Privacy Impact Assessment for

The Knowledge Portal (TKP)

October 29, 2025

Contact Point
Elizabeth Edenfield
Program Manager, USA Learning
Human Resources Solutions

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

Abstract

The Knowledge Portal (TKP) is a government-wide, web-based learning and development environment operated by the U.S. Office of Personnel Management (OPM) Human Resources Solutions (HRS) through the USA Learning program office. TKP serves as the enterprise system for delivering online learning, onboarding, and professional development programs supporting OPM and federal agencies across government.

The system consolidates multiple OPM HRS managed learning applications within a unified FedRAMP authorized boundary, providing government-wide access to e-learning and workforce development resources. TKP supports OPM's mission to strengthen the federal workforce through its six integrated, secure web applications that deliver mandatory, role-based, developmental and compliance training to OPM employees, and federal HR specialists.

TKP collects and maintains personally identifiable information (PII) necessary to administer training activities, such as usernames, government email addresses, agency/organizational affiliations, and course participation records. All applications within TKP's boundary employ standardized privacy and security controls, including Phishing Resistant Multi-Factor Authentication, encryption in transit and at rest, audit logging, and role-based access restrictions.

This Privacy Impact Assessment (PIA) is being updated and renewed because TKP continues to collect, maintain, and disseminate PII from federal employees and contractors in support of workforce training and development.

Overview

TKP serves as a shared service environment that integrates multiple learning applications supporting OPM's internal training requirements and government-wide federal workforce development initiatives. The applications are developed to comply with e-Learning standards while providing OPM with

a comprehensive and partitioned LMS footprint and delivering a variety of training content.

The Knowledge Portal operates under a single FedRAMP authorized boundary with standardized security protocols, authentication, and data management across six applications:

1) **Registrations.GoLearn** – Secure registration and access point for the OPM Retirement Services Benefits Officers Development Office (BODO) training program. Federal benefits officers and HR practitioners register for and complete specialized courses that build their expertise in administering federal employee retirement and benefits programs.
2) **Learning Connection** – Internal OPM Learning Management System (LMS) used to deliver mandatory and compliance training to OPM employees.
3) **USA Performance (USAP) Training** – USAP LMS used to assist with the onboarding and training of agency customers and administrators responsible for managing performance management processes at their agency.
4) **USA Staffing LMS** – USAS LMS used to deliver course content and assist with the onboarding and training of agency customers and administrators responsible for hiring and onboarding processes at their agency.
5) **USA Staffing (USAS) LCMS** – USAS Learning Content Management System (LCMS) used to create, curate, and maintain official USA Staffing training materials.
6) **USALearning Website** – Public facing website for the HRS Assisted Acquisition team and serves as an information access point for both prospective and current assisted acquisition customers.

Together, the above applications form TKP, sharing a common infrastructure and access controls. USA Learning is the official learning and development office for the United States Federal Government and supports the development of the Federal workforce by supporting agency missions of

quality e-Learning products, information, and services. The purpose of TKP is to allow OPM program offices to create, track, manage and distribute learning materials of any kind, on-site at an agency or virtually in support of the OPM and USA Learning missions.

The applications within TKP are contractor-owned and operated, Commercial Off-the-Shelf products that are managed by contractors. OPM program office retain full rights and ownership to their respective data within TKP's environment. They are all web-based applications using two major components – application/web servers and database servers.

USA Learning support and training services leverage the authority of the Economy Act (31 U.S.C. § 1535), Revolving Fund (5 U.S.C. § 1304(e)), and Training Program Assistance (5 U.S.C. § 4116). TKP allows application users to access their personal learning history, course catalogs, training progress, request training electronically, and launch/complete web-based training.

