Privacy Impact Assessment for

USA Suite Data Analytics (USADATA)

August 8, 2024

Contact Point
Caleb Judy
Business Program Manager
Human Resources Solutions

Reviewing Official
Senior Agency Official for Privacy

Abstract

USADATA is an Office of Personnel Management system used to provide advanced data analytics support to advance critical data projects in USA Staffing (USAS), USA Hire (USAH), USAJOBS (USAJ), and USA Performance (USAP). USADATA offers several advantages for federal data employees to focus on their workforce, organization health, and performance while improving their agency's customer experience regarding their agency workforce data. This Privacy Impact Assessment is being conducted because USADATA collects and maintains personally identifiable information from USAS, USAH, USAJ, and USAP.

Overview

Housed within the Office of Personnel Management's (OPM) Office of the Chief Information Officer (OCIO) organization, the USADATA platform propels federal human resources (HR) decision-making into new frontiers of efficiency, precision, and strategic impact. This platform is the cornerstone of a modernized HR ecosystem, harnessing the power of big data analytics, artificial intelligence, and intuitive interfaces to provide real-time, actionable intelligence that shapes the workforce of tomorrow.

At its core, the USADATA platform is designed to excite and engage its federal agency users by offering a seamless, user-centric experience. It brings to life the untapped potential within the extensive pools of federal HR data, converting it into a strategic springboard that enables members of the Senior Executive Service, HR professionals, hiring managers, and policymakers to make enlightened decisions about talent acquisition, workforce development, and organizational culture.

USADATA provides a cloud-based platform for sharing, collaborating, and consuming data analytics through Power BI apps, reports, and dashboards. The Power BI Service allows federal agency users to publish and distribute insights generated in Power BI Desktop, making data-driven decisions

accessible across an organization and the federal government. With features like real-time data refresh, sharing capabilities, and collaboration tools, Power BI Service enhances the efficiency of data analysis and reporting within a collaborative cloud environment for OPM's USAS, USAH, USAJ, and USAP systems.

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?

USADATA collects its source information from the USA Suite systems (USAS, USAH, USAJ, and USAP) and not the individuals themselves. The authorities for this system are available in the Privacy Impact Assessments for those systems and the applicable SORNs.

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

The Privacy Act System of Records Notices applicable to the information in USADATA are OPM/CENTRAL-13 (Executive Personnel Records); OPM/GOVT-2 (Employee Performance File System Records); OPM/GOVT-5 (Recruiting, Examining, and Placement Records); OPM/GOVT-6 (Personnel Research and Test Validation Records); and OPM/GOVT-7 (Applicant Race, Sex, National Origin, and Disability Status Records).

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

USADATA is in the process of obtaining an Authority to Operate (ATO) by September 2024. A system security plan was completed as part of the ATO package.

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

Yes. The records schedule number for USADATA is GRS 2.2, item 020.

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.

The information contained within USADATA is not covered by the Paperwork Reduction Act because it was obtained through the source systems of USAS, USAH, USAJ, and USAP.

Section 2.0. Characterization of the Information

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

USADATA collects the following information from USAS, USAH, USAJ, and USAP: vacancy identification number, title of job, first name, last name, address, city, state, ZIP code, email, country, citizenship, lowest grade, occupational specialties, geographic availability, veterans' preference (where applicable), and dates of active duty for military service (where applicable). USADATA also collects work location, position title, organization, supervisory status, performance review information, critical elements, weights of each element, performance requirements, performance standards, sub-elements, and strategic alignment.

Different agencies may pull additional data from the USA Suite systems into USADATA as needed, to include middle initial, telephone number, contact time, fax number, fax extension, permanent phone number, permanent phone number extension, place of employment, work address, work state, work country, work city, work ZIP code, employment availability (full time employment, temporary employment, jobs requiring travel, part time employment, special accommodation, other employment questions), background information, gender, date of birth, languages, hiring eligibility, professional skills, test location, availability date, service computation date, job preference, transition assistance plan, job related experience (years, months), and education information (college or university).

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

USADATA sources include the USA Suite core application systems of USAS, USAH, USAJ, and USAP. The data information is collected through a USADATA engineering process.

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, USADATA does not use any commercial or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

As data is collected in USADATA, accuracy is ensured by a combination of engineering processes verifying data quality and ensuring data integrity is established.

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

Privacy Risk: There is a risk that the information in USADATA is unreliable and will result in poor data quality leading to inaccurate analytical data for federal customer agencies.

Mitigation: USADATA mitigates this risk through several data engineering processes verifying data quality and data integrity on ingestion from the source systems of USAS, USAH, USAJ, and USAP as it is prepared for analytical presentation.

Section 3.0. Uses of the Information

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

USADATA is an OPM system used to provide advanced data analytics support to advance critical data projects in USAS, USAH, USAJ, and USAP. USADATA develops and deploys data reporting products and services for customers of these USA Suite applications. These products and services enable customers

to access the information needed to make data-driven decisions related to agency talent recruitment, applicant evaluation, staffing, onboarding, and performance management.

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 USADATA platform has search features that allow federal agency employees to query by keywords. This feature is not used to discover or locate predictive patterns or anomalies.

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

Within OPM, only USADATA staff have assigned roles and responsibilities within the USADATA platform system. USADATA program staff include both Human Resources Solutions (HRS) and OCIO personnel.

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

Privacy Risk: There is a risk that unauthorized individuals may access the information in USADATA and use it for an unauthorized purpose or that authorized users will access the information for unauthorized purposes

Mitigation: This risk is mitigated using access controls that restrict the ability to retrieve data based on an individual's authentication and authorization permissions that are built into the platform. The platform system maintains access roles that restrict and grant access to information and functionality to support the unique business process needs of a subscribing agency customer.

