Workday Peakon Employee Voice

Supplier Terms

G-Cloud 15

workday

Contents

Universal Main Subscription Agreement (MSA) 3

MSA- Frequently Asked Questions 13

Universal Data Processing Exhibit (DPE) 17

Addendum A: International Transfers of European Personal Data 21

Addendum B: Description of Processing 22

DPE - Frequently Asked Questions 24

Subprocessors 25
Adequacy Decisions 25
General Data Protection Regulation 26

Universal Security Exhibit 29

Production Support and Service Level Availability Policy (SLA) 32

Acceptable Use Policy 37

Workday Subscription Order Form Template 2

Additional Order Form Terms Addendum 4
Workday Service SKU Descriptions Addendum 6

Product Terms 7

Workday Training Order Form Template 9

Addendum A - Workday Training Terms 11

Addendum B - Bulk Training Credit Rates 15

Workday Consulting Customer Audit Program Order Form 16

Workday Application Penetration Testing Order Form Template 18

Workday Customer Application Penetration Testing Addendum 20

Universal Main Subscription Agreement (MSA)

This Agreement is between Workday Limited ("**Workday**") and the legal entity identified in the Order Form ("**Customer**"). This Agreement is incorporated by reference into the applicable G-Cloud 15 Call-Off Contract signed between Workday and Customer under the G-Cloud 15 Framework and forms part of Supplier Terms thereunder. For the purposes of these Supplier Terms, all references to Workday are hereby deemed to be references to Supplier, and all references to Customer are hereby deemed to be references to Buyer, as defined under the Call-Off Contract.

The parties agree as follows:

1. Provision of Service. Workday will make the Service available to Customer for use by Customer, its Affiliates and Authorised Parties for whom Customer enables access solely for the internal business purposes of Customer and its Affiliates, subject to this Agreement.

1.1 Invoices and Payment. All fees will be electronically invoiced to Customer in Customer's country of residence in accordance with the relevant Workday Order Form, and payment will be made by Customer from within its country of residence. All fees will be due and payable within 30 days of the invoice date, except fees subject to a reasonable and good faith dispute. Workday will email invoices to Customer within two business days of the date of the invoice. Customer must provide Workday with complete and accurate billing contact information including a valid email address. Upon Workday's request, Customer must make payments via electronic bank transfer. Customer may not withhold, reduce, or set off fees owed under this Agreement.

1.2 Overdue Payments. Any payment not received from Customer by the due date may accrue (except with respect to charges then under reasonable and good faith dispute), at Workday's discretion, late charges at the rate of 1% of the outstanding balance per month (or part thereof), or the maximum rate permitted by Law, whichever is lower, from the date such payment was due until the date paid.

1.3 Suspension for Non-Payment. Except for fees subject to a reasonable and good faith dispute, if a payment is more than 90 days past due and Workday has provided at least 30 days' prior written notice to Customer, Workday may suspend the Service, without liability to Customer, until such amounts are paid in full.

1.4 Taxes. Fees invoiced pursuant to this Agreement do not include, and may not be reduced to account for, any taxes, which may include local, state, provincial, federal or foreign taxes, withholding taxes, levies, duties or similar governmental assessments of any nature, including, but not limited to, value-added taxes, excise, use, goods and services taxes, consumption taxes or similar taxes (collectively "**Taxes**"). Customer must pay all Taxes imposed on the Service or any other services provided under this Agreement. If Workday has a legal obligation to pay or collect Taxes for which Customer is responsible under this Agreement, the appropriate amount will be computed based on Customer's address listed in the Signature Document or Workday Order Form for this Agreement which will be used as the ship-to address on the Workday Order Form, and invoiced to and paid by Customer, unless Customer provides Workday with a valid tax exemption certificate authorised by the appropriate taxing authority to accounts.receivable@Workday.com.

2. Customer Obligations. Customer will have sole responsibility for (a) the accuracy, quality, and legality of all Customer Content, (b) any Non-Workday Content it installs, uses, or enables; (c) obtaining and verifying it has all authorisations, consents, and rights necessary to use the Service; and (d) ensuring compliance with this Agreement and the AUP by its Affiliates and Authorised Parties, and any breach by its Affiliates or Authorised Parties will be deemed a breach by Customer. Customer will take reasonable endeavours to prevent unauthorised access to, or use of, the Service, and will notify Workday promptly of any unauthorised access or use. Customer will not: (1) use the Service in a manner that is inconsistent with the Documentation; (2) knowingly interfere with or disrupt performance of the Service or the data contained therein; or (3) attempt to gain access to the Service or its related systems or networks in a manner not set forth in the Documentation.

During the applicable Order Term, Workday reserves the right to suspend Customer's access to an applicable Service in the event Workday reasonably determines such action is necessary to preserve the integrity and/or security of such Service or if Workday in good faith reasonably determines that Customer has violated the AUP; however, Workday will use commercially reasonable efforts under the circumstances to provide Customer with an opportunity to remedy such violation or threat prior to such suspension. Workday will use commercially reasonable efforts to minimise the length and scope of suspension in light of the circumstances.

3. Proprietary Rights.

(a) Customer Ownership. As between Workday and Customer, Customer owns all right, title and interest to its Customer Content. Workday will have the right to use Customer Content to provide the Service, subject to this Agreement.

(b) Workday Ownership. As between Customer, Workday, and Workday's licensors, Workday or its licensors own all right, title and interest to the Service (including any third-party content Workday makes available through the Service) and Documentation, including all Intellectual Property Rights.

(c) Customer Input. Customer hereby grants Workday a royalty-free, worldwide, transferable, sub-licensable, irrevocable, perpetual licence to use or incorporate into its services any Customer Input. Workday will have no obligation to make Customer Input an Improvement. Customer will have no obligation to provide Customer Input.

3.1 Restrictions. Customer will not (a) modify, copy, or create derivative works based on the Service or Documentation; (b) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer in a service bureau, or otherwise make the Service or Documentation available to any third party other than to Authorised Parties as permitted herein; (c) reverse engineer or decompile any portion of the Service or Documentation, including but not limited to, any software utilised by Workday in the provision of the Service and Documentation, except to the extent required by Law; (d) access the Service or Documentation in order to build any commercially available product or service; or (e) copy any features, functions, integrations, interfaces or graphics of the Service or Documentation. Notwithstanding items (a) and (e), Customer may make a reasonable number of copies of the Documentation for internal business purposes only.

4. Confidentiality. Each party (the "**Recipient**") will use the same degree of care that it uses to protect its own confidential information of like kind (but in no event using less than a reasonable standard of care) not to disclose or use any Confidential Information of the other party (the "**Discloser**") except as reasonably necessary to perform the Recipient's obligations or to exercise the Recipient's rights under this Agreement or with the Discloser's prior written permission. For purposes of clarification, this Clause 4 also applies to Confidential Information either party or its Affiliates shares with the other party or its Affiliates related to potential future subscription services. Either party may disclose Confidential Information on a need-to-know basis to its (and its Affiliates'), directors, officers, employees, advisors, contractors and service providers, including third-party submission tools or online portal providers required by the Recipient for internal business purposes ("**Representatives**"), who are bound by confidentiality obligations at least as restrictive as those in this clause. The Recipient will be responsible for any acts or omission of its Representatives with respect to protection of the Discloser's Confidential Information.

The parties agree that (a) the Recipient's or its Representatives' online portal terms will not be binding on the Discloser submitting its Confidential Information to the Recipient through the Recipient's or its Representatives' online portal, (b) this Clause 4 applies to all such Confidential Information disclosed to the Recipient through such online portals; and (c) the Recipient's or its Representatives' online portal terms are superseded by this Agreement. To the extent required by Law, the Recipient's disclosure of the Discloser's Confidential Information will not be considered a breach of this Agreement if the Recipient promptly provides the Discloser with prior notice of such disclosure (to the extent legally permitted) and reasonable assistance, at the Discloser's cost, if the Discloser wishes to contest the disclosure. The Discloser may seek injunctive relief to enjoin any breach or threatened breach of this clause, it being acknowledged by the parties that other remedies may be inadequate.

5. Protection and Security of Customer Content and Privacy.

5.1 Security Program and Audit Reports. Workday maintains a security programme that conforms to the Workday Security Exhibit and Audit Reports (as set forth in the applicable Product Terms). Through Workday's Customer self-service systems or upon Customer's written request, Workday will make available to Customer Workday's then-current Audit Reports for the applicable Service application to enable Customer to verify Workday's compliance with its obligations under this Agreement. Audit Reports constitute Workday's Confidential Information and are subject to the confidentiality terms in this Agreement or separate confidentiality agreement terms (as applicable).

5.2 Privacy. Personal Data will only be processed in accordance with the Data Processing Exhibit.

5.3 Unauthorised Disclosure. If either party becomes aware of a Security Breach, that party must promptly notify the other party, unless legally prohibited from doing so, within 48 hours or any shorter period required by Law except that Customer is not required to notify Workday unless Customer reasonably determines there is a threat to the Service. Additionally, each party will reasonably assist the other party in mitigating any potential damage. As soon as reasonably practicable after any Security Breach, Workday will conduct a root cause analysis and, upon request, will share the results of its analysis and its remediation plan with Customer. Unless prohibited by Law, each party will provide the other party with reasonable notice of and the opportunity to review and comment on the content of all public notices, filings, or press releases about a Security Breach that identify the other party by name prior to any such publication.

6. Warranties. Each party warrants that it has the authority to enter into this Agreement and, in connection with its performance of this Agreement, will comply with all Laws. Workday warrants that during the applicable subscription Order Term: (a) the overall Service (1) will not be materially decreased; and (2) will perform materially in accordance with the feature descriptions in the Documentation; and (b) to the best of Workday's knowledge, the Service does not contain, and Workday will not knowingly introduce, any Malicious Code (collectively, the "**Service Warranty**"). Customer will use its reasonable endeavours to notify Workday in writing no later than 30 days after identifying a deficiency, but Customer's failure to notify Workday within that period will not affect Customer's right to receive warranty remedies unless Workday is impaired in its ability to correct the deficiency due to Customer's failure to notify. Notice of breaches of the warranty under item (2) above must be made through Workday's then-current error reporting system; notices of breaches of any other warranty must be made in writing to Workday in accordance with the notice provisions of this MSA. Customer's exclusive remedy and Workday's sole liability for breach of the Service Warranty are those described in Clause 9.1 for the affected Service.

6.1 Disclaimer. Except as expressly provided in this Agreement and to the maximum extent permitted by Law, Workday makes no warranties of any kind, whether express, implied, statutory or otherwise, and specifically disclaims all implied warranties, including any warranties of merchantability or fitness for a particular purpose. Workday does not warrant that the Service will be error-free or uninterrupted. The limited warranties provided in this Agreement are the sole and exclusive warranties provided to Customer. Customer agrees that it is not relying on delivery of future service features or product roadmaps in obtaining subscriptions to any Service.

7. Indemnification.

7.1 Workday Indemnity. Workday will defend Customer, at Workday's expense, against any third-party Claim brought against Customer alleging that the use of the Service as contemplated hereunder infringes that third party's Intellectual Property Rights and will indemnify and hold Customer harmless against any Losses arising from such third-party Claim. Workday will have no liability for Claims or Losses to the extent they arise from: (a) modification of the Service by anyone other than Workday; (b) use of the Service in a manner inconsistent with the Documentation or in violation of this Agreement; or (c) use of the Service in combination with any other product or service not provided by Workday. If Customer is prevented from using the Service or if Workday reasonably believes it will be prevented Workday may, at its sole option, obtain for Customer the right to continue use of the Service or replace or modify the Service so that it is no longer infringing. If neither of the foregoing options is reasonably available to Workday, then either party

may terminate the applicable Service and Workday's sole liability, in addition to the indemnification obligations in this clause, will be to refund any prepaid Subscription Fees for the Service that was to be provided after the effective date of termination.

7.2 Customer Indemnity. Customer will defend Workday, at Customer's expense, from any third-party Claim against Workday arising from: (a) Customer Content; (b) violations by Customer, its Affiliates or Authorised Parties of the AUP, and Customer will indemnify and hold Workday harmless against any Losses relating to such third-party Claim.

7.3 Conditions. The indemnitor's obligations in Clauses 7.1 and 7.2 are conditioned on the indemnitee: (a) promptly giving written notice of the third-party Claim to the indemnitor (although a delay of notice will not relieve the indemnitor of its obligations under this clause except to the extent that the indemnitor is prejudiced by such delay); (b) giving the indemnitor sole control of the defence and settlement of the third-party Claim (although indemnitor may not settle any third-party Claim unless it unconditionally releases indemnitee of all liability); and (c) providing to the indemnitor, at the indemnitor's cost, all reasonable assistance. Clauses 7.1 through 7.3 state each indemnitee's exclusive remedies and the indemnitor's sole obligations related to the subject matter of these clauses.

8. Limitation of Liability.

8.1. Limitation of Liability. Except with respect to (a) willful misconduct, fraud, or death or personal injury caused by negligence; (b) either party's indemnification obligations under this Agreement; (c) Customer's payment obligations; and (d) Workday's remediation obligations in Clause 8.3, the following limitation of liability caps will apply: In no event will either party or its Affiliates' total aggregate liability arising out of or related to this Agreement, whether in contract, tort (including negligence) or otherwise, exceed the fees paid or payable under this Agreement during the immediately preceding 12-month period for the Service from which the Claim arose ("**General Cap**"), except that for breach of either party's confidentiality, security, or privacy obligations, the breaching party's total aggregate liability will be increased to fees paid or payable under this Agreement during the immediately preceding 24-month period for the Service from which the Claim arose ("**Enhanced Cap**").

8.2 Exclusion of Damages. Except with respect to either party's indemnification obligations under this Agreement and the direct damages identified in Clause 8.4, in no event will either party or its Affiliates have any liability to the other party for: (a) any indirect, special, incidental, punitive or consequential losses or damages, however caused; or (b) whether the same are suffered directly or indirectly, any loss of: profits, anticipated savings, business opportunity or goodwill. Customer will not assert that its payment obligations as set forth in a Workday Order Form are excluded as Workday's lost profits.

