

Data Protection Impact Assessment – Workday ERP Solution

Document Name	Data Protection Impact Assessment – Workday ERP Solution
Author/Owner (name and job title)	Debra Holt, Programme Manager Gavin Aitken, Project Manager
Department/Team	PMO
Document Status (draft, published or superseded)	Draft
Version Number	V1.2
Release Date	05/05/2023
Approver (if applicable)	
Review Date	04/05/2025
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to the data protection impact assessment process. You should use this every time you want to implement or change a product or process. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting/using, why, where it will be stored and for how long, who will access it and why, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice, and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks to what you are proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If

that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The process

You should allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Step 1

- Complete DPIA screening assessment. If you conclude that you do not need to complete a DPIA then you must make a record of your decision.
- If you do need to complete a DPIA then start completing the paperwork and notify the IM Service. Depending on what you're doing, the DPIA might need to be reviewed by the DPIA forum. You need to ensure the paperwork is sufficiently detailed, accurate and thorough before the forum is able to review it. This particularly applies to your descriptions of the processing activities you are proposing and how any associated technology works alongside it.
-

Step 2

- The forum is likely to provide advice and recommendations. You should consider this advice. If you decide not to follow it, then you must document your reasons why. If you do follow it, then most actions will need to be completed before going live. For example, updating privacy information or refining access controls.
- The forum is able to escalate risks to our Data Protection Officer and/or Risk and Governance Board if it is not comfortable with the processing activity being suggested or wants sign-off on advice.

When you have completed the DPIA paperwork and any actions, accepting that you might need to revisit it, you should get sign-off from your IAO before your product or service goes live.

If there are residual risks that your IAO would like to discuss, they can contact dpo@ico.org.uk. That discussion can be escalated to our Data Protection Officer and/or Risk and Governance Board if required.

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your 'Screening Assessment - do I need to carry out a DPIA?' indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the [screening assessment](#) first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The [Information Management Service](#) is also available for further advice and support. Please keep in mind our [service standards](#) if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	ERP Solution
Project Manager:	Gavin Aitken
Information Asset Owner:	Director of Finance and Director of People Services
Controller(s)	ICO
Data processor(s)	Workday

1.2 [Describe your new service or process](#)

The implementation of the Workday fully integrated Enterprise Resource Planning (ERP) solution.

This solution will replace our existing Finance, Procurement, HR, Recruitment, Learning & Development and Payroll solutions providing a single solution, with a single set of data.

All data is currently held in multiple existing systems, namely:

- CiphR (HR)
- Capita (Payroll)
- i-Learn (L&D)
- Vacancy Filler (recruitment)
- Dynamics GP (finance)
- Purchase Management (procurement)
- Various spreadsheets

1.3 [Personal data inventory - explain what personal data is involved](#)

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
<p>HR staff records e.g., personal contact details, optional protected characteristics, salary and band level, pension details, and attendance records.</p> <p>L&D staff learning records</p>	<p>All ICO staff – permanent, temporary and secondees</p> <p>Former employees</p>	<p>ICO HR and Workforce Management staff for purposes of administrating the system.</p> <p>ICO employees will have access to add and amend personal details, or request change through HR.</p>	<p>None envisaged, as all ICO staff are UK based, so no overseas access or data transfers are expected.</p> <p>Data will be hosted in an Amazon Web Services (AWS) data centre based in Dublin, Europe</p>	<p>See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.</p>
<p>Third party contact details</p>	<p>Staff emergency contacts</p> <p>Referees (recruitment)</p>	<p>ICO HR and Workforce Management staff for purposes of administrating the system.</p>	<p>None envisaged, as all ICO staff are UK based, so no overseas access or data transfers are expected.</p> <p>Data will be hosted in an Amazon Web Services (AWS) data centre based in Dublin, Europe</p>	<p>See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.</p>

Financial information on payments to staff e.g. Salary and Expenses payments	All ICO staff – permanent, temporary and secondees Former employees	ICO Finance staff for purposes of administrating the system	No data transfer is expected as part of normal day-to-day use. Any specific data exports will be made to user OneDrive locations or Departmental Workgroup shares, based in the UK.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.
Supplier information for procurement of goods and services e.g. supplier name, address, email, telephone, banking details for payment	Suppliers of goods and services to the ICO	ICO staff with responsibility for the purchasing of goods and services on behalf of the organisation	No data transfer is expected as part of normal day-to-day use. Any specific data exports will be made to user OneDrive locations or Departmental Workgroup shares, based in the UK.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.
Data required to provide 3 rd party supplier system support e.g. staff name, email address, and contact number Role / system access level	All ICO staff – permanent, temporary and secondees	Workday for provision of system support only with authorisation from ICO system administrator	For the purposes of support data may be accessed from the USA, New Zealand, Australia, or Dublin. Follow the sun cover is provided 24 x 7, 365 days a year.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.
Special Category Data and data related to criminal convictions and offences.	All ICO staff – permanent, temporary and secondees Former employees	ICO staff will have access to enter and update their own personal data. HR staff will have access for business purposes.	No data transfer is expected as part of normal day-to-day use.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.

Banking transactions, Salaries, Expenses, Payments, Income and Refunds	All salaried staff. Staff claiming expenses. Customers and Suppliers. Registration fee payers. Any other income sources.	ICO Finance staff for purposes of administrating the system	International payments can be made via Bank to oversees staff.	Bank retains integration files between 30 and 120 days. After this period, the filenames are still visible however the contents are deleted.
Tax, National Insurance, Benefits and Deductions data	All ICO staff – permanent, temporary and secondees Former employees	ICO HR and Pensions staff for purposes of administrating the system.	No data transfer is expected as part of normal day-to-day use.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.
Pension contributions	All ICO staff – permanent, temporary and secondees Former employees	ICO HR and Pensions staff for purposes of administrating the system. ICO employees will have access to view personal details and request change through HR.	No data transfer is expected as part of normal day-to-day use.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply. Data will need to be retained until there are no surviving beneficiaries of the pension policy.
Electronic signature of contracts and letters	Job applicants, existing employees and Suppliers	ICO HR, Recruitment and Procurement staff for purposes of administrating the system.	No data transfer is expected as part of normal day-to-day use. If an employee or supplier is non-UK based they would still be required to electronically sign the document.	See our Retention and disposal policy Retention and disposal policy (ico.org.uk) the retention periods in this will apply.

