Hire EZ

Privacy Impact Assessment

June 13, 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Table of contents

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about the Hire EZ application on Salesforce. *The Presidential Innovation Fellows (PIF)* may, in the course of *Hire EZ*, 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

HIRE EZ

System, application or project includes information about

- Applicants for Presidential Innovation Fellows (PIF) program positions

System, application or project includes

- Name of Applicant
- Contact Information (e.g., address, telephone number, email address)
- Citizenship, Current Employer, Veteran Status
- User and Online Information (e.g., LinkedIn page, resume)

Overview

The Presidential Innovation Fellows (PIF) program pairs top innovators from the private sector, non-profits, and academia with top innovators in government to collaborate during focused 6-13 month "tours of duty" to develop solutions. The fellows are chosen to work on specific projects, chosen by customer agencies. While the fellows are employed by GSA, they are detailed to customer agencies on a cost reimbursable basis, to work on specific projects.

The HireEZ application on Salesforce is a web-based application used by the PIF team to support their mission that has a dual purpose: It allows applicants to apply for the fellowship program described above, and it is used to review, route and rank applicants by GSA and customer agency employees. PIF Users access the Hire EZ application via the Internet and use the tool for creating and managing hiring seasons, collecting and processing applicant data, ranking applicant qualifications based on such data, and notifying applicants of their application status.

Information stored and processed by Hire EZ includes a description about the PIF program, questions, criteria, applicant self assessment, application review scores and hiring status; as well as applicant data such as resumes, contact information, citizen and veteran status, and user and online information.

The PIF team uses Hire EZ to create hiring seasons and hosts the application submission form to join the fellowship on their team's webpage where interested individuals (applicants) can apply. Applicants submit their information (e.g., contact, citizenship, current employer, resume, user and online information) via the PIF.gov webpage and then that is received and processed within Salesforce.

The PII collected is shown below. All PII collected is for the purpose of applying for employment at GSA / PIF from all job applicants.

- Name
- Email Address
- Home Address
- Telephone Number
- Resume / Employment history
- Veteran and Citizenship Status
- User and Online Information (e.g., LinkedIn)

System of Records Notice (SORN) - GSA's Customer Engagement Organization, **GSA/CEO-1**

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

Hire EZ is a web-based application used by the General Services Administration's (GSA) Presidential Innovation Fellows (PIF) as a tool for electronic automation of application submission, processing and review. Hire EZ resides on the Salesforce platform that has an Enterprise License Agreement with GSA to provide enterprise services and cloud solutions.

The PIF team uses Hire EZ to create hiring seasons and hosts the application submission form to join the fellowship on their team's webpage where interested individuals (applicants) can apply. Applicants submit their information (e.g., contact, citizenship, current employer, resume, user and online information) via the PIF.gov webpage and then that is received and processed within Salesforce. PIF users and managers as well as customer agency employees are able to review and rank applications, as well as send notifications (via the application) to applicants notifying them of their application status.

Hire EZ's Software as a Service (SaaS) provided by Salesforce relies on Salesforce's hardware and software. The system has been designed to comply with the following laws, regulations, policies and legal authorities:

1.2 What legal authority and/or agreements allow GSA to collect the information?

Executive Order -- Presidential Innovation Fellows Program (August 17, 2015)[1].

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

The applicants are sorted by their Hiring Season and their name.

System of Records Notice (SORN) - **GSA/CEO-1**

[1] https://obamawhitehouse.archives.gov/the-press-office/2015/08/17/executive-order-presidential-innovation-fellows-program

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No, OMB's ICR process is not applicable to GSA's Hire EZ as it is not an information collection activity.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

The recommended retention period for all information contained in this application is three fiscal years, but no longer than 10 fiscal years.

The system allows the flexibility for the Application Owner to request that entire records be deleted by a Salesforce administrator.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

No, HireEZ is a management tool for creating and managing fellowship vacancies, notifying potential applicants of open hiring seasons via the Internet, collecting and processing applicant data, ranking applicant qualifications based on such data, and allowing PIF users and Partner Agency Employees to view qualified applicants and notify applicants of their application status.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

Yes, notice is provided via System of Records Notice (SORN) **GSA/CEO-1** as well as through a Privacy Act notice at the point of collection when the site is live/active.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

No, this PIA and notices provided during the application process address notice, consent and transparency requirements.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

All applicants seeking employment with the Presidential Innovation Fellows (PIF).

The PII collected is shown below. All PII collected is for the purpose of applying for employment at GSA / PIF from all job applicants.