8.3 Workday Remediation Obligations. If unauthorised disclosure of or access to Personal Data is caused by Workday's breach of its security, privacy, or data protection obligations under this Agreement, Workday will pay the reasonable and documented costs incurred by Customer in connection with the following items: (a) costs of any required forensic investigation to determine the cause of the breach; (b) providing notification of the Security Breach to applicable government and relevant industry self-regulatory agencies, to the media (if required by Law) and to individuals whose Personal Data have been disclosed or accessed ("**Affected Individuals**"); (c) providing a credit monitoring service to Affected Individuals who elect to receive it for a period of one year after the date on which such individuals were notified of the unauthorised disclosure or access; and (d) operating a call centre to respond to questions from Affected Individuals for a period of one year after the date on which such individuals were notified of the unauthorised disclosure or access. Notwithstanding the foregoing, or anything in this Agreement to the contrary, Workday will have no responsibility to pay costs of remediation to the extent they are due to gross negligence, willful misconduct or fraud by Customer, its Affiliates or their respective directors, officers, employees, agents, contractors or Authorised Parties.

8.4. Direct Damages. Subject to Clause 8.1, and notwithstanding Clause 8.2, if either party breaches its obligations under this Agreement, the following will be considered direct damages: (a) amounts paid to affected third parties as damages or settlements in response to Claims that flow directly from the breach;

(b) amounts paid for fines and penalties imposed by any governmental authority arising from the breach; and (c) reasonable legal fees to defend against third-party Claims arising from the breach.

9. Term. The term of this Agreement commences on and continues from the Effective Date (as defined in the Signature Document) or the Order Effective Date (as identified in the Workday Order Form) until all Workday Order Forms have expired or otherwise been terminated, unless extended pursuant to the written agreement of the parties ("**Term**"). Subscriptions to the Service commence on the Order Term start date as set forth in the applicable Workday Order Form.

9.1 Termination. Either party may terminate this Agreement: (a) upon 30 days' prior written notice to the other party for a material breach by the other party if such breach remains uncured at the expiration of such notice period; or (b) to the extent permitted by Law, immediately in the event the other party becomes the subject of a petition in bankruptcy or any other proceeding or process relating to insolvency, receivership, liquidation, administration or assignment for the benefit of creditors. For clarity, (1) Customer will have the right to terminate the affected Service for a breach of Service Warranty pursuant to Clause 9.1(a) above; and (2) a breach or termination of any PSA or SOW will not be considered a material breach or a cause of termination of this Agreement.

If this Agreement is terminated, all Workday Order Forms are simultaneously terminated and Customer will, as of the date of any termination, immediately cease accessing and otherwise utilising the Service (except as permitted under Clauses 9.2 and 9.3) and Workday Confidential Information. Upon termination by Customer pursuant to this clause, Workday will refund Customer any prepaid Subscription Fees for the affected Service that was to be provided after the effective date of termination. Termination for any reason will not relieve Customer of the obligation to pay any Subscription Fees accrued or due and payable to Workday prior to the effective date of termination and termination for any reason other than for uncured material breach by Workday or as otherwise stated in this Agreement will not relieve Customer of the obligation to pay all future amounts due under all Workday Order Forms.

9.2 Retrieval of Customer Content. Upon Customer's written request made on or prior to expiration or termination of this Agreement (including any Transition Period), Workday will give Customer limited access to the Service for a period of up to 60 days, at no additional cost, solely for purposes of retrieving Customer Content ("**Retrieval Period**"). After such Retrieval Period (or if there is no Retrieval Period, after termination or expiration of this Agreement or applicable Workday Order Form) and subject to Workday's legal obligations, Workday has no obligation to maintain or provide any Customer Content and will, unless legally prohibited, delete Customer Content by deleting the applicable Instance; provided, however, that Workday will not be required to remove copies of Customer Content from its backup media and servers until such time as the backup copies are scheduled to be deleted, provided further that in all cases Workday will continue to protect Customer Content in accordance with this Agreement. Customer Content will be made available for retrieval through extraction in a machine-readable format as described in the Documentation.

9.3 Transition Period Before Final Termination. If this Agreement is terminated and Customer submits a written request to Workday prior to any such termination for a one-time transition period, Workday will continue to provide the Service for up to three months after the effective date of such termination (the "**Transition Period**"). Monthly fees for the Transition Period will be 1/12 of the fee for the immediately preceding 12-month period plus an additional five percent. If Customer requests transition assistance during the Transition Period, Workday will provide consulting cooperation and assistance regarding the Service as set forth in a statement of work, governed by a professional services agreement, at Workday's then-current rates for consulting services unless a different rate is mutually agreed upon by the parties. Notwithstanding the foregoing, if Workday is prevented from performing, or termination of this Agreement was due to Customer's breach, Workday has no obligation to perform under this clause unless it receives (a) payment of all fees not subject to reasonable and good faith dispute, (b) prepayment of fees for further services, and (c) certification of ongoing compliance with the terms of this Agreement during the Transition Period.

9.4 Surviving Provisions. Clauses 1.1, 1.2, 3, 4, 5 (for so long as Workday retains Customer Content), 6.1, 7, 8, 9.1 (as far as it relates to payment obligations), 9.2, 9.3, 9.4, 10, and 11 will survive any termination or expiration of this Agreement.

10. General Provisions.

10.1 Relationship of the Parties. The parties are independent contractors. This Agreement does not create nor is it intended to create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. There are no third-party beneficiaries to this Agreement.

10.2 Notices. Unless expressly stated otherwise, all notices under this Agreement must be in writing and will be deemed to have been given upon: (1) personal delivery; and (2) the third business day after pre-paid recorded mail with proof of delivery. Notices to Workday must be sent to the address shown in or linked from the Signature Document or Workday Order Form, addressed to the attention of its Legal Department with a copy sent by email to legal@Workday.com. Notices to Customer must be sent to the address shown in the Signature Document or Workday Order Form, addressed to Customer's signatory of this Agreement. Each party may modify its recipient of notices by providing notice pursuant to this Agreement.

10.3 Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right or any other right. Other than as expressly stated, the remedies provided in this Agreement are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

10.4 Force Majeure. Neither party will be liable for any failure or delay in performance under this Agreement caused by unforeseeable events beyond that party's control and where the failure or delay is through no fault of the affected party and could not have been reasonably avoided ("**Force Majeure**"). Dates by which performance obligations are scheduled to be met will be extended for a period equal to the time lost due to any delay so caused, provided that notice of the Force Majeure event is given in writing within 15 days after the Force Majeure event begins. Such notice must identify the nature of the Force Majeure event, its expected duration and the probable impact on the performance of the affected party's obligations.

10.5 Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (which consent must not be unreasonably withheld or delayed). Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Workday Order Forms) upon written notice without consent of the other party in connection with a merger, acquisition, corporate reorganisation, or sale of all or substantially all of its assets so long as the assignee: (a) is an entity registered in a territory in which Workday is approved to provide the Service; and (b) agrees to be bound in writing by all of the terms of this Agreement and all past due Subscription Fees are paid in full. Any attempt by a party to assign its rights or obligations under this Agreement other than as permitted by this clause will be void. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

10.6 Governing Law and Jurisdiction and Local Law Requirements. This Agreement, and any dispute or Claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or Claims), will be governed by and construed in accordance with the laws of England and Wales and the parties irrevocably submit to the exclusive jurisdiction of the courts in England.

10.7 Export. Each party will comply with the applicable export laws and regulations of the United States and other applicable jurisdictions in providing and using the Service. Without limiting the generality of the foregoing, Customer will not make the Service available to any person or entity that: (1) is located in a country that is subject to a European Union, United Nations or U.S. government embargo; (2) is listed on any European Union, United Nations or U.S. government list of prohibited or restricted parties; or (3) is engaged in activities directly or indirectly related to proliferation of weapons of mass destruction.

10.8 Anti-Corruption. Each party will comply with all applicable anti-corruption Laws, in relation to this Agreement. Each party agrees that it will not offer to pay or give anything of value to anyone, including foreign governmental officials or related persons or entities on either party's behalf to corruptly: (i) influence

any official act or decision; (ii) secure any improper advantage; (iii) obtain or retain business, or direct business to any person or entity; or (iv) for the purpose of inducing or rewarding any favourable action in any matter related to the subject of this Agreement or the business of either party. Each party further agrees to keep accurate books and records in relation to this Agreement. Each party further agrees to cooperate with the other party in any anti-corruption due diligence process and/or investigation in relation to this Agreement.

10.9 Code of Conduct. Workday uses commercially reasonable efforts to ensure that Workday, all of Workday's employees and any Workday subcontractors who perform any part of the Service under this Agreement on behalf of Workday, comply with Workday's written code of conduct available at https://codeofconduct.Workday.com/index.php, as may be modified by Workday from time to time.

10.10 Background Checks. Unless prohibited by law, Workday agrees to conduct (or have previously conducted) a criminal background check on personnel employed by Workday (or will require its subcontractors to conduct a background check on their own personnel) who will have access to Customer Data. Such background check shall be in the form generally used by Workday in its initial hiring of employees or contracting for contractors or, as applicable, during the employment-screening process. Workday will not allow any person performing under this Agreement on behalf of Workday to be assigned to have access to Customer Data whose background check revealed a conviction of any violent crime or crime involving theft, dishonesty, moral turpitude, breach of trust, or money laundering.

10.11 Workday SLA Service Credits. If, in any rolling six-month period, Workday fails to meet the monthly commitments for Service Availability or Service Response (as applicable) described in the applicable Product Terms SLA (a "**Failure**"), Customer must request the following remedies no later than 60 days after the applicable Failure occurs: (a) a meeting to discuss possible corrective actions for the first Failure; (b) a 10% Service Credit for a second Failure; (c) a 20% Service Credit for a third Failure; and (d) a 30% Service Credit for a fourth Failure. In this Agreement, **"Service Credit"** means a credit equal to the stated percentage of the applicable monthly Subscription Fee for the affected Service. When Workday has confirmed the Failure, Workday will deduct the highest applicable Service Credit from the next invoice for Subscription Fees or, if there is no subsequent invoice, will refund the Service Credit to Customer. The remedies in this clause are Customer's exclusive remedies for any Failure.

10.12 Business Continuity. Workday shall maintain and operate in accordance with business continuity and disaster recovery plans as specified in Workday's Security Exhibit. Such plans shall be tested and reviewed by Workday on at least a semi-annual basis for effectiveness. Upon Customer's request, Workday shall provide Customer a summary description of its business continuity/disaster recovery plans and a copy of executive summaries on the semi-annual tests of its business continuity/disaster recovery plans. Workday's business continuity and disaster recovery plans will not be materially or substantially decreased or diminished by Workday during the Term.

10.13 Miscellaneous. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. In the event of a conflict, the provisions of an Workday Order Form will take precedence over provisions of this MSA and over any other exhibit or attachment. Customer acknowledges that it has had the opportunity to review all exhibits and attachments hereto. This Agreement supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter and is entered into without reliance on any promise or representation other than those expressly contained in this Agreement. Except as otherwise stated in this Agreement, no modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by Law, and the remaining provisions of this Agreement will remain in effect. Notwithstanding anything to the contrary in this Agreement, no terms or conditions in a Customer purchase order or in any other Customer order documentation will be incorporated into or form any part of this Agreement, and all such terms or conditions will be null and void.

Purchase orders are for administrative convenience only and Workday may issue an invoice and collect payment without a corresponding purchase order. Customer's failure or delay to issue a purchase order

will not extend the payment due date. If a purchase order is required, it must be sent by email to accounts.receivable@Workday.com 10 business days prior to the date the invoice is issued in order to be included on the related invoice. This Agreement may be executed in counterparts and/or by electronic signatures.

11. Definitions.

The following definitions will apply to this Agreement.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with either party. For purposes of the preceding sentence, "control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" means this Main Subscription Agreement, including the SLA, Security Exhibit, Data Processing Exhibit, and any other exhibits, addenda, or attachments hereto, and any fully executed Workday Order Form.

"**Audit Reports**" means the (a) most recently issued security audit reports and (b) other security relevant assessment reports and certifications for the applicable Service (as identified in the Product Terms) that are prepared by Workday's independent third party audit or obtained by Workday from other independent third parties, which may be updated by Workday from time to time, provided that no update will materially decrease the protections provided by the controls set forth in the applicable Audit Report during the Term.

"**AUP**" means the acceptable use policy for the applicable Service located at https://www.Workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html.

"**Authorised Parties**" means Customer's or its Affiliates' directors, officers, employees, users, contractors, and third-party providers who are authorised to access Customer's Instance or receive Customer Content by Customer (a) in writing, (b) through the Service's security designation, or (c) by system integration or other data exchange process.

"**Claim**" means a claim, demand, lawsuit or other legal proceeding brought against a party to this Agreement.

"**Confidential Information**" means (a) any software utilised by Workday in the provision of the Service and its respective source code; (b) Customer Content; (c) each party's business or technical information, including but not limited to the Documentation, training materials, any information relating to software plans, designs, costs, prices and names, finances, marketing plans, business opportunities, personnel, research, development or know-how and other significant and valuable business information that would otherwise be considered to be trade secrets under Law, that is designated by the Discloser as "confidential" or "proprietary" or the Recipient knows or should reasonably know is confidential or proprietary; and (d) the negotiated terms, conditions and pricing of this Agreement (but not its existence or parties). Confidential Information does not include any information that, without the Recipient's breach of an obligation owed to the Discloser: (1) is or becomes generally known to the public; (2) was known to the Recipient prior to disclosure by the Discloser; (3) was independently developed by the Recipient; or (4) is received by the Recipient from a third party. Customer Content will not be subject to the exclusions set forth in this definition.

"**Customer Content**" means electronic data or information submitted to the Service by Customer, its Affiliates or Authorised Parties.

"**Customer Input**" means suggestions, enhancement requests, recommendations or other feedback provided by Customer, its Affiliates and/or Authorised Parties relating to the operation or functionality of the Service.

"**Data Processing Exhibit**" or "**DPE**" means the Universal Data Processing Exhibit located at https://www.Workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html, which may be updated by Workday from time to time to comply with applicable Data Protection Laws applicable to Workday as a data Processor, provided that no update will materially decrease Workday's Data Processor obligations under the DPE.

"**Documentation**" means the then-current version of the Workday electronic Administrator Guide for the applicable Service application, which may be updated by Workday from time to time.

"**Enhanced Features**" will have the same meaning as set forth in the applicable Product Terms.

"**Improvements**" means all improvements (including verification of such improvements), updates, enhancements (including Enhanced Features), error corrections, bug fixes, prevention of or addressing service or technical problems, release notes, upgrades and changes to the Service and Documentation, as developed by Workday and made available to Customers generally without a separate charge.

"**Instance**" means a unique instance of the Service, with a separate set of Customer Content held by Workday in a logically separated database (i.e., a database segregated through password-controlled access).

