Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 363
System Name: GSA Online University (GSAOLU)
CPO Approval Date: 4/6/2022
PIA Expiration Date: 4/5/2025

Information System Security Manager (ISSM) Approval

Richard Banach

System Owner/Program Manager Approval

Monica Shackelford

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA Online University (GSAOLU)

B: System, application, or project includes information about:
OLU contains information about GSA Employees and Contractors. OLU also contains a limited information about Federal Employees and Contractors outside GSA (i.e. those who do not have a GSA network account).

C: For the categories listed above, how many records are there for each?
OLU contains 1.3 million training course records about unique federal employees and contractors as of 2022.

D: System, application, or project includes these data elements:
OLU contains Individual Name, Contact Information, and User Information

Overview:

GSA Online University is a SaaS learning management solution utilized for the administration, documentation, tracking, reporting and delivery of e-learning for GSA. GSA OLU supports required learning for all of GSA's estimated 12,000 employees. An estimated 5,000 contractors also utilize the system to complete mandatory training.

GSA OLU supports GSA Office of Human Resource Management (OHRM) needs and their stakeholder's learning requirements by providing an enterprise-wide system to manage online training, instructor-led training, individual development plans, and competency management.

GSA OLU also supports an external client base. This provides online training to other federal agencies, their employees and contractors, and is external to GSA. The GSA OLU provides standard or required training on the use of products and services.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 are the authorities for maintaining personnel information.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
SORNs GSA/Agency-1 and OPM-GOVT -1 covering GSAs personnel and training records.

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
1. Title: GRS 02.6/010 Non-Mission Employee Training Program Records. Description: Non-mission employee training program records. Records about planning, assessing, managing, and evaluating an agency's training program: plans, reports, and program evaluations, organizational and occupational needs assessments, employee skills assessments, employee training statistics, notices about training opportunities, schedules, or courses, mandatory training tracking and reporting files, logistics and coordination documents, Authorization, Agreement, and Certification of Training (SF-182) and similar records, registration forms, employee attendance records, syllabi, presentations, instructor guides, handbooks, and lesson plans, reference and working files on course content, other course materials, such as presentations and videos, student, class, or instructor evaluations. NOTE: Financial records related to purchase of training or travel for training are scheduled under GRS 1.1, item 010. Exclusion: This item does not cover ethics-related training. Ethics training is scheduled by GRS 2.6, item 020. Retention Instructions: Temporary. Destroy when 3 years old or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use. Legal Authority: DAA-GRS-2016-0014-0001 (GRS 02.6/010) 2. Title: GRS 02.6/020 Ethics Training Records. Description: Records include but are not limited to: administration of new employee ethics orientations, annual, and other types of ethics training, agency annual written plans, notices about training requirements and course offerings. Retention Instructions: Temporary. Destroy when 6 years old or

when superseded whichever is later, but longer retention is authorized if required for business use. Legal Authority: DAA-GRS-2016-0014-0002 (GRS 02.6/020) In addition, the following systems information resides in the OLU system that is used to add to the actual records in the form of directories, or other profile information of the employee or contractor. That information will be updated, managed, reported, and serve as content for system upgrades or conversions. The following record items cover use of that PII: 3. Title: GRS 02.6/030 Individual Employee Training Records. Description: Records documenting training required by all or most Federal agencies, such as information system security and anti-harassment training, and training to develop job skills. Records may include: completion certificates or verification documents for mandatory training required of all Federal employees or specific groups of employees (e.g., supervisors, contractors), Individual Development Plans (IDPs), mentoring or coaching agreements. Exclusion: Academic transcripts, professional licenses, civil service exams, or documentation of mission-related training are not covered by this item." Retention Instructions: Temporary. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use. Legal Authority: DAA-GRS-2016-0014-0003 (GRS 02.6/030) 4. Title: GRS 04.2/130 Personally Identifiable Information Extracts. Description: System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information. Legal citation: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify." Retention Instructions: Temporary. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate. Legal Authority: DAA-GRS-2013-0007-0012 (GRS 04.2/130) 5. Title: GRS 04.2/140 Personally Identifiable Information Extract Logs. Description: Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date. Retention Instructions: Temporary. Destroy when business use ceases. Legal Authority: DAA-GRS-2013-0007-0013 (GRS 04.2/140)

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.
A Privacy Banner is provided prior to the collection or sharing of personal information. Notice is also provided through SORNs GSA/Agency-1 and OPM-GOVT-1 - General Personnel Records, as well as this PIA, posted on www.gsa.gov/pia.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
OLU contains User Principal Name is used for internal record identification, Name for display and reporting purposes, Email address for SecureAuth and MAX.gov SSO login.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
OLU has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, along with system and information integrity.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.

OLU does not monitor GSA employees and contractors. OLU is used for training purposes only.

3.5 What kinds of report(s) can be produced on individuals?
OLU can be used for reporting on courses taken by the individual.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
OLU does not necessarily contain PII data.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Federal Agencies

4.2How: If so, how will GSA share the information?
OLU Provides information for the transmission of GSA employees training records to OPM's Enterprise Human Resources Integration (EHRI) for the Federal Government's human capital management. This disclosure is covered by SORNs OPM-GOVT-1 and GSA Agency-1.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?
Within GSA, OLU interacts with HR Links and GCIMS. Outside of GSA, OLU interfaces with SkillPort - Percipio to access courses for training. SkillPort - Percipio provides two types of training: A training course can be requested from the SkillPort - Percipio library and the course is loaded into the OLU for execution by the individual. A contract is in place for SkillPort -Percipio to provide the courses to GSA.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The PII information is uploaded daily from the system of record (HR Links and GCIMS). Note: Daily extract from HR Links which contains the employee name and their GSA email address The GCIMS extract contains the same information for contract personnel.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
OLU has individual and administrative role access to the data in the system. The access authorization is covered under the NIST SP 800-53 security and privacy controls defined in the System Security Plan.

6.1b: What is the authorization process to gain access?
The access authorization is covered under the NIST SP 800-53 security and privacy controls defined in the System Security Plan.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
4/30/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
OLU has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, along with system and information integrity.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
The system owner and Privacy Office rely on the GSA Information Breach Notification Policy to identify and address potential incidents and breaches. The Information System Security Officer, along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
The opportunities are defined under SORNs GSA/Agency-1 and OPM-GOVT-1.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
OLU only collects the minimum information in order to provide training to the employees and contractors as required by federal law and to send that information to OPM as required by federal policy.

7.2: What are the procedures that allow individuals to access their information?
OLU has a basic account created for all individuals through which they can view and update their training course information.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
Security and privacy training is given through the OLU as part of the on-boarding process and annual refresher training to all GSA employees and contractors.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
No training is provided on this specific system that requires a PIA. The security and privacy training employees receive annually covers the overall process.