- Name
- Email Address
- Home Address
- Telephone Number
- Resume / Employment history
- Veteran and Citizenship Status
- User and Online Information (e.g., LinkedIn)

3.3 Why is the collection and use of the PII necessary to the system, application or project?

The HireEZ application on Salesforce is a web-based application used by the PIF team that has a dual purpose: It allows applicants to apply for the fellowship program described above, and it is used to review, route and rank applicants by GSA and partner agency employees. PIF Users access the Hire EZ application via the internet and use the tool for creating and managing hiring seasons, collecting and processing applicant data, ranking applicant qualifications based on such data, and notifying applicants of their application status.

Information stored and processed by Hire EZ includes a description about the PIF program, questions, criteria, application review scores and hiring status; as well as

applicant data such as resumes (not as attachments), contact information, citizen and veteran status, and user and online information.

The PIF team uses Hire EZ to create hiring seasons and hosts the application Salesforce submission form to join the fellowship on their team's webpage where interested individuals (applicants) can apply. Applicants submit their information (e.g., contact, citizenship, current employer, resume, user and online information) via the PIF.gov webpage and then that is received and processed within Salesforce.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No Hire EZ does not create or aggregate new data about an individual. The system does take the applicant reviewer ratings from Review Round 1 and Review Round 2 to determine what rating band the applicant falls within. The applicant falls into one of the following bands based off their Review Round Scores: Qualified, Well Qualified, Best Qualified, Superior. This information is used to determine which applicants will move to the next review round and ultimately get interviewed by the PIF team.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

This control is implemented by the Salesforce Organization. Assigned authorizations for controlling access are enforced through Force.com Administration Setup Profiles, Permission Sets & Public Groups.

1.) Practice least privilege permissions, where any user of the Hire EZ Salesforce application will have only the minimum privileges necessary to perform their particular job function.

2.) Assign a designated application owner. That application owner will:

- receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application);

- attend Security de-briefs, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team; and

● work with Salesforce release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes.

3.6 Will the system monitor the public, GSA employees or contractors?

No, the system does not monitor the public, employees or contractors. All logs of internal GSA associates and partner agency employees who access the system are reviewed on a monthly basis per GSA policy.

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

Hire EZ may create reports related to hiring seasons for a particular qualification category or for application review scores.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

Hire EZ does not de-identify data for reporting. The system does take the applicant reviewer ratings from Review Round 1 and Review Round 2 to determine what rating band the applicant falls within. The applicant falls into one of the following bands based off their Review Round Scores: Qualified, Well Qualified, Best Qualified, Superior. This information is used to determine which applicants will move to the next review round and ultimately get interviewed by the PIF team.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

Given the reporting capability, the security and privacy measures include access controls, awareness and training for users and auditing capability to ensure accountability.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

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?

Hire EZ limits information to what is required to carry out PIF employment activities.

Salesforce technical staff may access applicant data for the limited purpose of resolving reported system issues. Any unauthorized access must be reported in accordance with GSA's incident response procedural guide.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

Hire EZ shares demographic information with OPM as federally mandated.

Partner Agency Employees who are appointed as application reviewers for the PIF program will login through a Salesforce Community and will only have access to the applicants that are relevant for them to rank. This decision is made by the Application Owner (PIF team) of the Hire EZ application.

The system does take the applicant reviewer ratings from Review Round 1 and Review Round 2 to determine what rating band the applicant falls within. The applicant falls into one of the following bands based off their Review Round Scores: Qualified, Well Qualified, Best Qualified, Superior. This information is used to determine which applicants will move to the next review round and ultimately get interviewed by the PIF team.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Information is being directly provided by the individuals. It is the responsibility of the individual to assure the data provided is correct.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

No. The Hire EZ application has no internal or external connections to other systems.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

Partner Agency Employees who are appointed as application reviewers for the PIF program will login through a Salesforce Community and will only have access to the applicants that are relevant for them to rank.

Risk is mitigated through access controls implemented by the Salesforce Organization. Assigned authorizations for controlling access are enforced through Force.com Administration Setup Profiles, Permission Sets & Public Groups.

1.) Practice least privilege permissions, where any user of the Hire EZ Salesforce app will have only the minimum privileges necessary to perform their particular job function.

2.) Assign a designated application owner. That application owner will:

● receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application);

● attend Security de-briefs, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team; and

● work with release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Individuals/job applicants provide and self-certify the accuracy of the information in the system.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

Hire EZ data is logged and audited and otherwise controlled to ensure confidentiality, integrity and availability.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

Hire EZ has individual and administrative role access to the data in the system.