1.4 [Identify a lawful basis for your processing](#)

A variety of categories of personal data will be processed for different purposes within the ERP solution. More detail available in [ROPA](#). The relevant lawful basis for processing are:

Article 6(1)(b) – contract

Article 6(1)(c) – legal obligation

Article 6(1)(e) – public task

Article 6(1)(f) – legitimate interests

Where special category data is processed the relevant processing conditions are:

Article 9(2)(b) – employment

Article 9(2)(g) – public interest

For special category and criminal offence data the relevant DPA 2018 Schedule 1 conditions are:

Schedule 1 part 1 paragraph 1 - employment

Schedule 1 part 2 Paragraph 6(2)(a) – statutory and government purposes

1.5 [Explain why it is necessary to process this personal data](#)

Processing is necessary as part of legitimate business operation for the management of employee HR records, disciplinary, training, appraisals, absence, leave, pay and benefits.

The ICO processes personal data in line with its own legitimate business operations

ICO will be an independent controller for such processing, the legal basis of which is legitimate interest and will consist of the following:

- (1) billing and account management
- (2) compensation (e.g., calculating employee remuneration)
- (3) internal reporting and modelling (e.g., forecasting, revenue, and capacity planning)
- (4) maintaining staff records
- (5) improving the core functionality of accessibility, data accuracy and timeliness
- (6) financial reporting and compliance with legal obligations

1.6 [Outline your approach to completing this DPIA](#)

The DPIA screening assessment has been completed, which indicated a full DPIA assessment is required, due to the processing of a significant volume of personal data including special category data.

We have consulted with colleagues from Finance, HR, and L&D along with the supplier to understand the privacy impact and any associated risks. An international transfer risk assessment is in the process of being undertaken, with our Commercial Legal colleagues. Cyber security has been consulted for a security assessment.

We will not be consulting with data subjects as the categories of data are already processed by the ICO within other systems which we will be replacing with Workday as a single centralised ERP solution. The processing will not include any automated decision making that will have a legal or similar detrimental effect on individuals.

2.0 Data flows

ERP software itself is a database of information and workflows that are meant to automate and quicken business processes such as authorisation approval, inventory management and accounting.

There is a business transaction source, a flow of information and approval stages with storage along the way, a result (payment, absence approval, purchase order etc) and an information lifecycle. Access control is via Role Based User Access (RBAC) and retention/deletion data schedules and automated processing are triggered at regular times.

There is information originating from ERP itself which also has a lifecycle that will be within the ERP approval and storage process. Information coming out of ERP includes payments, payroll, tax, national insurance and pension data going to banks, HMRC and MyCSP.

The following services are in scope.

Current System & location	Current Services	New Services Workday	Stakeholders	Categories of information	Migration
Ciphr (HR system) – cloud hosted	Absence management Organisation management	Absence management, Organisation management, Business process management, Performance management, Health and wellbeing management	All staff have access to: Update Personal information, Absence, Performance, Sick leave Managers have access to review and approve: Team absence, performance and sick leave HR has access to: organisation management, business process management,	Contact Payment Absence Performance Equal opportunities Sick leave	Excel data reports extracted from Ciphr. Data migrated via Workday workbooks (Excel) and transmitted via sftp.

			health and wellbeing management		
None	None	Talent Optimization: Feedback, Survey campaigns, Embedded analytics, Goal management, Performance management, Talent review, Succession planning, Career and development planning	All staff have access to: Feedback, goal management, development review, performance management and career development Talent team has access to: Maintain data Analysis and reporting Development review HR has access to: Succession data Manager has access to: Succession data Development review	Goals Performance	None
None	None	Workday Help: HR knowledge base Case management Service level reporting	All staff have access to: search for help and if necessary log cases HR has access to: Tracking and management of HR workload Reporting and analytics	Performance Attendance Grievance Health Whistleblowing	None
Capita (Payroll)	Production of payslips and notification of payments to HMRC and MyCSP. Calculations and checks still carried out by ICO.	Workday Payroll with link to HMRC for tax and NI contributions, and manual upload of pension contributions to MyCSP (payroll brought completely in-house)	All staff have access to: Payslips and P60 Payroll team has access to: Timesheets Absence Sickness	Banking details Tax coding Salary Taxation and NI Overtime, backpay, bought/sold leave Student loans, CCJs	Excel data reports extracted from Ciph. Data migrated via Workday workbooks (Excel) and transmitted via sftp.

			<p>Deductions Additional payments</p> <p>Finance has access to: Reports from MyCSP HMRC Gateway Audit</p> <p>MyCSP has access to: Payroll contribution data via file upload to secure portal</p>	<p>Sickness, absence, leave Health scheme Parking scheme Cycle to work scheme Childcare voucher scheme Pension contributions</p>	
i-Learn (Learning and Development) – cloud hosted	Booking, recording, and tracking of learning	Learning	<p>All staff have access to: Booking and undertaking learning Taking mandatory training</p> <p>L&D has access to: Assign learning Track learning Book learning in calendars</p>	Learning and development records	Learning content exported as SCORM files and uploaded into Workday; transmitted via sftp.
Vacancy Filler (Recruitment) – cloud hosted	Creation and tracking of vacancies / applicants	Recruitment	<p>Managers have access to: Review responses, conduct interviews and provide feedback</p> <p>HR has access to: create and publish job vacancies, track, review, shortlist, arrange interviews, provide feedback, make offers and undertake pre-employment checks. Book interview slots in calendars.</p>	<p>Contact information Application responses Employment history References Qualifications Interview scoring Feedback</p> <p>Protected characteristics, to ensure compliance with Equality Act 2010</p>	The Recruitment team will define a point at which new vacancies are entered into Workday. Existing vacancies will not be migrated.