"**Intellectual Property Rights**" means any and all common law, statutory and other industrial property rights and intellectual property rights, including copyrights, trademarks, trade secrets, patents and other proprietary rights issued, honored or enforceable under any applicable laws anywhere in the world, and all moral rights related thereto.

"**Law**" means any local, state, national and/or foreign law, treaties, and/or regulations applicable to the respective party.

"**Loss**" means reasonable attorneys' fees and any damages or costs finally awarded or entered into in settlement of a Claim.

"**Malicious Code**" means viruses, worms, time bombs, Trojan horses and other malicious code, files, scripts, agents or programs.

"**Non-Workday Content**" means a third-party product, web-based, offline, mobile, or other software application functionality or other content that is provided by Customer or a third party and interoperates with a Workday Service application.

"**Order Form**" means the fully executed ordering document (including Product Terms) under which Customer subscribes to Service application(s) or other services. Workday Order Forms do not include the terms of any preprinted terms on a Customer purchase order or other terms on a purchase order that are additional to or inconsistent with the terms of this Agreement.

"**Personal Data**" has the definition set forth in the DPE.

"**Product Terms**" means the product terms for a specific Service application as identified via URL in or attached to the subscription Workday Order Form, which may be updated by Workday from time to time; provided that no update will materially decrease the applicable security and privacy commitments and any such changes will not become effective until 30 days after publication of the updated Product Terms.

"**Production**" means Customer's use of or Workday's written verification of the availability of the Service (a) to administer its users (as identified in the applicable subscription Workday Order Form); (b) to generate data for Customer's books/records; or (c) in any decision support capacity. Production does not include any non-production sandbox, preview, or implementation Instance.

"**PSA**" means the optional, separate, and independent professional services agreement between Customer and Workday related to Workday's provision of implementation and other consulting services to Customer, subject to a statement of work ("**SOW**").

"**Security Breach**" means (a) any actual or reasonably suspected unauthorised use of, loss of, access to or disclosure of, Customer Content; provided that an incidental disclosure of Customer Content to an Authorised Party or Workday, or incidental access to Customer Content by an Authorised Party or Workday, where no reasonable suspicion exists that such disclosure or access involves theft, or is fraudulent, criminal or malicious in nature, will not be considered a "Security Breach" for purposes of this definition, unless such incidental disclosure or incidental access triggers a notification obligation under any

Law; (b) any Personal Data Breach as defined in the DPE; and (c) any security breach (or substantially similar term) as defined by Law affecting Customer Content.

"**Security Exhibit**" means the Universal Security Exhibit located at https://www.Workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html, which may be updated by Workday from time to time, provided that no update will materially decrease the protections provided by the controls set forth in the Security Exhibit during the Term.

"**Service**" means the applicable Workday software-as-a-service application (as described in the Documentation and Product Terms) as subscribed to under an Workday Order Form and Improvements, including non-Production versions. For purposes of clarification, Service excludes professional services, support services, training services, and Non-Workday Content.

"**Signature Document**" means the document signed by the parties which lists all the terms and conditions forming part of this Agreement to which the parties agree to be bound.

"**SLA**" means the Production support and service level availability policy for the Service application(s) identified in the applicable Product Terms, which may be updated by Workday from time to time, provided that no update will materially decrease Workday's responsibilities under the SLA during the applicable Order Term.

"**Subscription Fees**" means all amounts invoiced to and payable by Customer for the applicable Service under an Workday Order Form.

MSA- Frequently Asked Questions

Thank you for reviewing Workday's contract documents. As you review the attached documents, we hope this FAQ will help you better understand what is being purchased and how Workday's enterprise cloud service model works.

This FAQ does not form part of the contract and is provided for informational purposes only and will not be a part of the final agreement package.

1. What is my company purchasing?

Workday provides fully functional enterprise cloud applications through the Internet using a genuine one-to-many cloud delivery model. Our customers upload their Customer Content to Workday's Software as a Service (SaaS) solution and configure the Service application to leverage the features required for the customer's internal business purposes. All customers are on the same release version of the Workday Service applications. Workday provides its Service on a single code line so that all customers on a specific application are on the same release using the same operational infrastructure and the same security and support operations.

2. How is Workday's cloud Service different from installed, on premise software?

Workday's cloud-based, mobile, and in-memory object-oriented applications operate on a true one-to-many business model. Application service providers offer a customisable model, where each customer is treated differently - essentially they offer outsourced hosting of installed software. Workday's one-to-many business model is different and allows for a more cost-effective delivery of solutions by ensuring that all customers are always on the same release version. Customers avoid costly and disruptive upgrades. As Workday rolls out new feature releases, customers can adopt new features on their own time, which makes Workday's cloud applications highly configurable by each customer.

3. How does Workday protect the Customer Content in the Service?

Protecting the security and privacy of our Customers' Content is one of Workday's top priorities. Workday maintains a comprehensive security program that takes into account the state of the art, the nature and purposes of the Service, the type of Customer Content in the Service, the legal environment in which Workday operates, and our customers' need for security and confidentiality. Workday monitors, evaluates, and adjusts this security program in light of changing technology and the changing legal and business environments in which it operates.

Data Security:

- Controls: We employ rigorous security measures at the organisational, architectural, and operational levels and we are committed to investing in world class technology compliance programs. Workday's cybersecurity compliance program was deployed to enhance privacy and security, build trust and provide assurance to our customers that their Customer Content and Workday's applications and infrastructure are secure. The cornerstone of our cybersecurity compliance program is our independent third-party audits, industry standard ISO certifications, and detailed self-assessment evaluations that Workday completes annually and makes available free-of-charge to customers via self-service framework. The list of applicable privacy and compliance documentation that Workday makes available to our customers includes, but isn't limited to:

- SOC 1 and SOC 2 audit reports;
- ISO 27001, ISO 27017, ISO 27018 and ISO 27701 certificates;
- Shared Assessments SIG questionnaire;
- CSA CAIQ questionnaire;

- Web & Mobile Applications Independent Security Report
- Networks and Systems Independent Security Report
- Disaster Recovery (DR) Plan and Executive Summary
- Workday Continuity Strategy & Plan
- Tier II CyberGRX Assessment Report
- Transfer Impact Assessments Whitepaper
- Code of Conduct

In combination, all of these materials:

- Provide an in-depth view into Workday's data privacy, data security, and operational processes and control environments related to Workday's provision of the Service; and
- Enable our customers to conduct (via self-service) risk assessments of Workday's provision of the Service.

The validation of the operational effectiveness of our control environment is facilitated through the independent third-party auditor testing procedures performed and summarised in the Audit Reports, which are made available to our customers at any point during the subscription Order Form term. Thus, customers have independent verification of and visibility into the security controls protecting their data. Further, Workday contractually commits that it will not materially decrease the protections provided by the controls set forth in Workday's Security Exhibit and Audit Reports during the Agreement Term.

Data Privacy:

- **Universal Data Processing Exhibit:** The MSA includes a link to an exhibit that details the terms and conditions applicable to Workday's processing of Personal Data. This DPE provides our customers with contractual protections relating to Workday's compliance with data protection laws applicable to Workday as a data processor.
- **Additional Disclosure Restrictions:** In Section 3 of the MSA, Workday contractually commits to use Customer Content to provide the Service, subject to the terms of the Agreement.

4. Why can't my organisation's security and privacy exhibits be joined to the contract?

Workday maintains a formal and comprehensive security program designed to ensure the security and integrity of each customer's data, to protect against security threats and data breaches, and to prevent unauthorised access to the data of its customers. The specifics of Workday's security program are detailed in our Universal Security Exhibit, our third-party security audits, and international certifications. As a true cloud provider, Workday operates a multi-tenanted platform where all customers share a platform and single version of the Service with logical segregation between customers. All our security controls are designed from the ground up for a cloud environment with security controls applied to each applicable application, including all environments where data from our customers is present. Workday commits to not materially decrease the protection of the controls provided by our Audit Reports (e.g., applicable SOC1, SOC2) and the Universal Security Exhibit. In addition, our privacy controls are described in our Universal Data Processing Exhibit, so customers have contractual commitments that Workday complies with data protections laws applicable to Workday in our role as a data processor. These controls form part of our one-to-many business model and enable Workday to meet its security and data privacy commitments while also enabling Workday to continually enhance, evolve, and develop our security and privacy programs to the benefit of all customers equally. This means, however, that we cannot contractually commit to individual customers' security and privacy standards, terms, or policies without breaking our one-to-many business model. In order to provide transparency, visibility and continuous assurance to our customers as

to the effectiveness of our security and privacy controls Workday conducts independent third-party audits and makes the result of these audit reports available to our customers upon request.

5. How do we get our data back when the relationship ends?

Customers always own their Customer Content throughout the course of the relationship (see Section 3, "Proprietary Rights"). Customers can download copies of their Customer Content stored in the Service at any time during the Term. Workday has a standard process for a final data download during the customer's subscription term and upon termination of relationship, which can be found in the MSA (see Section 9.2, "Retrieval of Customer Content").

6. Does Workday offer an SLA?

Yes, Workday has a service level availability policy for applicable Service applications, so customers always know Workday's commitments regarding service levels. The success of Workday's cloud delivery business model is predicated upon the efficiency of our one-to-many infrastructure. Since Workday delivers its Service applications from the same operational business model for our entire customer base, the applicable SLA cannot be modified on a customer by customer basis. Workday provides Service Credits in the event of certain SLA Failures; these can be found in the SLA Service Credit section of the Agreement.

7. What is Workday's pricing methodology?

Workday's business model is structured on a subscription price model based on number of employees, users, other size metrics, and, for some Service applications, usage. During the subscription Order Term, the subscription fee may not be reduced. Thus, Workday cannot accommodate a customer's request to decrease its payment obligations to Workday based upon a reduction in customer's employee/user count or applicable usage metric regardless of the reason for such reduction (customer downsizing, customer acquired by another entity, customer divestiture of an affiliate, etc.).

8. Does Workday offer an acceptance test period?

Workday's cloud-based business delivery model is fundamentally different from other business delivery models. Since Workday runs the Service for all customers on a single code line, the viability of the Service has already been demonstrated by the existing customers who run their businesses on the same single code line. Thus, the concept of an acceptance test is made obsolete and does not exist in Workday's business model.

9. Will Workday permit customers to audit Workday?

Most Workday customers rely upon the independent third-party audits, industry standard ISO certifications, and detailed self-assessment evaluations that Workday completes annually and makes available free-of-charge to customers via self-service framework. As such, we strongly encourage our customers to rely upon and use Workday's existing privacy, compliance, and security materials instead of performing any unique assessment reviews and electing to participate in the fee-based Workday's customer audit program. Workday's customer audit program is Workday's fee-based audit-as-a-service offering that enables customers to conduct compliance reviews of our data security, data privacy, and other operational processes and supports their relevant audit requirements related to Workday's provision of the Service to the customer.

11. Does Workday offer unlimited liability?

Workday understands that our customers are concerned about the protection of their Customer Content and the remedies available in the event of a breach. Workday has developed a structure unique in the industry because it covers the primary costs associated with a breach of personally identifiable information, providing an exceptionally high level of protection for our customers.

- **Specified Remediation Costs outside Limitation of Liability:** In Section 8.3 of the MSA, Workday agrees to pay certain remediation costs and such costs are not subject to any limitation of liability. Specifically, in the event that any unauthorised disclosure of or access to Personal Data is caused by Workday's breach of its security or privacy obligations, Workday will pay the reasonable and documented costs incurred by Customer in connection with the following items: (1) costs of any required forensic investigation to determine the cause of the breach, (2) providing notification of the security breach to applicable government and relevant industry self-regulatory agencies, to the media (if required by applicable law) and to individuals whose Personal Data may have been accessed or acquired, (3) providing credit monitoring service to individuals whose Personal Data may have been accessed or acquired (for a specified period), and (4) operating a call center to respond to questions from individuals whose Personal Data may have been accessed or acquired (for a specified period). These four items represent the full extent of remediation costs Workday will cover outside the limitation of liability.

- **Other Damages / Breaches are subject to Limitation of Liability:** Workday also agrees to uncapped liability for our intellectual property indemnity as set forth in Section 7 of the MSA and for breaches arising out of our gross negligence, willful misconduct or fraud as set forth in Clause 8.1 of the MSA. A fundamental principle of Workday's business model is that any other damages and any other breaches of the Agreement are subject to a limitation of liability (see Section 8.1 of the MSA)

Universal Data Processing Exhibit (DPE)

This Universal Data Processing Exhibit is an exhibit to the Agreement between Workday and Customer and sets forth the obligations and rights of the parties regarding the Processing of Personal Data pursuant to such Agreement. This Universal Data Processing Exhibit is incorporated by reference into the relevant Call-Off Contract between Workday and Customer entered into under the G-Cloud 15 Framework and forms part of the Supplier Terms thereunder.

1. Definitions.

Unless otherwise defined below, all capitalised terms have the meaning given within the applicable Agreement and/or exhibits thereto.

"**Agreement**" means the MSA, the Professional Services Agreement, and Order Forms, including any exhibits or attachments applicable to the Covered Service.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data and any substantively analogous term or role defined under applicable Data Protection Laws.

"**Covered Data**" means (i) Customer Content and/or Customer Data (as defined in the MSA), and (ii) Professional Services Data.

"**Covered Service**" means (i) any Service provided under the MSA, and/or, (ii) any Professional Services.

"**DPE**" means this Universal Data Processing Exhibit including any appendices, or documents incorporated by reference.

"**Data Protection Laws**" means all data protection or privacy laws and regulations applicable to the Processing of Personal Data.

"**Data Subject**" means the person to whom the Personal Data relates.

"**Europe**" **or** "**European**" means the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") and Switzerland.

"**GDPR**" means either or both the (i) General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**") and (ii) EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") as the context may require.

"**Personal Data**" means any Covered Data that relates to an identified or identifiable natural person, or (ii) is defined as "personal data" or "personal information" (or any substantively analogous term) by applicable Data Protection Laws.

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

"**Processing**" or "**Process**" means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller and any substantively analogous term or role defined under applicable Data Protection Laws.

"**Professional Services**" means the professional or consulting services provided to Customer under a Professional Services Agreement.

"**Professional Services Agreement**" means any agreement between the parties for the provision of consulting or professional services, including but not limited to the following agreements or terms: the

Professional Services Agreement, the Delivery Assurance terms, the Professional Services Addendum, and/or the Consulting and Training Addendum and Amendment.