OPM's Learning Connection application within TKP also supports OPM in accomplishing federal reporting requirements to submit training records to the Enterprise Human Resources Integration (EHRI) monthly.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

- 5 U.S.C. Chapter 41 – Training.
- 5 CRF Part 410, Training.
- 5 CRF Part 412, Supervisory, Management, and Executive Development.
- OPM Guide to Human Resources Reporting.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

OPM/GOVT-1, General Personnel Records (77 FR 73694, 87 FR 5874, 88 FR 56058), available at www.opm.gov/privacy.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes: GRS 2.6, item 030, Individual employee training records.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not Applicable

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The applications may contain PII obtained by customer agencies.

The following groups of individuals access TKP for the following reasons:

- All OPM employees access TKP to complete mandatory trainings and may also use it to complete optional trainings.
- Federal staff across the government access TKP to complete OPM provided trainings. For example, OPM's Retirement Serviced Benefits Officers Development Office (BODO) provides federal benefits officers and HR practitioners specialized courses on topics that range from coverage determinations to offset computations to processing retirement applications that build their expertise.
- Additional OPM employees and/or contractors access TKP to develop and lead trainings hosted by OPM, manage the system, provide technical support to other employees, and validate whether people are completing their required courses.

TKP applications data collected may include employee information, such as full name, government email address, job title, pay plan, supervisory status, training assignments, registration details, course completions, and organization information, such as agency/organization name, address, description, and other associated information. The exact information collected, used, disseminated and maintained is determined by the OPM program offices responsible for the individual application.

2.2. What are the sources of the information and how is the information collected for the project?

The applications collect information directly from the individual employees via self-registration or the individual's employer through a web-based interface or completion of a registration action.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4. Discuss how accuracy of the data is ensured.

As data are collected within TKP, accuracy is maintained through a combination of system design controls, field-level validation, and user confirmation mechanisms.

Each of the six applications enforces structures data-entry parameters and restricted value sets to reduce errors. TKP invites users to validate their personal and organizational information. Administrative interfaces and integrations incorporate automated data-integrity checks.

OPM-HRS and program office administrators are responsible for verifying the accuracy of user and training data within their respective applications. Users are reminded that they must provide complete and accurate information. For example, users selecting an employing agency or office must choose from standardized lists.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in the system is not accurate, or that the information is incomplete, resulting in a user account profile that does not reflect the training record of an individual.

Mitigation: This risk is not mitigated directly by the system. However, since all individuals are required to review their profile information before submitting it to OPM, it is assumed to be accurate when coming from the individual. Additionally, both the individuals and the agency LMS administrators have the ability to review and update any inaccurate information by contacting the related agency's LMS administrator. Additionally, customer agency representatives verify the employee's information before it is uploaded into the system.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The purpose of the USA Learning Program Office is to deliver training for various federal agencies via an online interface. TKP applications are developed to comply with e-Learning standards and use the information collected to provide online training courses and curricula to Federal agencies to satisfy the government required e-Training initiatives.

The information collected in OPM's Learning Connection specifically is sent by the vendor to OPM's EHRI monthly.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

The system uses internal tools only to search and query features and enable OPM and customer agencies to run reports. The system does not use any other tools, programs, or other technology to conduct electronic searches,

queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

OPM Program Office employees, contractors that manage the applications within TKP, and officials designated by the program office have access to the system applications as assigned according to their roles and responsibilities. No other OPM offices have direct access to the system, although the EHRI employees have access to the information sent monthly.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unintentional disclosure of PII to unauthorized individuals or entities while data is in transit between the system and the customer agency or the EHRI.

Mitigation: This risk is mitigated using secure, encrypted connections, documented in Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU), as well as through providing users with security and privacy awareness training.

Privacy Risk: There is a risk that an unauthorized person may access the information in the system or that an authorized person may access the information in the system for an unauthorized purpose.

Mitigation: This risk is mitigated using role-based access controls, unique user IDs, phishing resistant multi-factor authentication, and audit systems.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Each program office provides a Privacy Act statement to its application users, which notifies the individual about the authority to collect the information requested, the purposes for which it will be used, other routine

uses of the information, and the consequences of declining to provide the information. OPM provides guidance to the program offices regarding the statement but does not review the content. The program office determines where and how the Privacy Act statement is displayed on their view of each LMS. In addition to the Privacy Act statements, this PIA and the SORN referenced in Section 1.4 also provide notice to the individual users.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals are informed through Privacy Act statements that providing information is voluntary but that failure to provide the information will result in access restrictions to the applications. The individual does not have the opportunity to consent to specific uses of the information.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive notice concerning why their information is being collected and what it will be used for.