Microsoft Dynamics GP (Finance) – on premises	Core financials	Accounting and finance, Revenue management, Financial reporting and consolidation, Financial planning, Project billing, Audit and internal controls	Finance has access to: post journals, maintain chart of accounts and cost centres, undertake budgeting and forecasting, review system audit, and approve transactions	Financial Budgets Transaction audits	Via Workday workbooks (Excel) and transmitted via sftp. Ongoing uploads of journals via EIB (Enterprise Interface Builder) directly into Workday.
None	Resource and capability modelling	Workforce Planning	HR Finance Management Team	Staff resources, Skills, Projects, Work load, Predicted demand, Locations, Costs and Salaries	None
Spreadsheets	Flexi record	Time Tracking	All employees have access to maintain their time tracking records Managers have access to approve time tracking records HR has access for reporting and analytics. Payroll has access to ensure correct salary payment and deductions	Staff attendance, absence and leave	Holiday, TOIL (Time of in Lieu) and banked leave balances transferred via HCM Workday workbooks (Excel) and transmitted via sftp. Flex leave balance added by individuals.
Spreadsheets	Expenses	Expenses	Employees have access to raise expense claims Managers have access to: Authorise expenses Finance has access to review and audit expense claims	Details of expense claim Personal bank details for payment	None

Spreadsheets	Payroll changes	Workday Payroll	<p>All staff.</p> <p>HR and Payroll teams have access to data for payroll preparation and queries.</p> <p>Finance will have access to approve payment and authorise submission.</p>	Personal information, tax (HMRC submissions) and pension (MyCSP submissions) and bank details	One-time copy of data from legacy systems via workbooks, transferred via sftp.
Spreadsheets	Staff loans and training costs	Finance	<p>All employees with outstanding loans and training costs</p> <p>Finance Payroll</p> <p>HR, Finance and Payroll teams will have access to data for recovery of any outstanding costs at end of employment.</p>	Personal information – name, address, contact details and bank details. Loan details – amount, repayment schedule and current outstanding amount.	Upload via EIB (Enterprise Interface Builder) directly into Workday.
Spreadsheets	Customers	Finance	All active customers Finance	Name Address Contact details Bank details	Via Workday workbooks (Excel) and transferred via sftp.
Spreadsheets	Suppliers	Finance	All active suppliers Finance Procurement	Name, address, bank details, VAT number, ICO data protection number	Via Workday workbooks (Excel) and transferred via sftp.
m-hance Purchase Management – on-premises	Purchase management	Procurement Inventory	<p>Employees have access to initiate purchase order requisitions.</p> <p>Managers have access to: Approve purchase requisitions and supplier</p>	Supplier details Payment Financial budgets Transaction audits	Via Workday workbooks (Excel) and transferred via sftp.

			<p>invoices, and review their budget.</p> <p>Finance has access to: review transactions and budgets, and report any variances</p>		
Spreadsheets	Asset management	Assets	<p>Procurement Finance Facilities IT</p> <p>have access to add and analyse assets</p>	Location, financial, acquisition date, term, and depreciation schedule	Via Workday workbooks (Excel) and transferred via sftp.
Spreadsheets	Contract management	Contract Management	<p>Procurement Legal Services Finance</p> <p>Have access to add and review contracts</p>	Supplier details, financial, and legal	Via Workday workbooks (Excel) and transferred via sftp.
MyCSP (Civil Service Pensions)	Currently handled by Capita	Access to MyCSP Connect portal for upload of payroll pension files	Payroll	<p>Personal details including:</p> <p>Name Age Sex NINO Salary Pension contribution</p>	None
HMRC (tax and NI)	Currently handled by Capita	Integration for Workday to submit/receive transactions to/from HMRC.	<p>Payroll Finance</p>	<p>Personal details including:</p> <p>Name Age Sex NINO Salary Tax code Tax paid Taxable benefits Allowances</p>	None

				Student loans, CCJs	
NatWest (banking)	Faster Payments	Integration for Workday to submit payments to the bank. New BACS facility for payments.	Finance has access to: Approve payments Check payments Audit	Supplier, customer and employee bank account information to process payments/refunds Value and type of transactions	Via Workday workbooks (Excel) and transmitted via sftp.
RBS (Corporate Credit Cards)	On line access	MasterCard Connect portal to provide statement download in cdf3 format for upload into Workday	Corporate credit card holders Finance	Corporate credit card details Card holder name Card number Contact and address Transaction details	None
Letters and Contracts	Signature approval of contracts and letters Employment offer letter Employment contract Supplier contract Letter of variation	Integration for Workday to submit documents to DocuSign for electronic signature.	HR Recruitment Procurement Job applicants Existing employees Suppliers	Personal or Supplier details including: Name Address Salary / value Terms / contract details	None

For further information please refer to the Workday website <https://www.workday.com/en-gb/homepage.html>

An overview of the data flows into and out of Workday is shown below.

MasterCard and MyCSP data flows are not automatic and require manual interaction to put/get data to/from the respective secure portals.



Data migration

Data transfer from legacy systems to Workday is done via secure file transfer protocol (SFTP) only. This is an approved and secure method of file transfer between the ICO and Workday, using public and private keys limited to a single user. ICO access to the SFTP server and the ability to transfer data is limited and controlled. Data transfer via email is not permitted. ICO provides data in workbooks via SFTP to Workday for validation and upload into the tenant builds, and Workday can return workbooks via SFTP requiring further amendment. Individual SFTP files can be manually deleted at any time by the ICO or Workday, and all SFTP data will be deleted by Workday 60 days after system go live. Data is stored and worked on in private Microsoft Teams channels and network workgroup shared folders. These have controlled access and will be deleted after go live.

During the workshops, data that needs to be migrated will be identified and tested. There will 3 data transfers:

1. Initial test migration to identify data sources, assist design and highlight areas of improvement;
2. Further improved migration to prepare system for user acceptance testing; and
3. Final migration for go live.

Historical data retention

Not all legacy data will be migrated into the ERP system, for example there may be more sickness detail than is required. Where historical information is required for legal or regulatory reasons, it will be retained and access controlled.

The following areas of historical data retention have been identified.

Finance (GP Dynamics) is still to be decided; the existing licence runs until 10 December 2023.

Historical Data Source	Services	Solution	Stakeholders	Location
Capita	Payroll, HMRC and MyCSP submissions, P11D and P60 forms	Read-only database to view historical data for 3 years to June 2026	HR and Payroll to have access for queries, reporting, SAR and FOI requests	On-premises
Ciphr	Human Resources Absence management Organisation management	Read-only access to current system for 12 months only to April 2024. Data dump (SQL) to be provided at a later date.	HR to have access for investigations, grievances, absence, queries, reporting, SAR and FOI requests	Read-only system is cloud hosted. SQL data dump will be held on-premises.
GP Dynamics	Finance and Purchase Management	To be decided before contract end December 2023v	Finance to have access for queries, reporting and FOI requests.	To be decided

Decommissioning

As part of the decommission phase, the legacy systems and data will be deleted. Thus any data not transferred to the ERP system will not be retained, other than data mentioned above.

Any servers and licensing not required will be deleted/cancelled.