"**Professional Services Data**" means electronic data or information that is provided to Workday under a Professional Services Agreement for the purpose of being input into a Service, or any other Covered Data accessed within or extracted from a Service to perform the Professional Services.

"**Restricted Transfer**" means (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a recipient in a country outside of the EEA which is not subject to a valid adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a recipient in a country outside the UK which is not based on adequacy regulations pursuant to Chapter V of the UK GDPR; and (iii) where the Swiss Federal Act on Data Protection of September 25, 2020 ("**Swiss FADP**") applies, a transfer of Personal Data from Switzerland to recipient in a country outside Switzerland which has not been recognised to provide an adequate level of protection by the Federal Council.

"**Subprocessor**" means a Workday Affiliate or third-party entity engaged by Workday or a Workday Affiliate as a Processor under this DPE.

"**Subprocessor List**" means the subprocessor list identifying the Subprocessors that are authorised to Process Personal Data, accessible through Workday's website (currently located at https://www.workday.com/en-us/legal/subprocessors.html).

2. Processing Personal Data.

2.1 Scope and Role of the Parties. This DPE applies to the Processing of Personal Data by Workday to provide the Covered Service. For the purposes of this DPE, Customer is a Controller or a Processor and Workday is a Processor.

2.2 Instructions for Processing. Workday shall only Process Personal Data in accordance with Customer's documented instructions. Customer instructs Workday to Process Personal Data to provide the Covered Service in accordance with the Agreement (including this DPE) and as further specified via Customer's use of the Covered Service. Workday will comply with additional written instructions issued by Customer if they are consistent with the terms and scope of the Agreement.

2.3 Compliance with Laws. Each party will comply with its obligations related to the Processing of Personal Data under applicable Data Protection Laws. Customer shall ensure that any instruction it issues to Workday complies with applicable Data Protection Laws. Workday shall inform Customer without undue delay if, in its reasonable opinion, an instruction issued by Customer violates applicable European Data Protection Laws.

2.4 Description of Processing. The agreed subject-matter, the nature, purpose and duration of data processing, the types of Personal Data and categories of Data Subjects are set forth in Addendum B to the DPE.

3. Subprocessors.

3.1 Use of Subprocessors. Customer agrees that Workday and Workday Affiliates may engage Subprocessors. Workday or the relevant Workday Affiliate engaging a Subprocessor shall ensure that such Subprocessor has entered into a written agreement that is no less protective than this DPE. Workday shall be liable for the acts and omissions of any Subprocessors to the same extent as if the acts or omissions were performed by Workday.

3.2 Notification of New Subprocessors. Workday shall make available to Customer a Subprocessor List and provide Customer with a mechanism to obtain notice of any updates to the Subprocessor List. At least thirty (30) days prior to authorising any new Subprocessor to Process Personal Data, Workday shall provide notice to Customer by updating the Subprocessor List.

3.3 Subprocessor Objection Right. Customer may object to Workday's use of a new Subprocessor on reasonable grounds relating to data protection by providing written notice to Workday within fourteen (14) days following Workday's notification pursuant to Section 3.2 above. Should Workday choose to retain

the objected-to Subprocessor, Workday will notify Customer and Customer may terminate the relevant portion(s) of the Covered Service within thirty (30) days. Upon any termination by Customer pursuant to this Section, Workday shall refund Customer any prepaid fees for the terminated portion(s) of the Covered Service that were to be provided after the effective date of termination.

4. Data Subject Rights.

4.1 Assistance with Data Subject Requests. Workday will, in a manner consistent with the functionality of the Covered Service and Workday's role as a Processor, provide reasonable support to Customer to enable Customer to respond to Data Subject requests to exercise their rights under applicable Data Protection Laws ("**Data Subject Requests**").

4.2 Handling of Data Subject Requests. For the avoidance of doubt, Customer is responsible for responding to Data Subject Requests. If Workday receives a Data Subject Request or other complaint from a Data Subject regarding the Processing of Personal Data, Workday will promptly forward such request or complaint to Customer, provided the Data Subject has given sufficient information for Workday to identify Customer.

5. Workday Personnel.

Workday shall require screening of its personnel who may have access to Personal Data, and shall require such personnel (i) to Process Personal Data in accordance with Customer's instructions as set forth in this DPE, (ii) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and (iii) to be subject to confidentiality obligations which survive their employment termination.

6. Personal Data Breach.

If Workday becomes aware of a Personal Data Breach, it shall without undue delay notify Customer in accordance with the Unauthorised Disclosure provisions of the MSA. Workday shall take appropriate measures to address and mitigate the adverse effects of the Personal Data Breach. To the extent Customer requires additional information from Workday to meet its Personal Data Breach notification obligations under applicable Data Protection Laws, Workday shall provide reasonable assistance to provide such information to Customer taking into account the nature of Processing and the information available to Workday.

7. Security of Processing.

Workday shall implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data as described in the Universal Security Exhibit.

8. Audit.

Where Workday has obtained third-party audit reports and certifications for its Covered Services ("**Audit Reports and Certifications**"), Workday will, at Customer's request and subject to the confidentiality terms set forth in the MSA, make its most recent Audit Reports and Certifications available to Customer for the applicable Covered Service.

To the extent that Workday has not obtained Audit Reports and Certifications for a Covered Service, or that Customer reasonably determines that the Audit Reports and Certifications are not sufficient to demonstrate compliance or to respond to a regulatory audit, Workday will allow Customer or an independent auditor appointed by Customer to conduct an audit, subject to the following: (a) Customer and Workday will mutually agree upon the scope, timing, duration, and control and evidence requirements; (b) Customer is responsible for all costs and fees related to such audit and will reimburse Workday for any services performed by Workday at Workday's then-current rates; and (c) to the extent the audit is conducted by a third-party audit firm; (i) the third-party audit firm is not a competitor of Workday; and (ii) Customer has, prior to such audit, entered into an agreement with such third-party audit firm containing confidentiality terms no less protective than the confidentiality terms set forth in the MSA.

9. Data Protection Impact Assessments.

Workday will, at Customer's request and subject to the confidentiality terms set forth in the MSA, make its most recent Audit Reports and Certifications available to Customer. To the extent Customer requires additional assistance to meet its obligations under applicable Data Protection Laws to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer's use of the Covered Service, Workday will, taking into account the nature of Processing and the information available to Workday, provide reasonable assistance to Customer.

10. Return and Deletion of Personal Data.

Upon termination of the Covered Service, Workday shall, and shall cause any Subprocessors to, at the choice of Customer, return all Personal Data to Customer or securely return and delete Personal Data in accordance with the relevant provisions of the Agreement.

11. International Transfers of Personal Data.

To the extent Customer's use of the Covered Services involves a Restricted Transfer Addendum A to this DPE will apply.

12. General Provisions.

12.1 Customer Affiliates. Customer is responsible for coordinating all communication with Workday on behalf of its Affiliates with regard to this DPE. Customer represents that it is authorised to enter into this DPE and any transfer safeguards entered into under this DPE, issue instructions, and make and receive any communications or notifications in relation to this DPE on behalf of its Affiliates.

12.2 Termination. The term of this DPE will end simultaneously and automatically at the later of (i) the termination of the Agreement or, (ii) when all Personal Data is deleted from Workday's systems.

12.3 Conflict. This DPE is subject to the non-conflicting terms of the Agreement. With regard to the subject matter of this DPE, if inconsistencies between the provisions of this DPE and the Agreement arise, the provisions of this DPE shall prevail with regard to the parties' data protection obligations.

12.4 Customer Affiliate Enforcement. Customer's Affiliates may enforce the terms of this DPE directly against Workday, subject to the following provisions:

i. Customer will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Agreement (each an "**Affiliate Claim**") directly against Workday on behalf of such Affiliate, except where the Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to such Affiliate Claim; and

ii. for the purpose of any Affiliate Claim brought directly against Workday by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

12.5 Remedies. Customer's remedies (including those of its Affiliates) with respect to any breach by Workday (including any breach caused by Workday's Affiliates and Subprocessors) of the applicable terms of this DPE, and the overall aggregate liability of Workday and its Affiliates arising out of, or in connection with the Agreement (including this DPE) will be subject to any aggregate limitation of liability that has been agreed between the parties under the Agreement.

12.6 Miscellaneous. The section headings contained in this DPE are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPE.

Addendum A: International Transfers of European Personal Data

1. Definitions.

"**Data Privacy Framework**" means the EU-U.S., Swiss-U.S., and UK-U.S. Extension to the Data Privacy Framework maintained by the United States Department of Commerce determined to provide an adequate level of protection for Personal Data transfers to certified commercial organisations in the United States under (i) the European Commission's Adequacy Decision 2023/4745 of 10 July 2023 and (ii) other applicable Data Protection Laws.

"**SCCs**" means (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 ("**EU SCCs**"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the UK Data Protection Act 2018 (version B1.0 of 21 March 2022) as updated or amended ("**UK Addendum**"); and (iii) where the Swiss Federal Act on Data Protection applies, the EU SCCs with Swiss modifications.

"**Workday BCRs**" means Workday's EU Processor Binding Corporate Rules ("**EU BCRs**") and UK Processor Binding Corporate Rules ("**UK BCRs**"). The Workday BCRs are accessible through Workday's website (currently located at http://workday.com/legal/bcrs.html).

2. Data Privacy Framework.

Workday, Inc. is self-certified to and complies with the Data Privacy Framework and will remain certified for the term of the Agreement.

3. Transfer Mechanisms.

3.1 BCRs. The EU BCRs apply to the Processing of Personal Data protected by the EU GDPR and the UK BCRs apply to the Processing of Personal Data protected by the UK GDPR, for the Covered Services listed in Schedule 3 to the Workday BCRs. All provisions of the Workday BCRs are incorporated by this reference and shall be binding and enforceable for Customer according to Section 1.4 of the Workday BCRs as if they were set forth in this DPE in their entirety. If any conflict or inconsistency arises between this DPE and the Workday BCRs, the Workday BCRs shall prevail.

3.2 SCCs. Restricted Transfers of Personal Data will be governed by SCCs Module 3 implemented between Workday (as "data exporter") and its Subprocessors (as "data importers").

3.3 Order of Precedence. Where more than one transfer mechanism applies, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) the Workday BCRs, and (ii) the SCCs.

3.4 Transfer Impact Assessments. Workday has carried out transfer impact assessments in accordance with the GDPR evaluating Workday's opinion that the DPE including the Workday BCRs and SCCs provide appropriate safeguards taking into account the information available to Workday and the nature of the Processing. Upon request, Workday shall provide Customer with a summary of such transfer impact assessments to Customer.

3.5 Notifying Data Subjects. Where required by Data Protection Laws, Customer shall inform Data Subjects that their Personal Data could be transmitted to a third country not providing adequate protection.

Addendum B: Description of Processing

Categories of data subjects whose personal data is transferred

1. Job applicants, candidates, current and former members of staff.
2. Related persons (e.g., emergency contacts, dependents, or beneficiaries).
3. Staff of prospects, customers, business partners and Workdays.

Categories of personal data transferred

Customer determines the categories of Personal Data Processed within Covered Services subscribed to. Typically, the transferred personal data will include the categories of data identified below:

1. Job applicants, candidates, current and former members of staff:

Name; contact information (including home and work address; home and work telephone numbers; mobile telephone numbers; web address; instant messenger; home and work email address); marital status; citizenship information; visa information; national and governmental identification information; drivers' license information; passport information; banking details; military service information; date of birth and birth place; gender; employee identification information; education, language(s) and special competencies; certification information; probation period and employment duration information; job or position title; business title; job type or code; business site; company, supervisory, cost center and region affiliation; work schedule and status (full-time or part-time, regular or temporary); compensation and related information (including pay type and information regarding raises and salary adjustments); payroll information; allowance, bonus, commission and stock plan information; leave of absence information; employment history; work experience information; skills, information on internal project appointments; accomplishment information; sentiments, personal opinions, feedback, training and development information; award information; membership information; information on emergency contacts, beneficiaries and dependents.

2. Related persons:

Name and contact information (including home address; home and work telephone numbers; mobile telephone numbers); date of birth; gender.

3. Staff of prospects, customers, business partners and Workdays:

Name and contact information (including work address; work telephone numbers; mobile telephone numbers; web address; instant messenger; work email address); business title; company; course enrollment information, including completion of courses, exam results and feedback provided.

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

Unless otherwise agreed, the transferred Personal Data may comprise special categories of personal data, such as ethnicity, religious beliefs, trade union membership information and health data (employee sick leave, disability information). Taking into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons, Workday has implemented the technical and organisational measures, including specialised training of staff and system access logs, to ensure an appropriate level of protection for such sensitive data.

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

Transfers will be made on a continuous basis.

Nature of the processing

Workday acts as a processor for the Personal Data Customer submits electronically into Workday's enterprise cloud applications or provides to Workday in connection with the Agreement.

-Processing Personal Data to set up, operate, maintain and support the enterprise cloud applications

-Storage of Personal Data in secure data centers

-Provision of Covered Services

Purpose(s) of the data transfer and further processing

Provision of enterprise cloud applications and professional services (as applicable) to Workday customers.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data will be retained for the duration of the Agreement in accordance with Section 12.2 of this DPE.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter and duration of the processing is outlined above within this Addendum. The nature of the specific sub-processing services are further particularised within the Subprocessor List (currently located at: https://www.workday.com/en-us/legal/subprocessors.html).

DPE - Frequently Asked Questions

Protecting the personal data our customers submit to Workday is one of our highest priorities and is integral to the success of our business. These FAQs provide information to assist customers when (1) selecting Workday as an enterprise cloud provider to process their workers' personal data and (2) reviewing Workday's Universal Data Processing Exhibit (or "DPE").

These FAQs do not form part of the contract or the DPE and are for informational purposes only.

What is Workday's role?

Workday acts as a processor for the personal data our customers submit electronically into our enterprise cloud applications or, where applicable, submit to Workday for implementation and consulting services ("Personal Data"). As such, Workday processes Personal Data on behalf of and according to our customers' instructions who are the controllers (or businesses).

Workday's customers either act as the controller or the processor of such Personal Data as set out in Section 2.1 of the DPE.

Does Workday make available a data processing agreement?

Workday offers a comprehensive DPE that operates seamlessly as part of Workday's UMSA to provide robust contractual terms for Workday's processing of Personal Data.

The DPE supports Workday's one-to-many service delivery model and our underlying technical and operational processes, such as our certifications, the performance of audits and our use of subprocessors.

Who are the parties to the DPE?

