Data at rest, using at least AES 256.

6.4 Supplier will encrypt all UKG Personal Data in transit and at rest with at least TLS 1.2.

6.5 Supplier will maintain the security of systems and employee laptops using standardized builds that include a hardened operating system, malware protection, and host-based security software.

6.6 Supplier will ensure that all system configuration changes are limited to authorized individuals, in accordance with documented change management procedures and using approved systems and tools.

6.7 On request by UKG, Supplier will either return all UKG Personal Data in a format requested by UKG or securely delete UKG Personal Data from its systems in accordance with current industry standards such as NIST 800-88 or an equivalent.

6.8 Supplier will follow industry standard encryption key management procedures.

7. **Application Security**

7.1 Supplier will maintain a secure systems development life cycle process for Supplier's systems that Process or store UKG Personal Data, including at a minimum:

(a) evidence of a secure code review process;

(b) perform periodic application penetration and vulnerability test executed by a specialized third party;

(c) implement a procedure that results in timely resolution of all discovered critical, high and medium risk vulnerabilities; and

(d) a security checkpoint in change management.

7.2 Supplier will apply patch management, vulnerability assessment, strong access control and system hardening measures in accordance with industry best practices.

7.3 Supplier will provide to UKG upon UKG's request, evidence that periodic application penetration tests are performed and discovered vulnerabilities are remediated in a timely manner.

8. **Security Monitoring and Detection**

8.1 Supplier will perform security monitoring on its systems to detect any unauthorized activities or viruses.

8.2 Supplier will maintain content filtering technologies to monitor connections to the internet.

8.3 Supplier will monitor CERT notifications that may affect Supplier's systems, and Supplier will patch its systems in accordance with a documented procedure that prioritizes the remediation of vulnerabilities based on risk.

8.4 Supplier will ensure that its systems stay current with patch management.

8.5 Supplier will have effective and up-to-date endpoint protection in place, including capabilities for dynamic exploit protection, dynamic malware protection, mitigation, remediation, and forensics, on all Supplier systems that are used to Process or store UKG Personal Data.

9. **Incident Event Management**

9.1 Supplier will maintain security incident response plans to manage response to security events. Supplier will test its security incident response plan on at least an annual basis.

9.2 Supplier will report Personal Data Breaches of UKG Personal Data to UKG pursuant to the terms of the DPA.

9.3 Supplier will assess security events and suspected incidents against defined criteria and responds to incidents in such a way that takes into consideration their potential impact to the UKG.

9.4 Supplier will consult with UKG prior to conducting a forensic investigation following a Personal Data Breach affecting UKG Personal Data or the environment under which it is stored (to the extent the same is under Supplier's direct control) and conduct investigations in accordance with legal requirements for preserving evidence. Supplier will keep UKG apprised of the forensic investigations and remediation.

9.5 Supplier will contain and mitigate incidents in accordance with documented incident management procedures and response plans.

9.6 Supplier will mitigate newly identified vulnerabilities. Any vulnerabilities that cannot be fixed, that could have a material impact on the security of UKG Personal Data will be reported to UKG.

9.7 Supplier will conduct post incident reviews to identify root-causes and identify actions required to minimize the risk of similar incidents re-occurring. Response strategies and plans will be updated in response to any lessons learned.

10. **Supplier Risk Management**

Supplier will maintain a third-party risk management program to ensure that all of Supplier's service providers (and such service provider's own subcontractors) comply with this Schedule 2 and Supplier's requirements ("**Service Provider Program**"). Upon UKG's request, Supplier will provide UKG a copy of its Service Provider Program. Supplier will require each of its service providers who have access to UKG Personal Data or host UKG Personal Data to comply with this Schedule 2. Supplier will regularly audit and monitor its service providers to ensure their compliance with this Schedule 2 and Supplier's requirements.

11. **Compliance**

11.1 Supplier will conduct an annual compliance assessment of its information security program. Supplier will provide the results of the assessment to UKG on request.

11.2 Supplier will support the UKG and/or UKG's independent auditors in assessing compliance with the information security policy by completing a questionnaire one time per year.

11.3 On an annual basis, Supplier will provide to UKG all available SOC 2 (Type II) or other audit reports or certifications (e.g., ISO 27001) applicable to Supplier's Services. In the event the Supplier receives a qualified SOC report UKG will have the right to terminate the Agreement.

11.4 Upon UKG's request, Supplier will permit UKG to perform a penetration test on Supplier's systems storing UKG Personal Data.

11.5 Unless otherwise agreed by UKG, all UKG Personal Data will be stored in the United States of America. Unless otherwise agreed by UKG, all personnel supporting the Services will be located in the United States of America.

11.6 If Processing credit card information, Supplier will maintain compliance with the Payment Card Industry Data Security Standard.

12. **Business Resiliency**

12.1 Supplier will maintain adequate business continuity and disaster recovery plans to ensure the uninterrupted performance of the Services ("**BC & DR Plans**"). Supplier's BC & DR Plans will be tested annually. Upon UKG's request, Supplier will provide a copy of the BC & DR Plan. The BC & DR Plan will ensure a recovery time objective and a recovery point objective of 4 hours.

Schedule 3: Supplier's Subprocessors

Please complete the below by inserting name, address and services provided by third party Subprocessors. If this Schedule remains unfilled, Supplier is deemed not to be using any Subprocessor.

Subprocessor Name	Subprocessor Legal Name	Registered address	Role in delivery of the services	Applicable Safeguards	Country of Processing

Schedule 4: Additional Applicable Privacy Provisions

The following provisions will apply if and to the extent applicable to the Processing of UKG Personal Data by Supplier.

1. **U.S. Privacy Laws**
   "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 "CCPA"); 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").

2. **Obligations.** Supplier is a "Service Provider" or "Processor", and receives from UKG Personal Data that constitutes "personal information" (as defined under U.S. Privacy Laws), Supplier in its role as a Service Provider or Processor shall not:

   i. "Sell" or "Share" (as defined under the CCPA as amended or modified) such Personal Information;

   ii. retain, use, or disclose such Personal Information for any purpose other than performing the Services or Business Purpose under the Agreement;

   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 such Personal Information outside of the direct business relationship between UKG and Service Provider unless otherwise permitted under the Agreement;

   v. combine the Personal Information that the Service Provider receives from, or on behalf of, UKG with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer.

3. Supplier, in its role as a Service Provider or Processor, certifies that it understands these requirements and agrees to comply with the US Privacy Laws as applicable to Service Provider in its provision of the Services to UKG under the Agreement, including handling of any consumer requests as set out in Clause 7 of this DPA. For clarity, Supplier shall notify UKG if it makes a determination that it can no longer meet its obligations under the CCPA, and UKG may take reasonable and appropriate steps to stop and remediate the unauthorized Processing of Personal Information.

4. In the event of any conflict between the terms of Sections 1 and 2 of Schedule 4 and any other terms of the DPA, the terms in this Sections 1 and 2 of Schedule 4 shall control but only to the extent they apply to handling of Personal Information.