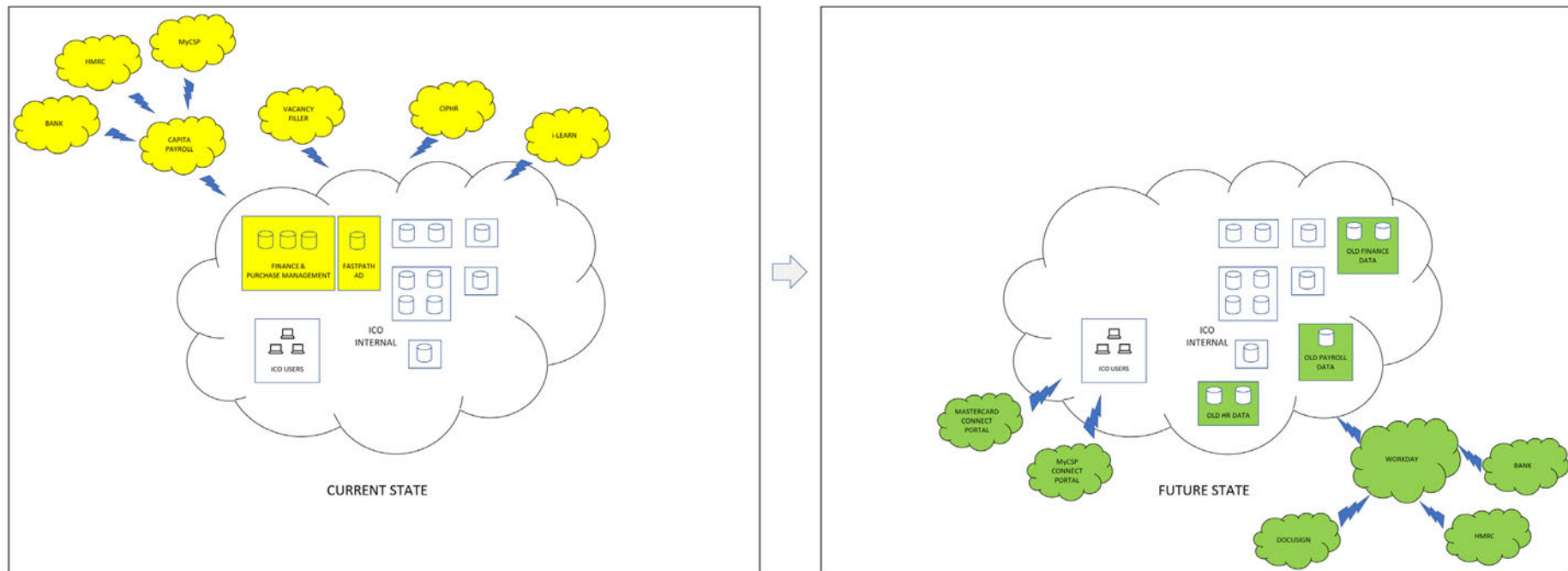
Contract end dates for legacy systems are noted below

Contract	Supplier	Expiry Date
Human Resources	Ciphr	03/05/2023
Payroll	Capita	30/06/2023
Learning & Development	Learning Pool	06/07/2023
Recruitment	Vacancy Filler	12/09/2023
Finance - <i>Fastpath AD subscription and support</i>	m-hance	29/09/2023
Finance - <i>Dynamics GP & Purchase Management</i>	m-hance	10/12/2023

Current and Future System Overview

High level overview of current systems on the left, with the systems to be decommissioned after go live denoted in the upper part of the diagram in yellow; namely Capita Payroll (and associated links or emails to the bank, HMRC and MyCSP), Vacancy Filler, CiphR, i-Learn, Finance GP Dynamics, Purchase Management and Fastpath AD.

On the right, the future state is shown, with the replacement systems in the lower part of the diagram highlighted in green. Here, Workday integrates with the bank and HMRC, and there is new access to secure portals for MyCSP and MasterCard for file sending from and uploading into Workday.

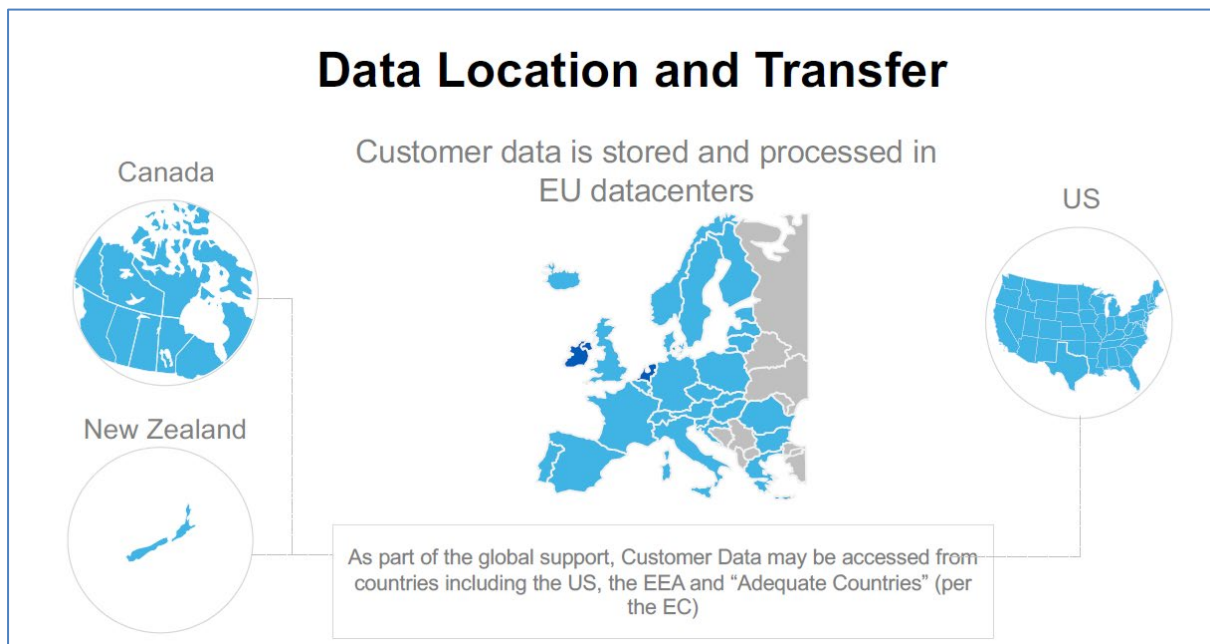


Data Location

There will be a separate tenant for each of the ICO test environments:

At go live there will be tenants for production, sandbox and preview. All other tenants and the STFP data will be deleted 60 days after go live.

- Production is the live system;
- Sandbox is for testing configuration, and this tenant is overwritten from Production every Friday; and
- Preview is for testing the twice-yearly product upgrades.



Products hosted in Workday's Co-Location Data Centres with Production in Dublin, Ireland (Digital Realty Trust) and Disaster Recovery in Amsterdam, Netherlands (Equinix):

- Core Financials
- Core HCM
- Talent Optimisation
- Cloud Connect for Third Party Payroll
- Workday Payroll
- Recruiting
- Learning
- Procurement
- Workday Help (Ticketing)
- Workday Help (Reporting)
- Time Tracking
- Expenses

Products hosted in Amazon Web Services Data Centres with Production in Dublin, Ireland (EU-West1) and Disaster Recovery in Frankfurt, Germany (EU-Central1):

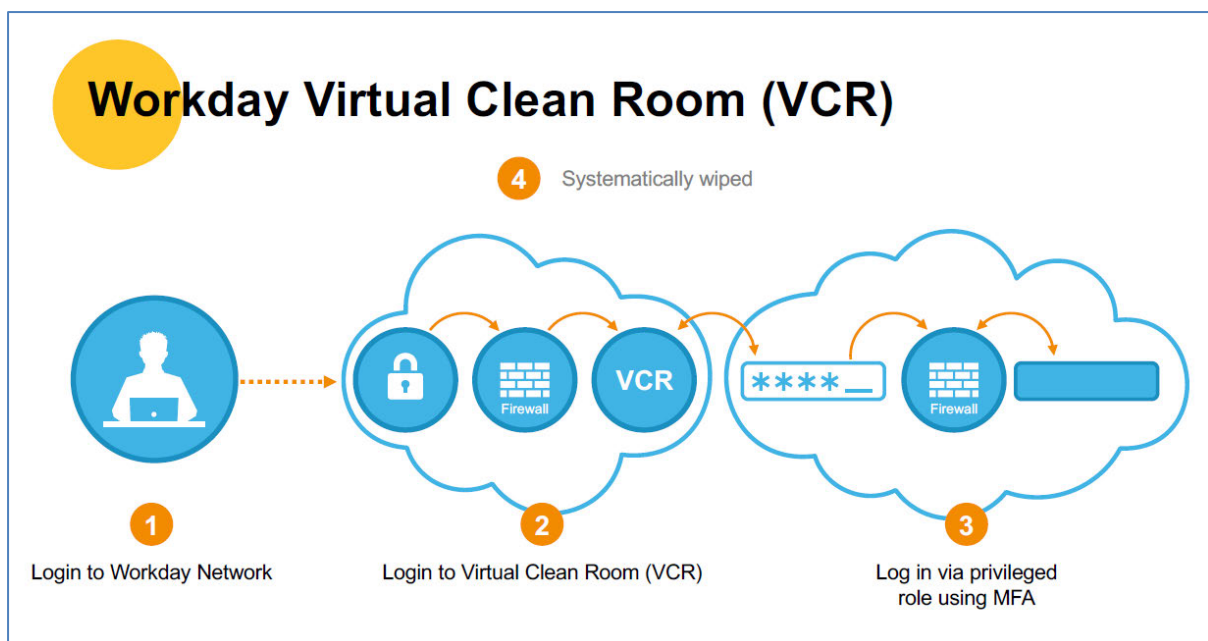
- Workday Adaptive Planning
- Workday Help (Knowledge-Base)
- Workday Media Cloud (video and audio content necessary for Learning)

Support and Remote access

Workday Support is available 24/7, 365 days a year (on a follow-the-sun basis) from the following primary support locations:

- California, United States of America
- Dublin, Ireland
- Auckland, New Zealand

Remote support, where a connection is necessary from outside the Californian and Dublin offices is provided via a Workday Virtual Clean Room (VCR). This is a virtual remote desktop connection valid only for that session, and the VCR session is terminated once the support engineer logs out. The VCR is reset back to its baseline configuration after 24 hours.



An overseas data transfer risk assessment was completed and approved in January 2022:

<https://edrm/sites/corp/im/CommsEng/layouts/15/DocIdRedir.aspx?ID=CORP-1602634889-1105>

A full audit trail is maintained, which allows the ICO to view access logs within our tenants.

List of 3rd party sub processors:

Name of Entity	Entity Country*	Entity Type	Applicable Service(s)
Amazon Web Services, Inc.	United States	Third-party hosting and service provider	Workday Adaptive Planning; Innovation Services (including Workday Help); Media Cloud;
Cloudflare, Inc.	United States	Third-party content delivery network	Media Cloud;
Zendesk, Inc.	United States	Third-party service provider (support software)	Workday Adaptive Planning;

*does not reflect where the data centres are located

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our [privacy notices](#)?

Yes No

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

N/A

3. If [consent](#) is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes No N/a

4. If legitimate interests is your lawful basis for processing have you completed a [legitimate interest assessment](#)?

Yes No N/a

If applicable, please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes No

6. How will you ensure the personal data remains accurate for the duration of your processing?

Individuals will have continuous access to check and update their own data once the system is operational.

As part of the system set up, or at agreed intervals e.g. annually, we can configure a task for colleagues to be required to check and update their personal details, thus maintaining data accuracy.

System administrators will use defined security group based access to view and/or update data in the system.

Data gathering and configuration for the system builds provide the opportunity to review, streamline and update information before finalising in Workday. Examples include cost centres, financial chart of accounts, supplier details and

formalisation of manual processes into structured and managed business workflow.

Data accuracy will be improved by:

- Moving to a single data entry model – entered once, used many times
- Improved security – role based access, supervisory access and audited
- Data validation – legacy data reviewed and validated during migration
- Mandatory fields and values – avoids missing or invalid data values

7. If the personal data isn't being obtained directly from the data subject what steps will you take to [verify accuracy](#)?

Data sanitisation and checks will be undertaken on the current systems by the relevant administrators. This has been highlighted as a recommended activity following discussion with several other ALBs who have adopted Workday ERP. This is then validated for accuracy or missing data.