You are entering into our DPE as either a controller or a processor and Workday Limited is your processor. Any subsequent processors (both internal Workday subsidiaries and third parties) are subprocessors of Workday Limited but are not party to the DPE.

Will Workday's DPE work for companies operating globally?

Workday has customers around the globe, so we offer our customers industry-leading data processing terms that address data protection requirements around the globe. Our DPE incorporates the core privacy principles that underlie many international data protection laws.

Traditionally, European data protection laws have been among the world's strictest. To provide our global customers with a robust framework, we have used the strict GDPR requirements as the baseline for our DPE. As new laws take effect, we adjust as necessary to ensure continued compliance with data protection laws

Does Workday comply with data protection laws?

Workday complies with all data protection laws directly applicable to Workday.

Nevertheless, it is our customers' responsibility to determine whether it is appropriate for them to use our enterprise cloud applications to process their Personal Data considering the specific laws and regulations to which they are subject. It is also our customers' responsibility to configure and use our enterprise cloud applications in a manner consistent with their legal and regulatory obligations.

Does Workday have a Privacy Statement?

Yes, Workday maintains a privacy statement that applies when Workday is the controller of personal data. Currently, our privacy statement can be found at https://www.workday.com/en-us/privacy.html.

Does Workday's DPE cover professional services delivered by Workday?

Yes, Workday's DPE covers consulting and professional services delivered by Workday.

Subprocessors

Does Workday use subprocessors?

Workday uses subprocessors to provide the Covered Services (e.g., as part of our global follow-the-sun operations to make updates to our enterprise cloud applications and prevent or address service or technical issues). Any subprocessor that Workday engages to process our customers' Personal Data undergoes a thorough information security and data protection due diligence review and agrees to abide by data protection terms no less protective than the DPE.

Which subprocessors is Workday using?

Workday's subprocessor list can be accessed through the Workday website at https://www.workday.com/en-us/legal/subprocessors.html

How does Workday inform its customers about new subprocessors?

Workday will update the subprocessor list at least thirty days prior to authorising a new subprocessor to process Personal Data. Customers can subscribe to receiving email notifications for each Covered Service by signing up here. Our customers are responsible for ensuring that the individuals in their organisation who need to be notified about new subprocessors (e.g., their Privacy Team or Data Protection Officer) subscribe to the relevant Covered Service email updates and monitor their email accounts.

Can customers object to Workday's use of a new subprocessor?

Where required by law, Workday's customers can object to Workday's use of a new subprocessor on reasonable grounds relating to data protection. If Workday decides to retain a subprocessor to which a customer has objected, then the customer has the option to terminate the affected Covered Service.

International Data Transfers

Is Personal Data transferred outside of Europe in connection with Workday enterprise cloud applications?

In order to provide its enterprise cloud applications, Workday may use subprocessors (both Workday affiliates and third parties) located outside the European Economic Area ("EEA"), the United Kingdom ("UK") and Switzerland (together, "Europe"). For example, Workday provides 24/7 follow-the-sun support which necessarily means a degree of processing data in multiple time zones. For the purpose of international transfers, Workday Limited (our European headquarters in Ireland) is the "data exporter" under the GDPR and our customers are not transferring personal data outside of Europe.

How does Workday protect Personal Data transferred outside of Europe?

Workday uses the following data transfer mechanisms to legitimise transfers of Personal Data outside of Europe:

Adequacy Decisions

The European Commission recognises certain countries (and properly certified commercial organisations) around the world as offering an adequate level of protection for personal data. Workday relies on adequacy decisions in relation to transfers of Personal Data to the United States ("U.S."), New Zealand, Switzerland and the UK.

U.S. Data Privacy Frameworks

Workday, Inc. is self-certified under the EU-U.S., Swiss-U.S. and UK-U.S Extension to the Data Privacy Framework maintained by the U.S. Department of Commerce. Workday, Inc.'s certifications can be

inspected in the official Data Privacy Framework List of the U.S. Department of Commerce by searching for 'Workday'.

Binding Corporate Rules

Workday is one of the few companies worldwide to have an approved set of Processor Binding Corporate Rules (or "BCRs"). BCRs are a set of internal data protection policies that govern personal data processing within a multinational group. Under its BCRs, Workday can share the Personal Data it processes on behalf of its customers within its group in compliance with EU data protection laws. A list of enterprise cloud applications covered by the BCRs is provided in the Addendum of the DPE. The BCRs are accessible on Workday's website at http://workday.com/legal/bcrs.html.

Standard Contractual Clauses

Workday uses the European Commission's processor-to-processor Standard Contractual Clauses (Commission Implementing Decision 2021/914 of 4 June 2021) ("SCCs"). Workday has an Intra-Group Data Transfer and Processing Agreement ("IGDTPA") in place which incorporates the SCCs and reflects the data protection obligations agreed directly with our customers. Workday customers may also enter into the controller-to-processor SCCs directly with Workday, Inc.

The UK's Information Commissioner Office has validated the European Commission's SCCs as an equal alternative to the UK international data transfer agreement ("UK IDTA"). This simplifies the position for businesses that process UK Personal Data. For consistency across our customer base, we implement the SCCs via the ICO's "UK Addendum" as opposed to the UK IDTA within Workday's IGDTPA.

How does Workday assist customers in conducting transfer impact assessments (TIAs)?

Workday has conducted transfer impact assessments in line with the recommendations issued by the European Data Protection Board. Workday has published a comprehensive TIA Whitepaper to assist customers who choose to perform their own TIAs in connection with their use of Workday's enterprise cloud applications.

General Data Protection Regulation

What is the General Data Protection Regulation?

The General Data Protection Regulation (the "EU GDPR") is a European data protection law that took effect on May 25, 2018. The EU GDPR sets a global standard for data protection compliance by implementing strict requirements on how organisations handle and protect personal data. Following Brexit, section 3 of the European Union (Withdrawal) Act 2018 brought the EU GDPR into UK law (the "UK GDPR"). For the purpose of our relationship with our customers, at this time, they do not differ in substance so we refer to both laws collectively as "GDPR".

We are committed to supporting our customers' journey to compliance with the GDPR when they use Workday's enterprise cloud applications.

How does Workday assist its customers in fulfilling their obligations to respond to data subject requests under Chapter III of the GDPR?

Workday offers a suite of configurable features to help customers respond to their workers' requests to exercise their data protection rights such as requests to access, correct, delete or restrict the processing of their Personal Data and comply with data portability requests under the GDPR.

What technical and organisational measures has Workday implemented to protect Personal Data?

Workday has implemented robust technical and organisational measures designed to protect our customers' Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

However, data security is a shared responsibility. Our customers are responsible for implementing and maintaining privacy protections and security measures for components of the Workday enterprise cloud applications that they control.

Workday is certified to various industry standards such as ISO 27001, 27017, and 27018. See Workday's SOC 2 reports for more information on our technical and organisational measures.

Furthermore, Workday adheres to the EU Cloud Code of Conduct ("EUCoC") which provides independent third-party verification of Workday's technical and organisational measures. According to Article 28 (5) of the EU GDPR, adherence to a Code of Conduct can be used to demonstrate that sufficient guarantees have been made to implement appropriate technical and organisational measures as a processor. Workday's adherence report can be accessed at https://eucoc.cloud/en/public-register/list-of-adherent-services/.

How does Workday assist its customers fulfilling their obligation to notify personal data breaches?

Under the GDPR, controllers must notify the competent data protection supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Workday maintains incident response policies and plans, including a security incident policy, an incident response plan and a breach disclosure plan. If Workday becomes aware of a personal data breach affecting our customers' Personal Data, Workday will notify our customers without undue delay and assist our customers to meet their personal data breach notification obligations by providing the relevant information regarding the personal data breach.

How does Workday assist its customers with the GDPR requirements to conduct data protection impact assessments and prior consultations in relation to their use of a Workday enterprise cloud application?

To help identify risks to individuals' rights, Article 35 of the GDPR requires controllers to carry out a Data Protection Impact Assessment ("DPIA") if a specific processing activity is likely to result in a "high risk" to the rights and freedoms of an individual.

Where customers require additional information from Workday to carry out a DPIA in relation to their use of our enterprise cloud applications, they can rely on the information in Workday's applicable audit reports and certifications. In addition, our customers can request Workday's assistance.

Does Workday's DPE meet the GDPR requirements for a data processing agreement?

Workday's DPE addresses the specific data processing agreement requirements laid out in Article 28 of the GDPR. The quick reference checklist below identifies each of the specific requirements of Article 28 GDPR and matches them against the relevant sections of Workday's DPE.

GDPR Requirement		DPE
Art.28 (3)	**Subject-matter and duration of the processing, the nature and purpose of the processing.**	**Sec. 2.4**
Art.28 (3)	**Type of personal data and categories of data subjects.**	**Sec. 2.4**
Art. 28 (3) (a)	**Processor processes the personal data only on documented instructions from the controller.**	**Sec. 2.2**

Art.28 (3) (b)	Persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.	Sec. 5
Art.28 (3) (c)	Processor has taken all measures required pursuant to Article 32 (Security of Processing).	Sec. 7
Art.28 (3) (d)	Processor respects the conditions referred to in paragraph 2 and 4 for engaging another processor.	Sec. 3
Art.28 (3) (e)	Processor assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.	Sec. 4
Art. 28 (3) (f)	Processor assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36.	
	Article 32 (Security of processing)	Sec. 7
	Article 33 (Notification of a personal data breach to the supervisory authority) Article 34 (Communication of a personal data breach to the data subject)	Sec. 6
	Article 35 (Data protection impact assessment) Article 36 (Prior consultation)	Sec. 9
Art. 28 (3) (g)	Processor will, at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services.	Sec. 10
Art.28 (3) (h)	Processor makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	Sec. 8

Universal Security Exhibit

This Workday Universal Security Exhibit applies to the Covered Service and Covered Data and is incorporated by reference into the relevant Call-Off Contract between Workday and Customer entered into under the G-Cloud 15 Framework and forming part of the Supplier Terms thereunder. Capitalised terms used herein have the meanings given in the Agreement, including attached exhibits, that refers to this Workday Universal Security Exhibit.

Workday maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of Covered Data as well as the associated risks, are appropriate to (a) the type of information that Workday will store as Covered Data; and (b) the need for security and confidentiality of such information. Workday's security program is designed to:

- Protect the confidentiality, integrity, and availability of Covered Data in Workday's possession or control or to which Workday has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Covered Data;
- Protect against unauthorised or unlawful access, use, disclosure, alteration, or destruction of Covered Data;
- Protect against accidental loss or destruction of, or damage to, Covered Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Workday may be regulated. Without limiting the generality of the foregoing, Workday's security program includes:

1. **Security Awareness and Training**. Mandatory employee security awareness and training programs, which include:

Training on how to implement and comply with its information security program; and

Promoting a culture of security awareness.

2. **Access Controls**. Policies, procedures, and logical controls:

To limit access to its information systems and the facility or facilities in which they are housed to properly authorised persons;

To prevent those workforce members and others who should not have access from obtaining access; and

To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the data centers housing Covered Data is limited to properly authorised individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any security breach of any application or system directly associated with the accessing, processing, storage or transmission of Covered Data.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Covered Data or production systems that contain Covered Data.

6. **Audit Controls**. Technical or procedural mechanisms put in place to promote efficient and effective operations, as well as compliance with policies.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Covered Data and to protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorised access to Covered Data that is being transmitted over a public electronic communications network or stored electronically

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Covered Data, taking into account available technology so that such data cannot be practicably read or reconstructed

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its information security program, including:

    a) Designating a security official with overall responsibility; and

    b) Defining security roles and responsibilities for individuals with security responsibilities.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

    a) Reviewing changes affecting systems handling authentication, authorisation, and auditing;

    b) Reviewing privileged access to Workday production systems processing Covered Data; and

    c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Workday makes to production systems, applications, and databases processing Covered Data. Such policies and procedures include:

a) A process for documenting, testing and approving the patching and maintenance of the Covered Service;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c) A process for Workday to utilise a third party to conduct web application level security assessments. These assessments generally include testing, where applicable, for:

    i) Cross-site request forgery

    ii) Services scanning

    iii) Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing)

    iv) XML and SOAP attacks

    v) Weak session management

    vi) Data validation flaws and data model constraint inconsistencies

    vii) Insufficient authentication

    viii) Insufficient authorisation

14. Program Adjustments. Workday monitors, evaluates, and adjusts, as appropriate, the security program in light of:

a) Any relevant changes in technology and any internal or external threats to Workday or the Covered Data;

b) Security and data privacy regulations applicable to Workday; and

c) Workday's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

Production Support and Service Level Availability Policy (SLA)

Workday's Service is based on a multi-tenanted operating model that applies common, consistent management practices for all customers using the service. This common operating model allows Workday to provide the high level of service reflected in our business agreements. This document (the "SLA") communicates Workday's Production Support and Service Level Availability Policy its customers. Capitalised terms, unless otherwise defined herein, shall have the same meaning as in the primary Service subscription agreement between Workday and Customer ("MSA").

1. Service Availability:

Workday's Service Availability commitment for a given calendar month is 99.9%.

Service Availability is calculated per month as follows:

$$\left(\frac{\text{Total} - \text{Unplanned Outage} - \text{Planned Maintenance}}{\text{Total} - \text{Planned Maintenance}} \right) \text{ X } 100\% \geq 99.9\%$$

Definitions:

- **Total** is the total minutes in the month
- **Unplanned Outage** is total minutes that the Service is not available in the month outside of the Planned Maintenance window
- **Planned Maintenance** is total minutes of planned maintenance in the month.

Currently, Planned Maintenance is three (3) hours for weekly maintenance, plus four (4) hours for monthly maintenance, plus four (4) hours for quarterly maintenance. The Planned Maintenance windows can be found at Workday VNDLY Scheduled Maintenance (https://community.workday.com/node/521701). All times are subject to change upon 30 days' notice provided via the Workday Community site ("Community") and any such change shall not lengthen the duration of the associated maintenance window. If actual maintenance exceeds the time allotted for Planned Maintenance, it is considered an Unplanned Outage. If actual maintenance is less than time allotted for Planned Maintenance, that time is not applied as a credit to offset any Unplanned Outage time for the month.

The measurement point for Service Availability is the availability of the Production Instances at the Production data center's Internet connection points. Upon Customer request not more than once per month via the Workday case management system on Community, Workday will provide a Service Availability report.