Privacy Risk: There is risk that the information in USADATA will be used outside of the scope of the purpose for which the initial collection was made.

Mitigation: This risk is mitigated by providing access, through access controls built into USADATA, only to authorized and registered agency users.

When agency users are authorized to access USADATA, they are informed regarding the appropriate use of the information it contains and agree to adhere to the Rules of Behavior.

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.

The platform system provides notices with a Privacy Policy, Full Terms and Conditions of Use, and Rules of Behavior which are presented to every user of USADATA.

USADATA users are also presented with a link to the Privacy Act Statement located on the footer of authenticated pages within the USA Suite applications.

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

When users sign in at USADATA, they are provided with and consent to the online Full Terms and Conditions of Use. These terms and conditions inform the user that their access and use of USADATA and all other USA Suite applications constitutes their consent for review by all authorized government and law enforcement personnel to monitor, record, audit, and take action as necessary to process their use of the system.

4.3. Privacy Impact Analysis: Related to Notice

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

Mitigation: USADATA mitigates this risk by requiring Full Terms and Conditions of Use consent upon login and providing access to the USADATA Privacy Policy on every page within the system.

Section 5.0. Data Retention by the Project

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

There is a business need for USADATA to retain information sourced from its affiliated USA Suite systems for up to 10 years. Retention beyond the standard 3 years before disposition (authorized in the records schedule referenced in Section 1.4) is authorized under the terms of the records schedule due to the information being required for business use relating to long-term talent acquisition, workforce development, and organizational culture analytics.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information in USADATA will be retained for longer than is necessary to fulfill the business need for the information.

Mitigation: This risk is mitigated because USADATA adheres to the records retention schedule and electronically deletes the information after the fulfillment of the business need.

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.

Information stored in USADATA is shared with approved federal customer agencies but is not shared with non-authorized users. Each federal customer agency only has access to information about its organization in USADATA and individual users are only permitted to access their agency data.

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

Any disclosure of information outside of OPM is done only consistent with the Privacy Act, such as pursuant to an applicable routine use in the relevant SORNs referenced in Section 1.2.

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

All federal customer agencies are subject to the SORNs referenced in Section 1.2 and are constrained in their re-dissemination of information based on their terms. In addition, agency users are subject to the Rules of Behavior that outline appropriate handling and use of USADATA information.

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

Records of requests for and disclosure of USA Suite data are managed by the USADATA program office and recorded by the User Support Branch and Talent Acquisitions Analytics Branch.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be disclosed and used for a purpose that is not consistent with the business purpose for which the information was initially collected

Mitigation: This risk is mitigated by disclosing information only pursuant to the routine uses in the relevant SORNs or as otherwise permitted by the Privacy Act and by requiring federal customer agencies to adhere to the Rules of Behavior and other relevant requirements contained in inter-agency agreements with USA Suite applications. Users are notified in the Rules of Behavior, agreed to annually, that unauthorized use or acts to accrue resources for unauthorized purposes, or otherwise misuse this system, are strictly prohibited and may result in criminal, civil, or administrative penalties.

Section 7.0. Redress

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

Users are required to authenticate into USADATA with a phishing-resistant multifactor authentication (PR-MFA). Users may also contact the OCIO USADATA Help Desk if they need assistance with access to their information.

Individuals with their federal HR data in USADATA can find instructions on how to request those records in the SORNs identified in Section 1.2 and the USA Suite system where they originally provided their information.

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

User information is managed through the USA Suite applications and updated accordingly. Users may also contact their federal agency representative to update inaccurate or erroneous information.

Individuals with their federal HR data in USADATA can find instructions on how to update the records that OPM or other federal agencies may have about them in the SORNs identified in Section 1.2 and the USA Suite system where they originally provided their information.

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

USADATA has an online help tool with a "Frequently Asked Questions" page that instructs users on how to obtain assistance, as well as a USADATA Help Desk that can assist users who have questions about correcting their information.

Individuals with their federal HR data in USADATA can find the procedures in the SORNs identified in Section 1.2 and the USA Suite system where they originally provided their information.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that federal agency customers will not be able to access or correct their agency information within USADATA.

Mitigation: This risk is mitigated by providing federal agency customers with direct access to USADATA and the ability to ensure all data is accurate, relevant, and up to date as well as access to other resources, such as the USADATA Help Desk.

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?

USADATA captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events. USADATA personnel review and analyze application audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions. Additionally, administrative access to the systems is limited to individuals within the OPM OCIO office only. These individuals are required to take OPM's annual IT administrator security training.

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

All OPM employees are required to take annual IT Security and Privacy Awareness Training. In addition, every agency user is required to accept the system's Rules of Behavior, which requires that they take the annual IT security and privacy training required by their agency. There are no role-based trainings currently required to use the system.

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 federal agency customer determines which individuals within their organization will be an authorized user of USADATA and assumes responsibility for ensuring that they choose the appropriate agency users. System access to USADATA is provided on an annual basis. Only authenticated and authorized users may obtain access to USADATA.

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?

Federal customer agencies are granted access to USADATA via a Statement of Service and associated Interagency Agreement (IAA). In addition, agency users electronically sign the agreement that contains the privacy and security policies for USADATA and the Rules of Behavior for all information types. Any new uses of the information or information-sharing agreements will be evaluated by the USADATA program in consultation with the appropriate OPM stakeholders, including the Office of the General Counsel, the Chief Privacy Officer, and the Chief Information Security Officer.

Responsible Officials

Caleb Judy
Business Program Manager
Human Resources Solutions

Approval Signature

Senior Agency Official for Privacy