There will be three data migration events; firstly to test the process and iron out data format issues, a second improved data migration to enable user testing of the system, and finally a third data migration will take place prior to go-live. The time between each migration allows correction of source data and improvements to the migration process to ensure the best possible accuracy. Audit checks will take place to ensure balances/record counts match between the old and new systems. Random spot checks can also be incorporated into the migration process and user acceptance testing to ensure confidence in the data transfer.

Individuals have recently had messages via the Intranet to check and update their contact details in MINFO.

Individuals will have continuous access to check and update their own personal data once the system is operational.

As part of the system set up, we can configure a task for colleagues to be required to update their personal details, thus further ensuring accuracy. This approach would allow only basic information to be initially migrated, leaving any sensitive data to be updated by the individual eg disability or ethnicity.

As part of the data extract, audit checks will be carried out eg to identify duplicates, or leavers still marked as current staff.

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes No

9. How will you ensure the personal data are deleted at the end of the retention period?

The system will have inbuilt retention schedules, which will be configured as part of the implementation and testing. System administrators (comprising Finance, HR and IT) will be responsible for setting and maintaining the retention schedules after the second iteration of data extracts. Using workflow, a business process can be defined to ensure periodic review.

For example, there is a purge supplier data function which can be run against inactive suppliers to remove any personal contact information.

As part of the data migration, cleansing, purging, and rationalisation exercises are taking place.

Retention and deletion will improve with the new service, as data from multiple sources will now be held once, centrally, and thus be easier to maintain than multiple systems.

All legacy data sources will be deleted as part of the decommissioning phase, except for any payroll, HR or financial historical data that must be retained for legal or regulatory reasons.

10. Will you need to update the [retention and disposal schedule](#)?

Yes No

Integrity and confidentiality

11. Where will the personal data be [stored](#)?

ICO systems: new Workday ERP tenant, cloud hosted in Dublin, Europe, with Disaster Recovery hosted in Amsterdam, Europe, and Frankfurt, Europe.

12. Are there appropriate [access controls](#) to keep the personal data secure?

Yes No

13. Have you contacted the [cyber security team](#) for a security assessment of your plans?

Yes No N/a

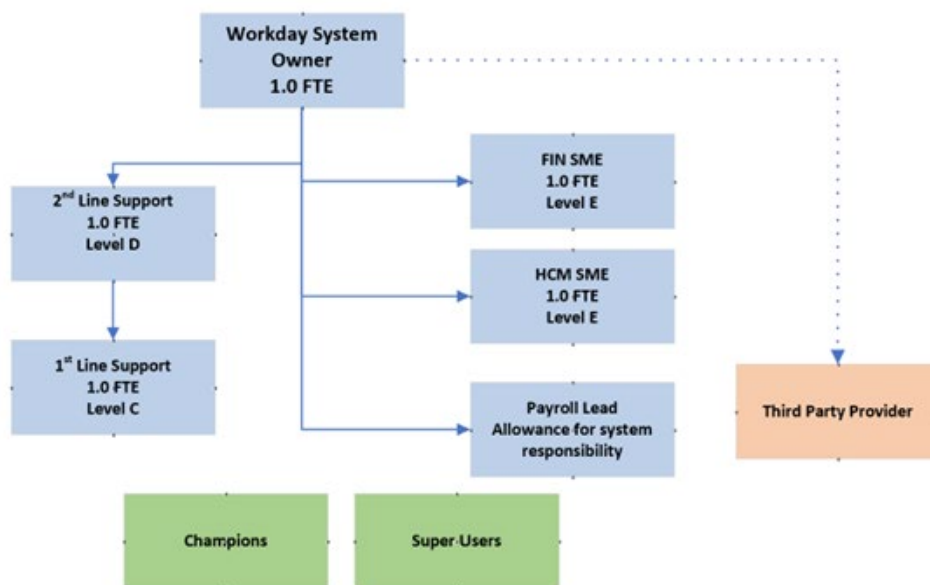
14. Please explain the policies, training, or other instructions you intend to put in place to enable staff to operate the new system or process securely.

A full training package will be delivered as part of the implementation. Policies and procedures will be reviewed internally as part of the implementation. There is an access control document.

Champions across all areas of the business will support day-to-day use within their teams. First and second line IT support will signpost any queries or requests as appropriate.

User guides and videos will be available via Iris for all processes to be undertaken by staff.

A hybrid support model will be put in place, led by a Product Owner, with third party support:



Accountability

15. Who will be the [Information Asset Owner](#) for this personal data?

Angela Donaldson (project visionary)
Sarah Lal (project visionary)
Paul Arnold (project sponsor)

16. Will you need to update our [Article 30 record of processing activities](#)?

Yes No

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes No N/a

Individual Rights

18. Is there a means of providing the data subjects with [access](#) to the personal data being processed?

Yes No

19. Can [inaccurate or incomplete](#) personal data be updated on receipt of a request from a data subject?

Yes No

20. Can we [restrict](#) our processing of the personal data on receipt of a request from a data subject?

Yes No

21. Can we [stop](#) our processing of the personal data on receipt of a request from a data subject?

Yes No N/a

22. Can we [extract and transmit](#) the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes No N/a

23. Can we [erase](#) the personal data on receipt of a request from the data subject?

Yes No

4.0 Risk assessment					
Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
1. Data being transferred outside UK without appropriate safeguards	Reduce	<p>During the course of normal support, Personal data will normally be transferred to</p> <ul style="list-style-type: none"> • California, United States of America • Dublin, Ireland; or • Auckland, New Zealand <p>The risks associated with potential transfers of personal data to these three jurisdictions were examined in a Transfer Risk Assessment (TRA). It was decided that international transfers to these jurisdictions could take place, under the implementation contract.</p> <p>It is agreed the proposed transfers can go ahead provided that the ICO implements procedures to ensure that data is only made accessible to Workday in the virtual clean room if either:</p> <ol style="list-style-type: none"> a. It will only be accessed by Workday Staff in either California, New Zealand, Ireland or another EU jurisdiction; or 	2	2	4 - Low

		b. The ICO's Commercial Legal Team has confirmed, in writing, that it may be accessed from another jurisdiction (other than those listed at point a, above).			
2. Data being transferred out of the system by Workday	Reduce	Workday Virtual Clean Room (VCR) will be used for support access; data cannot be exported from VCR. VCR content will be cleared down after 24 hours. ICO process to be implemented to ask from where support session is being made, to ensure access is only allowed from an approved country. System access is audited.	2	1	2 - Low
3. Lack of access control and insufficient restrictions to the data held in the ERP solution	Reduce	<p>Role based access control (RBAC) will be implemented during system configuration and testing to ensure segregation of duties, access to only relevant information, and ability to view and/or edit data, depending on role. Authentication will be through Azure Single Sign On and accounts kept in sync between Workday and Active Directory.</p> <p>Ongoing management of RBAC to be undertaken and periodically reviewed by internal support teams once they are established (system administrators for Finance and People Services). User access will be automatically disabled and synchronised with Active Directory once their leave date is reached within Workday.</p>	4	1	4 - low