2. Workday Feature Release and Service Update Process:

Periodically, Workday introduces new features in the Service with enhanced functionality across Workday applications. Features and functionality will be made available as part of a major feature release ("Feature Release") or as part of the weekly service updates ("Service Updates"). Feature Releases will take place approximately twice per year. The frequency of Feature Release availability may be increased or decreased by Workday at Workday's discretion with at least 30 days' prior notice to Customer on Community. Specific information and timelines for Feature Release and Service updates can be found on Community. Feature Releases will be performed during a weekend within any Planned Maintenance.

3. Service Response:

Workday's Service Response commitment is: (1) not less than 50% of online transactions in one second or less and (2) not more than 10% in 2.5 seconds or more. "Service Response" means the processing time of the Workday Production Instances in the Production data center to complete transactions submitted from a web browser. This Service Response commitment excludes online requests processed via background jobs, Workday Web Services, Innovation Services, Enhanced Features, or as analytics.

The time required to complete the request is measured from the point in time when the request has been fully received by the encryption endpoint in the Production data center, until the response begins to be returned for transmission to Customer. Customer may request a Service Response report not more than once per month via Community.

Customers may impact their own Service Response time by launching custom reports and integrations in excess of the limits set forth on Community. Workday may enforce reasonable and documented system limits to serve as guardrails for the Service where these reports and integrations negatively impact Service Response.

4. Production Disaster Recovery:

Workday will maintain a disaster recovery plan for the Workday Production Instances in conformance with Workday's most current Disaster Recovery Summary, which can be viewed on Community. Workday commits to a recovery time objective of 12 hours - measured from the time that the Workday Production Instance becomes unavailable until it is available again. Workday commits to a recovery point objective of 1 hour - measured from the time that the first transaction is lost until the Workday Production Instance becomes unavailable.

Workday will test the disaster recovery plan once every six months and will make available a written summary of the results of the most recent test for Customers on Community.

5. Case Submittal and Reporting:

Customer's Named Support Contacts may submit cases to Workday Support via Community. Named Support Contacts must be trained on the Workday products for which they initiate support requests. Each case will be assigned a unique case number. Workday will respond to each case in accordance with this SLA and will work diligently toward resolution of the issue taking into consideration its severity and impact on the Customer's business operations. Actual resolution time will depend on the nature of the case and the resolution itself. A resolution may consist of a fix, workaround, delivery of information or other reasonable solution to the issue. Case reporting is available on demand via Community.

6. Severity Level Determination:

Customer shall reasonably self-diagnose each support issue and shall recommend to Workday an appropriate Severity Level designation. Workday shall validate Customer's Severity Level designation or notify Customer of a proposed change in the Severity Level designation to a higher or lower level with justification for the proposal. In the event of a conflict regarding the appropriate Severity Level designation, each party shall promptly escalate such conflict to its management team for resolution through consultation

between the parties' management. In the rare case a conflict requires a management discussion, both parties shall make a representative available within one hour of the escalation.

7. Support Issue Production Severity Levels - Response and Escalation:

"Workday Response Commitment" means the period of time from when Customer logs the Production case in the Workday case management system via Community until Workday responds to Customer or escalates

within Workday, if appropriate. Because of the widely varying nature of issues, it is not possible to provide specific resolution commitments.

If Customer is not satisfied with the progress of a Severity Level 1 or 2 issue, Customer may escalate the case to Workday support management using the escalation process defined for Named Support Contacts. Upon escalation, Workday shall notify support senior management and shall assign a Workday escalation manager to work with Customer until the escalation is resolved.

Severity Level 1:

- Definition: The Service is unavailable or a Service issue prevents timely payroll processing, tax payments, entry into time tracking, financials closing (month-end, quarter-end or year-end), payment of supply chain invoices or creation of purchase orders, processing of candidate applications, issues that prevent financial aid disbursements, admissions, and registration activity of students. No workaround exists.
- Resolution: Workday will work to resolve the problem until the Service is returned to normal operation and will notify Customer of status changes.
- Escalation: If the problem has not been resolved within one hour, Workday will escalate the problem to the appropriate Workday organisation. The escalated problem will have higher priority than ongoing support, development or operations initiatives.
- Customer Response Commitment: Customer shall remain accessible for troubleshooting from the time a Severity 1 issue is logged until it is resolved.

Severity Level 2:

- Definition: An issue with the Service that prevents Customer from completing one or more critical business processes with a significant impact. No workaround exists.
- Resolution: Workday will work to resolve the problem until the Service is returned to normal operation and will notify Customer of status changes.
- Escalation: If the problem has not been resolved within six hours, Customer may request that Workday escalate the problem to the appropriate Workday organisation where the escalated problem will have higher priority than ongoing development or operations initiatives.
- Customer Response Commitment: Customer shall remain accessible for troubleshooting from the time a Severity 2 issue is logged until it is resolved.

Severity Level 3:

- Definition: An issue with the Service that prevents Customer from completing one or more important business processes that impact Customer's business operations. A workaround exists but is not optimal.
- Resolution: If resolution requires a Workday issue fix, Workday will add the issue fix to its development queue for future Service Updates and will suggest a potential workaround until the problem is resolved in a future Service Update. Workday will notify Customer of status changes.
- Escalation: If progress is not being made to Customer's satisfaction, Customer may request that Workday escalate the problem to the appropriate Workday organisation
- Customer Response Commitment: Customer will respond to Workday's requests for additional information and will implement recommended solutions in a timely manner.

Severity Level 4:

- Definition: An issue with the Service that delays Customer from completing one or more non-critical business processes that are not imperative to Customer's business operations. A workaround exists.
- Resolution: If resolution requires a Workday issue fix, Workday will add the issue fix to its development queue for future Service Updates and will suggest a potential workaround until the problem is resolved in a future Service Update. Workday will notify Customer of status changes.
- Escalation: If progress is not being made to Customer's satisfaction, Customer may request that Workday escalate the problem to the appropriate Workday organisation.
- Customer Response Commitment: Customer will respond to Workday's requests for additional information and will implement recommended solutions in a timely manner.

Severity Level 5 (Including Customer Care and Operations Requests):

- Definition: Non-system issues and requests such as Named Support Contact changes, SLA report. or general Service inquiries. Questions about product configuration and functionality should be addressed to Community.
- Resolution: Workday will respond to the request and will notify Customer of status changes.
- Escalation: If progress is not being made to Customer's satisfaction, Customer may request that Workday escalate the problem to the appropriate Workday organisation.
- Customer Response Commitment: Customer will respond to Workday's requests for additional information in a timely manner.

8. Support Hours and Support Response Commitments:

Workday provides Customer support 24 hours a day, 7 days a week for Severity Level 1 issues and will remain accessible for troubleshooting from the time a Severity 1 issue is logged until it is resolved. Workday provides Customer support on Mondays through Fridays (in Customer's local time) for all other Severity Levels. Workday Response Commitments start from the time the case is logged.

Support Issue Severity Level	Workday Response Commitment
1	1 hour / 7 days a week
2	6 hours / Monday – Friday
3	24 hours / Monday - Friday
4	24 hours / Monday – Friday
5	48 hours / Monday - Friday

9. Workday Support Scope:

Workday will support functionality that is delivered by Workday as part of the Service. For all other functionality, and for issues or errors in the Service caused by issues, errors, or changes in Customer's information systems, customisations, and third-party products or services, Workday may assist Customer and its third-party providers in diagnosing and resolving issues or errors, but Customer acknowledges that these matters are outside of Workday's support obligations. Failure to meet obligations or commitments under this SLA that is attributable to (1) Customer's acts or omissions (such as launching custom reports and integrations in excess of the limits set forth on Community); and (2) force majeure events shall be excused. Unless otherwise specified in the MSA or other applicable agreement, Customer must request

remedies for any Failure (however defined in the MSA or other applicable agreement) within 60 days after the applicable Failure occurs.

10. Workday Web Services API Support:

Workday recommends using the most recent version of the Workday Web Services ("WWS") APIs in order to receive optimum performance and stability. Prior versions of WWS APIs are updated to support backward-compatibility for all prior versions of WWS APIs that have not reached an end-of-life status. Workday will make end-of-life announcements no less than 18 months before the end-of-life of each WWS API. Workday will make announcements surrounding the WWS APIs through Community or, for APIs made available pursuant to the Workday Developer Program, through the Workday developer site. Backward-compatibility means that an integration created to work with a given WWS API version will continue to work with that same WWS API version even as Workday introduces new WWS API versions. With the exception of backward-compatibility updates, prior versions of WWS APIs are not enhanced.

11. Workday Developer Program App Support:

For customers subscribing to Workday Extend ("Extend") under an Order Form, Workday will support Extend in Production Tenants. All Apps developed pursuant to the Workday Developer Program, whether created by a customer, Workday or others, are expressly not covered by this SLA. Workday will not be responsible for any Service Availability downtime or delayed Service Response times caused by use of any Apps. Workday may modify or deprecate APIs, features and services made available pursuant to the Workday Developer Program in accordance with the Availability Statuses posted on the Workday developer site at developer.workday.com. Use of the developer site and all materials therein is governed by the Workday Developer Program Terms. "Apps" means the customisations, add-ons, extensions and/or other software solutions developed pursuant to the Workday Developer Program.

Acceptable Use Policy

This AUP is applicable to Customer's use of the Workday Service and is subject to change throughout the contract term. The latest version can be found at the following link: https://www.Workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html

This Acceptable Use Policy ("AUP") sets out the terms and conditions under which an individual or an organisation ("You" and "Your", as applicable) may use and interact with Workday Products (as defined herein). Unless otherwise defined herein, capitalized terms used in this AUP have the same meaning as set forth in the applicable agreement between You and Workday. This AUP is legally binding on You, and You are responsible for compliance with this AUP by Your Affiliates and Authorised Parties' use of Workday products, services, or features for which the applicable agreement or Order Form links to or references this AUP ("Workday Products"). Workday may revise this AUP by posting an updated version of the AUP on the Workday site and such updates will be effective upon posting.

Prohibited Uses

You may not use the Workday Products:

- In any way that breaches, promotes the breach of, or violates any Law;
- In any way that is unlawful, fraudulent, deceptive or misleading;
- For automated decision-making purposes (such as employment decisions) that have legal effects, unless You ensure a human being makes, reviews or oversees the final decisions;
- To sell or advertise the sale or purchase of any goods or services;
- To threaten, incite, promote, or encourage violence, self harm, or harm to individuals or specific groups including minors;
- To violate the privacy rights of others, including unlawful or unauthorized tracking, monitoring, or identification;
- To conduct unauthorized data scraping, web crawling, or other similar data extraction activity through a web client;
- To knowingly or recklessly upload, share, or transmit any data or material that contains viruses, spyware, adware, Trojan horses, worms, corrupt files, or other similar computer code designed to adversely affect the operation of the Workday Products or any computer software, hardware or networks;
- In any way that seeks to circumvent, disable, or otherwise compromise Workday Products or Workday environments, including the security of the Workday Products or Workday environments, any user account or any password; or
- To upload, send, or distribute unsolicited messaging, including SMS, emails, or comments.

Prohibited Content

All data, information, or materials ("**Content**") that You upload, contribute, submit, store, or add to the Workday Products must not:

- Infringe or misappropriate a third party's intellectual property or proprietary rights;
- Contain any material which is obscene, offensive, tortious, hurtful, inflammatory, or defamatory;
- Promote sexually explicit or pornographic material;
- Promote violence or any form of bullying or harassment, including threats, abuse, or invasion another's privacy;

- Promote discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age;
- Impersonate any individual or misrepresent Your identity or affiliation with any person or entity, or give the impression that information emanates from Workday (if that isn't the case); or
- Breach or promote the breach of any Law or any legal duty owed to a third-party, such as a contractual duty or a duty of confidence.

Compliance with This Policy

Workday is under no obligation to monitor, review, filter, moderate, or remove any Content from the Workday Products. Workday reserves the right, in its sole discretion, to determine whether or not You have abided by this AUP and will take whatever action it deems appropriate under the circumstances, including but not limited to:

- Immediate suspension of Your right to access or upload Content to the Workday Products;
- Immediate removal of any Content uploaded by You to the Workday Products;
- Taking legal action against You; or
- Disclosure of relevant information to law enforcement authorities.

Workday will use commercially reasonable efforts to provide You with notice of any such suspension and to minimise the length and scope of such suspension in light of the circumstances as set forth in the Agreement.

Compliance with Workday's Third-Party Subprocessors' Acceptable Use Policies and Additional Terms

The following additional terms and Acceptable Use Policies of Workday's third-party Subprocessors are incorporated by reference for applicable Workday Product and are subject to change at any time:

Applicable Service	**Applicable terms / Third-party Acceptable Use Policies**
Workday core Service to the extent a Customer Tenant and/or Instance (as applicable) is hosted by Amazon Web Services Workday Learning Media Cloud Extend and Extend Integration with Third Party Platform Services Workday's artificial intelligence and analytics features associated with all Product Lines	Amazon Web Services

Extend and Extend Integration with Third Party Platform Services Workday AI Gateway	You shall not: Misrepresent the origin of machine learning or artificial intelligence created content as original works Mislead with claims of expertise or capability in sensitive areas, such as employment, healthcare, finance, government services, or legal advice Make decisions in domains that affect economic opportunities, or material or individual rights or well being, such as employment, finance, legal, healthcare, housing, insurance, or social welfare without human review or other appropriate risk-mitigation techniques Identify natural persons using images of people
Workday AI Gateway	Google Generative AI Prohibited Use Policy You shall not: Use Workday AI Gateway to build applications used for clinical purposes (for clarity, non-clinical research, scheduling, or other administrative tasks is not restricted), as a substitute for professional medical advice, or in any manner that is overseen by or requires clearance or approval from any applicable regulatory authority.
Workday Messaging Peakon Messaging SMS Multi-Factor Authentication Candidate Experience Conversational Events and Campus Events features of Candidate Engagement	Twilio
Email Ingestion Email Analytics	Twilio SendGrid Email Policy
HiredScore AI for Recruiting HiredScore AI for Talent Mobility	Sinch Email Services

© 2026, Workday Limited.

Workday Subscription Order Form Template

ORDER FORM # xx to the MSA forming part of the Supplier Terms under G-Cloud 15 Call Off Contract Ref: xx

Customer Name	
Customer Address	
Workday Entity	Workday Limited (Registration number 521013) The Kings Building 152-155 Church Street Smithfield, Dublin 7, D07 AOTN
Universal Main Subscription Agreement (MSA)	This Order Form is subject to and governed by the MSA
Product Terms	Service SKUs are subject to the applicable Product Terms available at https://www.workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html, which are incorporated herein by reference.
MSA and Order Form Effective Date	The later of the dates of the parties' signatures below
Order Term	
Currency	GBP

Payment Schedule Table

Payment #	Payment Due Date	Payment Amount
1		
2		
	Total Payment Amount	

For the avoidance of doubt, the Payment Schedule Table will be used for invoicing purposes.