All access is granted via a request made by the user to the GSA IT Service desk (Service Now) which is then approved by the Salesforce minor application owner (Hire EZ in this case). Once approved, the user is then granted role-based access to the system by Salesforce system administrators.

This application is hosted in the Customer Engagement Org (CEO) of Salesforce. All GSA employees and partner agencies who require access to this application must have a Salesforce license within CEO as well as one of the custom Hire EZ Permission Sets in order to have access to this application. Partner Agency Employees who are appointed as application reviewers for the PIF program will login through a Salesforce Community and will only have access to the applicants that are relevant for them to rank.

Designated app owner has control over approving/denying user access requests (via ServiceNow).

- For Salesforce access we practice least privilege permissions, where any user of the Hire EZ Salesforce app will have only the minimum privileges necessary to perform their particular job function.

- Salesforce System Administrators operating within the Salesforce CEO org are required to have Tier 2S clearance to be granted their designated SNA account/credential. All System Administrators are required to access the system with provided SNA credentials. Designated by OPM, Tier 2S clearance is a moderate risk (formerly MBI Level 5B) required for Non-Sensitive Moderate Risk (Public Trust) positions.

6.2 Has GSA completed a system security plan for the information system(s) or application?

Yes, Salesforce is an element in the Enterprise Application Services (EAS) SSP with an ATO expiration date of 3/20/2020.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

As Salesforce is a cloud-based product, the minor application (Hire EZ) is protected by a multi-tiered security process. The cloud platform along with GSA's implementation of security controls provides a robust security profile. The data is protected by multiple access controls to the data, including login controls, profiles within the application and permission sets in the program. Program management has authority to grant access to the application at all application levels. All higher level system support staff are granted access based upon need to know/requirement based needs.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

Intrusion systems at the agency level provide a layer of security monitoring. Access to the GSA ORG unit is reviewed on a weekly basis, application permission sets are annually reviewed by the application owner.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

As with any application there are risks and GSA is required to follow all Federal mandates to secure information systems, regardless of PII status. By adhering to those mandates, GSA provides a high threshold of data security for data within its Information Systems.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

GSA does not actively solicit any information from individuals. Any information submitted by individuals (personal or otherwise) is completely voluntary.

7.2 What procedures allow individuals to access their information?

Should an individual request access to their information, it can and would be provided, in accordance with GSA's Privacy Act Rules at 41 C.F.R. 105-64 et seq..

7.3 Can individuals amend information about themselves? If so, how?

Individuals supply the original information. If information relevant to the inquiry is incorrect, then they can resubmit their application and information.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

Individuals who have submitted information have no access to data once it has been submitted since this is an internal application, but may be provided a copy. If an applicant needs to submit updated information then they would just submit a second application with their new information. If an applicant's contact information or relevant experience changed, the applicant would submit a new application with the updated information.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

All GSA employees and contractors with access to this system are required to complete IT Security Awareness and Privacy Training on an annual basis. Users who fail to comply may have all access to GSA systems revoked. High level system users receive annual role-based training for accessing systems with elevated rights. Those who fail to comply have access revoked.

Partner Agency Employees who are appointed as application reviewers for the PIF program will login through a Salesforce Community and will only have access to the applicants that are relevant for them to rank.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

GSA employees and contractors who use this system are required to complete IT Security Awareness and Privacy Training on an annual basis. Users who fail to comply may have all access to GSA systems revoked. High-level system users receive annual role-based training for accessing systems with elevated rights. Those who fail to comply have access revoked. These trainings help users identify and report potential incidents and decrease the risk that authorized users will access or use the applicants' data for unauthorized purposes.

Partner Agency Employees who are appointed as application reviewers for the PIF program will login through a Salesforce Community and will only have access to the applicants that are relevant for them to rank.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

Salesforce event monitoring is available for activity audits. Designated app owner has control over approving/denying stakeholder user access requests (via ServiceNow). Salesforce system administrators operating within the Salesforce EEO org are required to have Tier 2S clearance and use their designated SNA account. Access controls are monitored in accordance with GSA IT Policy.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

● Designated app owner has control over approving/denying stakeholder user access requests (via ServiceNow). App owners are required to conduct annual reviews of all users granted access to ensure continued/proper access it required.

● Practice least privilege permissions, where any user of the Hire EZ Salesforce app will have only the minimum privileges necessary to perform their particular job function. App owners are required to conduct annual reviews of all users granted access to ensure continued/proper access it required

● Salesforce system administrators operating within the Salesforce CEO org are required to have Tier 2S clearance and use their designated SNA account.

---

[1] OMB Memorandum *Preparing for and Responding to a 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.