4. Data loss during an import	Reduce	<p>The backup of legacy systems is unaffected and not covered by this DPIA. Workday manages backups of its systems, with disaster recovery described in section 2.0</p> <p>During the migration, data is transferred manually via sftp, ensuring source and destination file sizes match. The source data is unaffected.</p> <p>The import process runs a series of checks and any errors are highlighted for rework. Checks and balances will be run to ensure data matches eg number of employees, finance opening balances, etc.</p>	4	1	4 – low
5. Personal data is kept for longer than required	Reduce	<p>In built functionality to manage data retention/deletion will be used, to be configured with multi-workstream delivery team. System admins will be able to review and maintain. Business process 'workflow' tasks can be configured to automatically ensure review after agreed time periods.</p> <p>System audit log should confirm this is happening.</p>	3	1	3 – low
6. Use of ERP outside the organisation	Reduce	<p>Any external access will be controlled and managed by ICO system administrators. Access can only be made from an ICO managed device.</p> <p>Third party access will need prior approval and will be via a Workday and ICO approved mechanism.</p>	4	1	4 – low

		Workday Virtual Clean Room (VCR) will be used for Workday support access; data cannot be exported from VCR. VCR content will be cleared down after 24 hours. ICO process to be implemented to ask from where support session is being made, to ensure access is only allowed from an approved country. System access is audited.			
7. Workday suffers from a cyber-attack	Reduce	A Supplier Risk Assessment has confirmed Workday meets and exceeds our security requirements, and we have confidence in the security of the SaaS offering. Workday has a separate backup which is hosted in a different location, thus reducing the impact of any loss of data or access.	4	1	4 - low
8. Unable to handle subject access requests to search the database	Reduce	ERP solution provides consolidated single source of data, which provides more detailed and accurate searching and reporting function.	4	1	4 - low
9. Failing to comply with data processing regulations re: missing or inaccurate personal information	Reduce	Managed by user access control. Individuals will have access to and be able to check and amend their own data. There is a full system audit trail. Users will be able to request HR to change any information which they are unable to change.	4	1	4 - low

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is [here](#). Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	Date and project stage	Project Team Response
1.	<p>Section 1.4 – whilst the ICO will process the various categories of personal data to be migrated to ERP under different lawful basis, the DPIA can focus on our lawful basis for using Workday ERP as the method for this processing. Majority view was that legitimate interests is the most appropriate. Recommendation is for this section to be updated to remove other Article 6 lawful basis.</p> <p>We have however raised an advice request with Policy colleagues for clarity so section may need to be updated again.</p>	14/03/2022 - planning	<p>28/03/2022 Reject - policy advice received and section 1.4 should remain as is with multiple lawful basis listed.</p> <p>https://edrm/sites/corp/im/CommsEng/_layouts/15/DocIdRedir.aspx?ID=CORP-38861085-5</p>
2.	<p>Section 2.0 (data flow) –</p> <p>Please see email for general feedback on this section.</p>	14/03/2022 - planning	<p>28/03/2022 - removed architecture diagrams. Added section covering historical data retention.</p> <p>13/06/2022 – added section for Data migration and overview diagram showing current and future system overview.</p>

	The consensus view was that architecture diagrams aren't helpful in explaining the data flow so could be removed. Also some explanation is required about what is happening with data not migrated into ERP and the DPIA needs to be clear about how this data will be reviewed to see if ICO still needs to retain it.		
3.	<p>Section 3.0 Q5-7 (Accuracy) –</p> <p>More detail is needed to explain how the accuracy of personal data within ERP is maintained.</p> <p>It is clear that some elements can be maintained by prompting staff to update their own info but there are numerous areas that will require some ownership over data and individuals appointed to keep records accurate and this needs to be detailed. A few examples would be supplier contact details and HR information where it isn't appropriate for the individual to have access to amend.</p>	14/03/2022 - planning	21/06/2022 – updated Q5-7
4.	Section 3.0 Q4 - Finalise legitimate interest assessment.	14/03/2022 - planning	Reject - No longer required 16/2/2023
5.	Section 3.0 Q8 -10 (Retention and deletion) –	14/03/2022 - planning	21/06/2022 – updated Q8-10 18/01/2023 – updated Q9

	As part of the migration and implementation a clear process is required that ensures suitable retention periods are assigned to all data migrated along with a process for reviewing disposal decisions. Any automated deletion that is established in ERP needs to be approved by the relevant Information Asset Owners.		
6.	Section 3.0 Q21 and 23 – reconsider responses for these two questions. Answer shouldn't be N/A and you can't tick both Yes and No.	14/03/2022 - planning	28/03/2022 – Q21 and Q23 responses amended to Yes
7.	Section 4.0 (risk assessment) – Risk 1 - More information is required about the appropriate safeguards in place for the transfer of data to the USA to achieve the risk score that is currently reflected. This needs to be confirmed with the supplier as they still mention privacy shield on their website which is no longer valid.	14/03/2022 - planning	21/06/2022 – Updated response with reference to the Transfer Risk Assessment conducted by TLT and confirmation from the ICO's Commercial Legal Team
8.	Section 4.0 (risk assessment) Risk 2 – the risk description needs reconsidering. From the mitigation it seems the risk is really Workday exporting ICO data and doing something more with it rather than them being able to access it for	14/03/2022 - planning	21/06/2022 – Renamed risk description to represent risk of data being transferred out of the system by Workday. Mitigation to Risk 2 also addresses access from outside the UK.

	<p>support purposes which is to be expected.</p> <p>There also seems to be a risk of Workday accessing ICO data from a country that hasn't been approved. Clarity is required about which countries are approved and these should be documented in the DPIA.</p>		
9.	<p>Section 4.0 (risk assessment)</p> <p>Risk 3 (RBAC) – periodic reviews by system admins need to be scheduled and audited so there is assurance that these are taking place.</p>	14/03/2022 - planning	21/06/2022 – Updated to add ongoing management of RBAC by system administrators.
10.	<p>Section 4.0 (risk assessment)</p> <p>Risk 4 - More detail is required to provide assurance that this risk is mitigated. For example what is your backup process, where are backups stored and how do we identify whether data has or hasn't been migrated successfully.</p>	14/03/2022 - planning	21/06/2022 – Updated to add further details.
11.	<p>Section 4.0 (risk assessment)</p> <p>Risk 5 – the risk description needs reconsidering as the risk isn't clear. Recommend 'Personal data is kept for longer than required'.</p> <p>Periodic review by system admins is required to ensure disposal is</p>	14/03/2022 - planning	21/06/2022 – Updated to add further details.

	happening as planned. This should be scheduled as part of implementation and audited post implementation.		
12.	Section 4.0 (risk assessment) Risk 7 - consider rewording risk description to Workday suffers from a cyber-attack. Further mitigation required.	14/03/2022 - planning	17/01/2023 – Updated to add further details.
13.	Data flows 2.0 – The data flow could benefit from further clarity around the direction of data moving between the various integrations. Recommend direction of travel for data be added i.e. what is moving into Workday and what is moving out. There are a number of recipients of data involved (Banks, HMRC, MYCSP) which aren't identified in data inventory and need to be included so there is clarity on what categories of data are going where.	16/02/2023 - planning	04/05/2023 – Added data flow diagram in Section 2.0 showing source, destination and direction of data flow. Added other data recipients to data inventory in Section 1.3. Added electronic document signature to 1.3 and 2.0
14	Data flows 2.0: What is the significance of Canada for data transfers / support? This is mentioned in the diagram on page 21 but it's unclear from additional	16/02/2023 - planning	03/05/2023 - Workday in Canada provides product support, as part of 24/7 follow-the-sun availability. Access from this location would be by the normal Workday VCR process.

	content about overseas transfers elsewhere whether data will actually be transferred to Canada.		
15.	<p>Workday will hold some of our most sensitive data and offers the potential for ICO to undertake a wide variety of data processing activities and there is a risk that the scale and scope of our processing activities increases over time.</p> <p>Steps should be taken to make the teams using Workday aware of the current scope of this DPIA. Where there is a desire to undertake new processing activities using Workday that have not been included within the current scope of this DPIA (See section 2.0) or where additional personal data will be processed using Workday beyond what is detailed in the data inventory (see 1.3) then steps must be taken to update the DPIA and assess risks to data subjects.</p>	16/02/2023	04/05/2023 - Any new processing or fields of data will need to signed off by the System Administrator and Product Owner, following approval by the Director of the relevant business area.
16.	In the overseas transfer section of your data flows there is the statement " <i>None envisaged, as all ICO staff are UK based, so no overseas access or data transfers are expected</i> "	16/02/2023	03/05/2023 - Existing Security Policy and Conditional Access rules apply. ICO staff based outside the UK or working abroad will be subject to existing security controls and restrictions from which countries ICO systems can be accessed.

	Can you clarify this statement; are we putting procedures in place so staff aren't able to access these systems if working from abroad?		
17.	It would be beneficial to include analytics in your data inventory so it's clear what analytics are available and what colleagues will / won't have access to this data. It's not clear from the DPIA whether analytics data is anonymised in Workday so further clarity around this would be useful to understand any risks.	16/02/2023	04/05/2023 - Analytics are run through the separate Workday Workforce Adaptive Planning instance, which has restricted access to a small number of users. Data produced can be anonymised, if necessary.
18.	Data migration (section 2.0) 60 days is identified as the period for keeping workbooks for SFTP data transfer. This seems a relatively short period of time to retain. Is there a risk that we're deleting too soon? Risk 4 - mentions backups won't be affected but some services are being shut down, are you sure we have sufficient backups in case of any issues post go live.	16/02/2023	03/05/2023 - This data deletion is for transitory data only, and includes the three phases of data migration; foundation, End-to-end and Gold (final). The original data is retained within our legacy systems. Access to core HR, Finance and Payroll data will be retained to ensure we have access to historical data for FOI, SAR or other requests. The hosting and access method may change, however the data will be accessible for as long as required.
19.	As there is automated retention and disposal with Workday this must be used and our understanding is that system admins will be responsible for	16/02/2023	03/05/2023 – As part of the internal Support Team build and development, product specific training will be provided by Workday covering systems administration areas.

	ensuring appropriate review and disposal of personal data in Workday. Appropriate training to systems admins should be provided and periodic audits should take place to ensure this is happening.		
--	--	--	--

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Update privacy notice	Go Live	Information Management team	12/05/2023
Implement access controls	20/03/2023	Project Team	20/03/2023
Update Article 30 record of processing activity	Go live	Information Management team	12/05/2023
ICO process to be implemented to ask from where support session is being made	20/03/2023	Project Team	20/03/2023
Implement retention and deletion rules	20/03/2023	Project Team	20/03/2023

Overseas transfer risk assessment to be completed	Before go live	Project team	January 2022
Disposal of workbooks for SFTP transfers once they are no longer required.	30/06/2023	Project team	

7.0 Expected residual risk and sign off


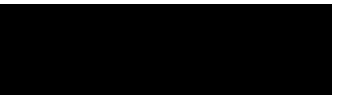
Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all your mitigation measures and complete all actions.

It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g., red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

The residual risk is low because of the mitigation controls put in place.

Administrators will be informed that they need to update the DPIA if there is new processing or a change in the processing of personal data within Workday.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
 Angela Donaldson – Director of Finance	11/05/2023	Delivered
 Sarah Lal - Director of People Services	11/05/2023	Delivered

8.0 [Change history](#)

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service, or process)

Version	Date	Author	Change description
V0.1	06/12/2021	Deb Holt / Gavin Aitken	First Draft
V0.1	14/03/2022	Steven Johnston	DPIA forum recommendations added to 5.0.
V1.0	18/01/2023	Deb Holt / Gavin Aitken	Recommendations addressed and document updated
V1.1	17/02/2023	Steven Johnston	Additional recommendations from DPIA forum added to 5.0
V1.2	05/05/2023	Gavin Aitken	Completed the recommendations from DPIA forum in 5.0

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, banning by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).

Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).
---------------	---

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (e.g., does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability \ Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)

Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)
-----------------	--------------	--------------	--------------	--------------	--------------

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted, and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions

- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from an unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g., fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behaviour
- Non-compliance with DP principles