Subscription Fees Table

Subscription Period	Date Range	Subscription Fee
1		
2		
	Total Subscription Fee	

Subscription Rights Table

SKU	Service	Pricing Metric	Annual Subscription Rights
EMPVCE	Peakon Employee Voice	FSE*	Full Enterprise

*For Pricing Metric details see the Full-Service Equivalent ("FSE") Count Table below.

Full-Service Equivalent ("FSE") Count Table

FSE Population Category	Baseline FSE Count
Full Enterprise	

© 2026, Workday Limited.

Customer Contact Information

	Billing, In Care of Responsible for payment processing and will receive invoicing and billing-related communications.	**Customer Support** Main point of contact for Workday Support and will receive initial login credentials.	**Subscriptions Contact** Main point of contact for responding to and fulfilling the Growth and Expansion Obligations.
Contact Name			
Phone/Fax #			
Email			

This Order Form is subject to and governed by the MSA between Customer and Workday referenced above and the Peakon Addendum located at https://www.workday.com/en-us/legal/contract-terms-and-conditions/index.html . In the event of a conflict, the provisions of this Order Form take precedence over the MSA and its exhibits and attachments. The parties further agree to the terms in any attached or referenced Addendums and Exhibits. All remittance advice and invoice inquiries shall be directed to Accounts.Receivable@workday.com.

IN WITNESS WHEREOF, this Order Form is entered into as of the Order Form Effective Date.

Customer	**Workday Limited**
Signature	Signature
Name	Name
Title	Title
Date Signed	Date Signed

© 2026, Workday Limited.

Additional Order Form Terms Addendum

1. General.
Unless otherwise defined herein, capitalised terms used in this Order Form have the same meaning as set forth in the MSA. The Total Subscription Fee is based on the maximum indicated in the Subscription Rights Table and any use in excess of such maximum(s) indicated will be subject to the Growth and Expansion section herein. Annual Subscription Rights limits may not be decreased during the Order Term.

2. FSE Metric Calculation and Worker Category Definitions.
The total FSE Count is calculated by categorising each Worker to one of the Worker Categories below, multiplying the applicable number of Workers by the Applicable Percentage, and then adding the FSE Count for each Worker Category.

FSE Calculation Table:

Worker Category	Total Workers	Applicable Percentage	FSE Count
Standard Full-Time		100.0%	
Standard Part-Time		50.0%	
Contingents		25.0%	
Total FSE Count:			

The Service may be used by Customer only for the Worker Categories listed above and as defined below.

A "**Standard Worker (Full Time)**" is an employee who is categorized in the Service by Customer as full time according to Customer's standard employment policies and in accordance with applicable laws with an Active Record.

A "**Standard Worker (Part Time)**" is an employee who is categorized in the Service by Customer as part time according to Customer's standard employment policies and in accordance with applicable laws with an Active Record.

A "**Contingent Worker**" is a non-employee independent contractor or worker either directly engaged by Customer or employed through another entity and who is categorized in the Service by the Customer as contingent with an Active Record in the Service.

Former Workers with Static Records shall be excluded from the FSE calculation but may continue to be maintained in the Service. "Static Records" are records in the Service for workers with whom Customer has no further relationship and to whom Customer does not provide self-service access. Static Records include former worker records used solely for historical reference. All other worker records are "Active Records".

3. Growth and Expansion.
A. Annual Reporting Obligation.
Customer will report to subscriptions@workday.com no earlier than 90 days and no later than 60 days ("**Annual Reporting Period**") based on the number of Active FSE Worker Records as of 90 days ("**Count Date**") prior to each anniversary of the Order Term start date. Customer agrees to pay fees for any excess Subscription Rights at the Expansion Rates described below to cover the period from the anniversary of the Order Term start date immediately following the Annual Reporting Period through the subsequent anniversary date (each a "**Reporting Cycle**"). Customer understands that an order form will be required to document any annual fees due pursuant to this section in its entirety. Such order form must be executed no later than 30 days prior to each anniversary of the Order Term start date until the Renewal (as defined below), at which time the Annual Reporting Obligation will be incorporated into the Renewal Term.

© 2026, Workday Limited.

a. FSE Metric Reporting.

Reporting for Active FSE Worker Records is based on the additional FSE Workers which are defined as any Active FSE Worker records exceeding the Baseline FSE Count.

FSE Metric Expansion Table

SKU	Annual FSE Expansion Rate
EMPVCE	

B. Growth Event Reporting Obligation.

In addition to the Annual Reporting Obligation, if Customer exceeds any Subscription Rights by 5% or more ("**Growth Event**") as a result of any one-time addition of Workers (e.g., M&A), Customer must report the excess Subscription Rights to subscriptions@workday.com within 30 days of the Growth Event. Customer agrees to pay fees from the start date of the Growth Event through the subsequent anniversary date which will be documented under a separate order form.

Subscription Fees for Additional FSE Workers are due in accordance with the terms of the Agreement. An Order Form will be required to document annual fees due pursuant to this section.

4. Renewal.

Customer may renew its subscription for the Service by notifying Workday prior to the end of the Order Term and Workday will generate a new Order Form for a single three-year renewal term ("Renewal Term") at the below pricing. Such order form must be executed no later than 30 days prior to the end of this Order Term.

Renewal Table

Renewal Term Years	Annual Renewal Subscription Fees
1st year of Renewal Term	Base Subscription Fee x (1+ (5% Innovation Index + Renewal Term CPI))
2nd year of Renewal Term	Previous Year Subscription Fee x (1+ (5% Innovation Index + Renewal Term CPI))
3rd year of Renewal Term	Previous Year Subscription Fee x (1+ (5% Innovation Index + Renewal Term CPI))

The "**Base Subscription Fee**" is XX. The Expansion Rates for the Renewal Term shall be increased by the same percentage as the Annual Renewal Subscription Fees per year in the Renewal Table. Annual Renewal Subscription Fees are valid only if Customer's Base Subscription Fee is equal to or greater than the Base Subscription Fee defined herein. Fees for the Renewal Term are due by the first day of each corresponding year of the Renewal Term. Individual payments shall match the Annual Renewal Subscription Fee as defined in the Renewal Table above. If Customer wishes to procure any additional SKUs or Subscription Rights for a Renewal Term that are not included in the Base Subscription Fee, fees for those items will be in addition to the fees anticipated under this section.

5. Additional Definitions (as applicable).

"**CPI**" means the consumer price index established by the United States Department of Labor for All Urban Consumers, US City Average, All Items (change in annual average).
"**Renewal Term CPI**" means CPI established for the calendar year prior to the most recent February 1 preceding the Renewal Term, if a positive number.
"**Innovation Index**" means the fixed annual rate of increase in Subscription Fees based on improved Service functionality and performance that is a result of Workday's efforts and investment in product development and infrastructure.

© 2026, Workday Limited.

Workday Service SKU Descriptions Addendum

Customer may only use the Service SKUs subscribed to as indicated in the body of this Order Form.

Service	Product Line	Description
Peakon Employee Voice	Peakon	Workday Peakon Employee Voice provides organisations with the data required to surface granular insights around employee engagement, sentiment and inclusion, capturing real-time feedback across the organisation. Workday Peakon Employee Voice delivers timely and relevant questions to your workforce and delivers data insights across the entire employee lifecycle, coupled with contextual guidance, targeted learning and development opportunities, action plans and reports, and prescriptive action tracking features. Workday Peakon Employee Voice provides standard question sets aligned to topics such as employee engagement, diversity & inclusion, health & wellbeing, manager and employee sentiment, as well as the ability to create custom questions. Global and industry benchmarks, aggregated from the results of standard questions sets, provide companies the ability to compare to similar organisations.

© 2026, Workday Limited.

Product Terms

These Product Terms apply to the Peakon Product Line SKUs subscribed to in an Order Form. Unless otherwise defined herein, capitalised terms used in these Product Terms have the same meaning as set forth in the Agreement or the Order Form.

These Product Terms may be updated by Workday from time to time; provided that no update materially decreases the applicable security and privacy commitments and any such changes will not become effective until 30 days after publication of the updated Product Terms.

The latest version of the Product Terms are accessible via the following link: https://www.workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html

Documentation	Documentation for this Product Line can be found here: https://doc.workday.com/
Audit Reports	Audit Reports applicable to this Product Line can be found here: https://community-content.workday.com/content/workday-community/en-us/reference/learn/resources/workday-compliance-program-product-line-coverage.html
Support	Support for this Product Line is provided as set forth in the Workday SLA found here: https://www.workday.com/en-us/legal/universal-contract-terms-and-conditions/index.html
Subprocessors	Subprocessors associated with this Product Line can be found here: https://www.workday.com/en-us/legal/subprocessors.html
Enhanced Features	Customer Content is required to train and improve Workday's artificial intelligence and analytics features associated with this Product Line.
Early Access	Through Workday's early access programs, Customer may access and use certain functionality associated with this Product Line that are not yet generally available ("**Peakon EA Functionality**"). By participating in such programs, Customer agrees and understands that (a) the Peakon EA Functionality is still in the design phase and remains subject to change and/or removal at Workday's sole discretion, and may therefore be used by Customer for evaluation and testing purposes only; (b) Customer is responsible for verifying the accuracy of the outputs of any such Peakon EA Functionality and making corrections as needed; (c) Workday will not support data conversions; (d) any data entered and configurations made by or for Customer before general availability may not be preserved; and (e) any products or features ultimately resulting from the Peakon EA Functionality may be distributed under various Workday offerings and may be subject to additional fees. Customer Content is used to train and improve Workday's artificial intelligence and analytics components associated with this Product Line.

© 2026, Workday Limited.

Additional Terms	The terms in this Additional Terms section apply only to the extent that Customer uses the specific functionality indicated below. While Workday has developed artificial intelligence and analytics features offered as part of this Product Line with a variety of situations in mind, Customer's use and configurations of such features may result in new and untested results and outcomes. Customer is responsible for assessing the suitability of any such features and results prior to making them available to its users. Customer shall not submit Protected Information to the features and functionality associated with this Product Line, which is not designed for the processing of Protected Information. "**Protected Information**" means Protected Health Information as defined in 45 C.F.R. §160.103 or other health information regulated under Data Protection Laws applicable to Customer. The Workday SLA applies to Peakon in all respects, except that Workday will make end of life announcements through a Workday Customer portal before the end of life of any Peakon API. Peakon Messaging: To the extent Customer elects to use the Peakon short message service ("**Peakon Messaging**"), Customer agrees that (a) any third-party subprocessor used to deliver Peakon Messaging ("**SMS Provider**") is, by necessity, a separate data controller of individual data subjects' telephone numbers as required for purposes of providing and optimising functionality and security, investigating improper use, and complying with applicable Law, audit, regulatory and compliance frameworks, and (b) once data is delivered from each applicable SMS Provider to telecommunications providers the data is no longer part of the Service. The SMS Provider's handling of this data as a separate data controller is set forth in the SMS Provider's Binding Corporate Rules: https://www.twilio.com/legal/binding-corporate-rules and Privacy Notice: https://www.twilio.com/legal/privacy.

© 2026, Workday Limited.

Workday Training Order Form Template

Customer Name	
Workday Entity Name	Workday Limited
Call-Off Contract Effective Date	
Order Effective Date	
Training Credit Order Term	18 months from the Order Effective Date
Training Subscription Order Term	
Currency	GBP
Total Training Fees	

Payment #	Payment Due Date	Payment Amount
1		
	Total Payment Amount	

SKU	Training Offering	Annual Rate	Quantity	Term	Total Training Fees

SKU	Training Offering	Price Per Credit	Quantity	Total Training Credit Fees
TC	Training Credits			

© 2026, Workday Limited.

Customer Contact Information	Billing, In Care of
Contact Name	
Street Address City/Town, Region/Postal Code Country	
Phone/Fax #	Phone: Fax:
Email (Required)	

SKU	Training Offering	Price Per Credit	Quantity	Total Training Credit Fees
			Total (TC) Training Fees	

This Order Form is subject to and governed by the Call-Off Contract. This Order Form (including the Addenda attached hereto) incorporates the Training Terms attached hereto as Addendum A ("**Training Terms**") and the Bulk Training Credit Rates attached hereto as Addendum B (the "**Bulk TC Rates**"). In the event of a conflict between the terms of the MSA, the Training Terms, this Order Form, and the attached Addenda, the order of precedence is this (i) Order Form, (ii) Addendum B (Bulk TC Rates), (iii) Addendum A (Training Terms), (iv) the MSA. All remittance advice and invoice inquiries shall be directed to Accounts.Receivable@workday.com.

© 2026, Workday Limited.

Addendum A - Workday Training Terms

These Training Terms apply to Courses and other training-related products and services offered to Workday's Customers and Partners ("**Workday Training**"). Capitalised terms used in these Training Terms that are not defined in this document have the meanings in the MSA (with respect to Customers) or in the Partner Agreement (with respect to Partners). Descriptions of Workday Training Courses and processes are provided in Workday Community. Workday Training may be purchased on an Order Form or in Workday Community. Purchaser is responsible to meet Workday's Course and other training requirements published in Workday Community and Workday Learning Center.

1. Permitted Use & Restrictions

a. Permitted Use. Workday Training is solely for use by (i) Customer Learners only to support Customer's internal use of the Service consistent with the MSA; and (ii) Partner Learners only for purposes consistent with the applicable Partner program, and unless otherwise agreed by Workday and Partner in writing, to enable such Partner to perform Workday-related services only for Customers. Workday Training and Training Content may be used only during the applicable term of Purchaser's agreement with Workday.

b. Restrictions. Except as expressly provided herein or with Workday's express prior written consent, neither Purchaser nor Learner will (i) allow any individual other than the enrolled Learner to attend Workday Training or use any Training Content, provided that Purchasers or Learners may request accommodations as provided in Workday Community; (ii) copy, modify, make derivative works of, or distribute any Training Content; or (iii) incorporate any Training Content (including screenshots) in any material. Failure to comply with these Training Terms may expose Purchaser and Learner to legal or disciplinary action by Workday, including restriction or removal from Workday Training, cancellation of certifications, and copyright infringement proceedings.