Mitigation: This risk is mitigated by the program office providing a Privacy Act statement to their individual users. The statement is typically displayed on the LMS homepage.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

GRS 2.6: Employee Training Records. Records are retained consistent with relevant OPM and NARA record schedules and policies. Retention allows tracking of long-term learning trends and meet federal reporting, audit, and compliance obligations.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the records in the system will be retained for longer than is necessary to meet the business need for which they were collected.

Mitigation: The USA Learning Program Office is working to mitigate this risk by developing guidance on records reviews. Guidance will include information on program office record reviews by system administrators to identify outdated, redundant, or obsolete information that no longer serves a valid business purpose. Automated and/or manual workflows to delete outdated data are in place in accordance with data retention policies.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. External Sharing: De-identified, aggregated training may be shared with OMB or relevant oversight bodies. Individual-level data is retained within OPM unless required by law.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Sharing aligns with existing routine uses under OPM SORN GOVT-1, General Personnel Records.

6.3. Does the project place limitations on re-dissemination?

No. There are no specific limitations placed on re-dissemination of the information in the system. Program offices who have access to the information are governed by their respective ISAs, MOUs, and contracts, as well as by the SORN referenced in Section 1.4.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The applications include audit logs and system administrators can create an audit report to track information access.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information in the system will be shared for a purpose other than that for which it was collected.

Mitigation: This risk is mitigated by encrypting the data encryption, ISAs, MOUs, and internal disclosure review procedures. Disclosure review procedures will be available to all elevated access users with and outline the need to verify legal authority for disclosure, ensuring that only the minimum necessary data is shared, and ensuring that appropriate safeguards are in place.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

End users can access their training history, profile, and learning progress through the learner dashboard. Individuals can also request access to their records by following the "record access procedure" described in OPM/GOVT-1.

Individuals requesting access must comply with the OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

End users completing a particular OPM assigned training can contact the program office that manages the training if incorrect information is found in an application. End users can also request amendment of their records by following the "contesting record procedure" described in OPM/GOVT-1.

7.3. How does the project notify individuals about the procedures for correcting their information?

Instructions on how to report or request record corrections are provided in application help documentation, through the user support center, applicable SORN, and through this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individual users will not understand that they can access and correct their training records and correct any erroneous information.

Mitigation: This risk is mitigated by providing users with information about how to access and amend their records. If users find inaccurate training information, they can contact their agency-based LMS administrator(s). The administrator can research and remediate incorrect information. In addition, individuals may follow the procedures for amending records outlined in the OPM/GOVT 1 SORN.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

TKP employs role-based access controls, monitoring, and audits. USA Learning also ensures that the practices stated in this PIA are followed by leveraging training, policies, the OPM Information Technologies Rules of Behavior requirements, and auditing and accounting.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Federal government personnel and contractors are required to take annual Security and Privacy Awareness training.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Each program office has a designated Technical Point of Contact who follows agency guidance to grant appropriate access to individuals at their respective program office.

Contractors that have access to the system are determined internally based on customer requirements, skill level, and resource availability.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The USA Learning program office enters into Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU) based on the needs of the OPM program offices and their applications. These MOUs and ISAs are used to establish policies and procedures related to the description and use of information and to designate points of contact in the program offices. MOUs and ISAs are valid for 3 years unless changes are required. These documents are routinely reviewed by the OPM Office of the Chief Information Officer and USA Learning Program Office staff as part of annual assessments of the system. If a change is required, both parties review and sign the updated documents.

Responsible Officials

Elizabeth Edenfield
Program Manager, USA Learning
Human Resources Solutions

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy