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: 482
System Name: GSA Implementation of Yello
CPO Approval Date: 11/7/2024
PIA Expiration Date: 11/7/2027

Information System Security Manager (ISSM) Approval

Sergio Mendoza-Jimenez

System Owner/Program Manager Approval

Christopher kuang

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA Implementation of Yello

B: System, application, or project includes information about:
Personal/work email, name, phone numbers (optional), pronouns (optional), work availability, location availability, US Citizenship, resume, portfolio document, interview feedback.

C: For the categories listed above, how many records are there for each?
one record per user

D: System, application, or project includes these data elements:
Personal/work email, name, phone numbers (optional), pronouns (optional), work availability, location availability, US Citizenship, resume, portfolio document, interview feedback.

Overview:

U.S. Digital Corps was created as a pipeline to bring early career tech talent to the federal government. To ensure our Fellows represent the people we serve, we attend events and career fairs across the country to bring awareness of this opportunity to students and early career tech talent. To ensure we can follow up with potential applicants we meet at events, we are looking to collect their email addresses as well as other details like their school, graduation date, and field of study to ensure we send them tailored information based on upcoming events and our five tracks (cybersecurity, data science and analytics, design, software engineering, and product management)

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The nature of the system requires it. Authority for the system comes from the Federal Property and Administrative Services Act of 1949 (63 Stat. 377); title 5 U.S.C. and title 31 U.S.C., generally; and Executive Order (E.O.) 12953, February 27, 1995.

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?
Reference System of Records Notice (SORN) - GSA/Agency-1

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.
Retention Instructions: Temporary. Destroy 1 year after date of submission.
Legal Disposition Authority: DAA-GRS-2014-0002-0011 (GRS 02.1/060)
Approved by NARA: 1/19/2017

Retention Instructions: Temporary. Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later.
Legal Disposition Authority: DAA-GRS-2017-0011-0001 (GRS 02.1/050)
Approved by NARA: 9/22/2017

Retention Instructions: Temporary. Destroy 2 years after termination of register.
Legal Disposition Authority: DAA-GRS-2017-0011-0002 (GRS 02.1/051)
Approved by NARA: 9/22/2017

Retention Instructions: Temporary. Destroy when 1 year old, but longer retention is authorized if required for business purposes.

Legal Disposition Authority: DAA-GRS-2018-0008-0003 (GRS 02.1/180)
Approved by NARA: 6/3/2019

Retention Instructions: Temporary. Destroy 2 years after case is closed by hire or non-selection, expiration of right to appeal a non-selection, or final settlement of any associated litigation, whichever is later.
Legal Disposition Authority: DAA-GRS-2014-0002-0008 (GRS 02.1/090)
Approved by NARA: 1/19/2017

Retention Instructions: Temporary. Destroy 3 years after employee separates from service or transfers to another agency.
Legal Disposition Authority: DAA-GRS-2017-0007-0007 (GRS 02.2/060) Temporary
Approved by NARA: 5/31/2017

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.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
It has to collect names and contact information in order to make hiring decisions. Without those specific pieces of information, the candidates would not be able to be contacted.

U.S. Digital Corps was created as a pipeline to bring early career tech talent to the federal government. To ensure our Fellows represent the people we serve, we attend events and career fairs across the country to bring awareness of this opportunity to students and early career tech talent. To ensure we can follow up with potential applicants we meet at events, we are looking to collect their email addresses as well as other details like their school, graduation date, and field of study to ensure we send them tailored information based on upcoming events and our five tracks (cybersecurity, data science and analytics, design, software engineering, and product management)

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?
The Yello Government Recruiting Solution (YGRS) system protects the confidentiality and integrity of all data in transit. YGRS prevents unauthorized disclosure of information and changes to information in transit for the YGRS system by encrypting all communications, including all data in transit traversing the boundary and inside the boundary.

The YGRS system protects the confidentiality and integrity of customer information at rest in system databases and AWS S3 storage.

Yello also uses secureAuth for Identity access management.

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

3.4 Explain: Please elaborate as needed.
Yello does not monitor job applicants.

3.5 What kinds of report(s) can be produced on individuals?

Yello may create reports related to job applicants for a particular position, job series or similar category.

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?
The information that the candidate enters into yello like name, email, phone is visible so that they can be contacted at a later time for open positions.

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?
None

4.2How: If so, how will GSA share the information?
It doesn't share with any other parties.

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?
-Yello uses SecureAuth for an Identity access management solution for:

-Internal Yello administrators have to go through secureAuth. The internal system owner has to go through secureAuth as well.

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
These are enterprise tools provided by OCISO. No formal agreements are required to use them.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
It's up to the candidate/user to enter correct information and self-certify.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Administrators and system owner.

6.1b: What is the authorization process to gain access?
the system uses secureAuth.

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.
8/12/2024

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Yello has implemented the required security and privacy controls according to NIST SP 800-53. Yello employs a variety of security measures 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, system and information integrity, and program management. For more details about individual security controls, please refer to the Yello SSP.

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?
IR controls are implemented reference the SSP IR controls. This includes
all incident response procedures.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
at the form submission page applicants have to check the box "I accept GSA privacy policy" in order to submit. If they do not wish to provide information then they don't check the box and will not be able to submit their information.

7.1Opt: Can they opt-in or opt-out?
Yes

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2: What are the procedures that allow individuals to access their information?
There is no way to access anything after the information is submitted.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?
They can go back in anytime and look at it or modify it.

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.
GSA provides Security awareness training as part of the on-boarding process to all GSA employees and contractors. They must complete their Security awareness training prior to gaining access to any Yello environment. All yello solution team personnel receive initial security awareness training upon on-boarding, and conduct annual refresher training.

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?

Yello has implemented the required security and privacy controls according to NIST SP 800-53. The system employs 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.