2. Product Specific Terms

a. Dedicated Training (*Customers only*). Customers may request Workday to present in-person or live virtual Courses to Customer Learners ("**Dedicated Training**"), subject to Workday's availability and approval. Fees for Dedicated Training are determined by the number of Learners and the Training Fees or Training Credits required for the Course, plus additional fees for Workday Training not provided at a Workday training center. The fees for Dedicated Training cancellation requests not received within the Cancellation Notice Period are 50% of the Training Fees or Training Credits plus all additional fees for onsite training. Additional health-related terms applicable to in-person training may be set forth in Workday Community.

b. Training Subscriptions. Workday Training Subscriptions (e.g., Learn On-Demand, Adoption Kit, Administrator Training Kits) may be used only by the "**Named Users**" identified by Customer in Workday Community during the Order Term. Partner Named Users are Learners registered in the Workday Learning Center. The Order Form for a Training subscription will specify the number of permitted Named Users.

c. eBooks. For certain Workday Training, Workday will make available one eBook to each Learner in electronic format. Learners may use the eBook only for Learner's individual, private study for the Workday Training and may print one copy for such use.

d. Workday Certification Programs. Workday offers certification programs to Customers and Partners as identified in the Training Catalog. Partner certifications are available only to certain partners as set forth in the Partner Agreements. To obtain and maintain certification, Learners must complete all requirements and pass applicable testing. Certifications: (i) are granted to individual Learners and are not owned or controlled by Purchasers; (ii) are not transferable to any Purchaser or another individual; (iii) automatically expire if the Learner fails to maintain updated certification requirements and when the Learner leaves employment or engagement with Purchaser, unless Workday consents (in writing at its sole discretion) to Learner's request to transfer certifications upon Learner's subsequent employment or engagement by another Purchaser; and (iv) may be canceled for other reasons at Workday's sole discretion.

© 2026, Workday Limited.

e. Downloadable Content (Customers). Customer may download the Downloadable Content during the Order Term covering the Downloadable Content and internally use, copy, modify, and create derivative works of the Downloadable Content solely to help Customer successfully roll out the Service across its organisation in accordance with the MSA and these Training Terms. Customer is solely responsible for any derivative works and other modifications to Downloadable Content made by or for Customer. Customer owns all derivative works and other materials that Customer is permitted to develop, make, or conceive under this section ("**Customer Improvements**"), except that Workday retains all underlying intellectual property rights in the Downloadable Content, the Service, and all Training Content. Customer may use the Workday property incorporated into the Customer Improvements only as provided in this section. Workday may create, modify, use, transfer, and distribute material that is substantially similar to Customer Improvements. Customer will reproduce all Workday proprietary rights notices on copies and revised versions of Downloadable Content. Workday may add, change, or remove Adoption Kits and portions of other Downloadable Content at any time, subject to the applicable Order Form terms.

3. Fees and Training Credits

a. Fees and Payment. Purchaser will pay Workday for all Workday Training enrolled in or taken under Purchaser's account, unless timely canceled in accordance with these Training Terms. No refunds or credits will be given for failure to meet Workday Training or Course requirements or for late cancellation. Workday is not responsible for costs incurred by Purchaser or Learners to participate in Workday Training. Training Fees are set forth in the Training Catalog. Purchaser will pay all Training Fees and fees for Training Credits in accordance with applicable Order Form, or, if none, the terms of the MSA or Partner Agreement, as applicable.

b. Training Credit Bulk Purchase Option. Fees for bulk purchases of Training Credits will be set forth in an Order Form and such fees will apply to the cumulative number of prepaid Training Credits purchased at any time during any rolling 12-month period during the Order Term. Bulk Training Credit Rates will not be applied retroactively for previously purchased Training Credits or for a la carte Workday Training purchases (e.g., Course purchases from the Workday Learning Center).

c. Training Credit Use. Purchaser may use Training Credits to pay for any TC-Eligible Course that starts on or after the Order Effective Date and ends on or before 18 months after the Order Effective Date. For Self-Directed Courses purchased with Training Credits, Learners must enroll in the Course before the Training Credit expiration date but can begin the Course after such date. Training Credits are decremented from Purchaser's Training Credit balance upon Course enrollment. If a Purchaser enrolls in a TC-Eligible Course without an adequate Training Credit balance, Workday will invoice Purchaser for the Training Fees for the Course. Self-Directed Courses also may be referred to as Learn Independent Courses.

4. Cancellation & Termination

a. Course Change or Cancellation by Purchaser or Learner. Subject to the exceptions in this Section, Purchaser or Learner may reschedule time or date of Course attendance or cancel a Course enrollment without charge if such change is entered into the Workday Learning Center within the applicable Cancellation Notice Period; provided, however, that all changes related to an exam that is scheduled with Workday's exam provider must be made in the provider's system. For timely changed or canceled Courses, Workday will restore the Training Credit(s) decremented or will not charge Purchaser for the Training Fees. Notwithstanding the foregoing sentences in this Section, the following events are deemed to be Course cancellations ineligible for credit or refund: (i) failure to timely meet Workday Training or Course requirements or attend an entire Course; (ii) Course changes and cancellations not within applicable Cancellation Notice Period; (iii) withdrawals or cancellations from Self-Directed or Refresher Courses or Workday Pro exams after the Purchaser's Training Coordinator has approved the Course or exam; and (iv) Learner does not take or pass any required exam.

b. Course Change or Cancellation by Workday. If Workday discontinues a Self-Directed or Refresher Training Course or an exam, the Learner must attend/take the Course or exam prior to the final offering date announced by Workday. Workday will not refund Training Fees or restore Training Credits if Learner does not do so. If Workday cancels any other Course, Workday will restore Training Credits decremented from Purchaser, or will not charge Purchaser for Training Fees, for such Course. Workday is not

© 2026, Workday Limited.

responsible for any costs or expenses incurred by Purchaser or Learner in connection with any Workday-canceled Workday Training.

5. Miscellaneous

a. Updates. Workday reserves the right to add, change, or discontinue Workday Training offerings from time to time without notice to Purchasers or Learners. Please consult the Training Catalog for the most current Workday Training offerings. Workday may modify these Training Terms from time to time in its sole discretion; provided the overall features and substance of the Workday Training program will not be materially decreased during the applicable Order Term.

b. Privacy. Workday may provide Purchaser and Learners with notices, including notices regarding changes to these Training Terms, by email, regular mail, or postings in Workday Community or the Workday website. Workday may provide information about a Learner's training activity to the applicable Purchaser, to subsequent Purchasers that hire or engage such Learner, and to third parties used by Workday from time to time to facilitate Workday Training. Workday's Privacy Statement currently located at https://www.workday.com/en-us/privacy.html applies to Workday Training. Purchaser will obtain all necessary rights and permissions (including consent from Learners and Purchaser's assignees, where required) to provide the Learner information described in this subsection to Workday so that Workday may provide Workday Training.

c. Order of Precedence. In the event of a conflict among these Training Terms, the applicable Order Form, the MSA or Partner Agreement, and any terms contained in Workday Community, as applicable, the order of priority is (1) the Order Form, (2) these Training Terms, (3) the MSA or Partner Agreement, as applicable, and (4) terms regarding Workday Training in Workday Community.

d. Miscellaneous. Workday Training is not subject to any SLA and is not part of the Service. Workday Training is not covered under any Workday audit report or ISO Certification. Any audit activities and Customer information requests will be addressed in accordance with the optional Universal Customer Audit Program Order Form.

6. Definitions

"**Cancellation Notice Period**" means (a) at least 7 full calendar days before Course start date, (b) within 24 hours of enrollment for Courses enrolled within 7 full calendar days of Course start date, or (c) at least 14 full calendar days before Course start date for Dedicated Training.

"**Course**" means any Workday Training course, exam, or other training offering listed in the Training Catalog or in the Workday Learning Center.

"**Downloadable Content**" means the portions of training offerings (e.g., Adoption Kit, Administrator Training Kits, Peakon Voice Fundamentals Course) that Workday expressly permits a Learner to download for use as described herein.

"**Learner**" means an individual employee, permitted independent contractor, or Authorised Party (for Customers only) of a Purchaser registered in the Workday Learning Center as a Learner under Purchaser's registered email domain.

"**Partner Agreement**" means the agreement under which the Purchaser is participating in any Workday Partner Program and such participation provides access to Workday Training.

"**Purchaser**" means a Customer or Partner that purchases Workday Training or is authorised to enroll Learners in Workday Training.

"**TC-Eligible Course**" means the Workday Training eligible to be purchased with Training Credits as identified in the Training Catalog with the number of "Credits" required for purchase.

"**Training Catalog**" means the applicable catalog of available Workday Training in Workday Community.

© 2026, Workday Limited.

"**Training Content**" means all Course materials (including, without limitation, eBooks; Downloadable Content; Course structure, look and feel, and descriptions) and all other material made available by Workday in connection with Workday Training, whether presented visually, audibly, electronically, or in printed form.

"**Training Credit**" means prepaid credits redeemable for Workday Training in lieu of paying Training Fees.

"**Training Fee**" means the fee (other than Training Credits) established by Workday from time to time for each Course.

© 2026, Workday Limited.

Addendum B - Bulk Training Credit Rates

The following rates apply to the bulk purchases made within the 12-month period following the Order Effective Date, with the discount level based on the cumulative number of Prepaid Training Credits Acquired as determined under the Section 3.b. of the Training Terms:

Prepaid Training Credits Acquired	Rate Per Training Credit
1-10	
11-25	
26-50	
51-75	
76-100	
101-249	
250+	

© 2026, Workday Limited.

Workday Consulting Customer Audit Program Order Form

Customer Name	
MSA Effective Date	
Order Effective Date	
Order Term	
Currency	GBP
Program Item	Audit Services

Program Costs

Customer will pay for Workdays's assistance with providing specific information regarding the Covered Service provided to Customerr under the applicable subscription Order Form at the hourly rate of £246 per hour. The hourly rate specified herein will remain in effect for the duration of the Order Term. Workday shall perform all Audit Services remotely unless mutually agreed otherwise with Customer. To the extent Workday personnel is required to travel for any onsite audit, Workday will provide Customer with an estimate of such travel expenses prior to travel, and Workday shall invoice Customer for such travel expenses in accordance with Workday's travel and expense policy.

Customer Billing

Workday will invoice Customer upon completion of the Program Item. The following table outlines the milestones that will indicate Program Item completion.

Program Item	Customer Billing Milestone
Audit Services	Workday will bill Customer for the hours spent and travel expenses incurred at the conclusion of the Audit Services.

This Order Form is only valid and binding on the parties when executed by both parties and is subject to the terms in the above-referenced MSA, including the Universal Data Processing Exhibit (UDPE). In the event of a conflict, the provisions of this Order Form take precedence over the MSA and its exhibits and attachments. All remittance advice and invoice inquiries can be directed to Accounts.Receivable@workday.com.

© 2026, Workday Limited.

Customer	Workday Limited
Signature	Signature
Name	Name
Title	Title
Date Signed	Date Signed

© 2026, Workday Limited.

Workday Application Penetration Testing Order Form Template

Customer Name	
Workday Entity	Workday Limited (Registration number 521013) The Kings Building 152-155 Church Street Smithfield, Dublin 7, D07 A0TN
Call-Off Contract Effective Date	
Order Effective Date	
Total Subscription Fee	No Fee

Customer Contact Information	**Customer Support**
Contact Name	
Street Address City/Town, County, Post Code, Country	
Phone/Fax #	
Email (required)	

This document is only valid and binding on the parties when executed by both parties and is subject to the terms in the above-referenced Call-Off Contract and Addendum attached hereto. In the event of any conflict, the terms of this Order Form and Addendum will prevail over the terms of the Call-Off Contract.

IN WITNESS WHEREOF, this Order Form is entered into and becomes a binding part of the above-referenced Call-Off Contract as of the Order Effective Date.

© 2026, Workday Limited.

Customer	**Workday Limited** (Registration number 521013) The Kings Building 152-155 Church Street Smithfield, Dublin 7, D07 A0TN
Signature:	Signature
Name:	Name:
Title:	Title:
Date Signed:	Date Signed:

© 2026, Workday Limited.

Workday Customer Application Penetration Testing Addendum

This Workday Customer Application Penetration Testing Addendum applies to Workday's Customer Application Penetration Testing Program ("**Pentest Program**") and is further described at https://community.workday.com/articles/580479 ("**Testing Program Scope**"). Unless defined in the Addendum, capitalised terms used herein shall have the meaning given to them under the MSA which forms part of the Call-Off Contract or under the Testing Program Scope. In the event of any conflict, the terms of this Addendum will prevail over the terms of the Call-Off Contract.

1. Scope of Testing

Customer may conduct an application-level vulnerability assessment of a mutually agreed environment ("**Testing**") solely for Customer's internal business purposes to evaluate the security of the Workday Service. All Testing must be done in accordance with this Addendum and the Testing Program Scope. Any Testing deviations from this Addendum and the Testing Program Scope must be mutually agreed in writing. All Testing Reports and Testing results are Workday's Confidential Information. Workday may terminate the Pentest Program and this Addendum by providing at least ninety (90) days' prior notice which may be provided through the Workday Community site.

2. Customer's Responsibilities

a) Customer Testing will be conducted only by Customer's employees and contractors with the proper skill, training, and expertise necessary to accomplish their assigned tasks and conduct Testing in a competent and professional manner. Workday reserves the right to disqualify Customer's selection of any third-party tester at its sole discretion based on past or current deficiencies in the third party's security practices.

b) Upon Workday's request, Customer must immediately cease any Testing. Further, Customer must immediately cease any Testing and notify Workday if Testing is likely to result in exposure to any other party's Confidential Information.

c) Customer may not access, retrieve, transfer, download, or modify any data residing on Workday's servers that does not belong to Customer (excluding sample data provided by Workday for Customer's evaluation and testing purposes).

3. Testing

Workday does not guarantee that Testing will detect all security weaknesses, potential security problems, or potential breaches. Workday has no liability for any breach of the terms under this Addendum or any other agreement to the extent the breach results from Testing activities of Workday or Customer hereunder. Customer will defend, indemnify, and hold Workday harmless from and against any and all claims, judgments, costs, awards, expenses (including reasonable attorneys' fees), and liability of any kind arising out of (a) any claim that the Testing conducted in connection with this Addendum caused harm to, or infringed the rights of a third party and (b) any breach of the terms herein by Customer, its employees subcontractors, or any third-party tester.

© 2026, Workday Limited.