TTS-DATA.gov

Privacy Impact Assessment

October 10 2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

richard.speidel@gsa.gov

Signature Page

Signed:

_____

Information System Security Manager (ISSM)

_____

Program Manager/System Owner

_____

Chief Privacy Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the Chief Privacy Officer is responsible for evaluating the PIAs for completeness of privacy related information.

Document Revision History

Date	Description	Version of Document
8/10/2018	Annual PIA Update	1.0

Table of contents

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 Technology Transformation Service (TTS) Data.gov. TTS may, in the course of Data.gov, 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

TTS-Data.gov

System, application or project includes information about

Federal employees, contractors, and the public

System, application or project includes

- First and last names (if user chooses to leave this information)
- Contact information (users have option to leave their email addresses)

Overview

Data.gov is a website providing a metadata catalog of datasets from agencies across the federal government. Users have the option of providing a name and email address when leaving a comment or asking a question about a particular dataset. Providing a name or email address is not required and users can choose to comment or ask questions anonymously. Email addresses that are

voluntarily provided are not made public, but are provided to an agency's open data point of contact when a request to a particular agency is made through Data.gov. For example, if an inquiry concerning an Environmental Protection Agency (EPA) dataset is received at Data.gov that inquiry is forwarded to the EPA open data lead by email.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA collects names and email addresses when users choose to leave comments or ask questions about a particular dataset. This information is retained in order to provide a direct response to the user from Data.gov or the agency responsible for the dataset in question.

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

GSA developed Data.gov pursuant to the E-Government Act of 2002 (44 USC § 3501). Data.gov has a Privacy Act Notice and the identifiable information that is collected in the system is voluntary and is not mandated by any other agreement.

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 information collected by Data.gov, email addresses and first/last names, are not retrieved by a personal identifier; therefore this system does not qualify as a Privacy Act System of Records and a SORN is not required.

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, an ICR has not been submitted because Data.gov is not an information collection.

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.

A records retention schedule is not required for the information collected in the Data.gov application; however, the system owner is evaluating how best to ensure that only timely and relevant information is maintained by the system.

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

The data collected by the system adheres to Principle of Individual Participation because it is collected directly from the user. The information collected is optional and privacy risks are minimal. The system itself captures email addresses and names, if they are provided, but this data can only be viewed by authorized Content Administrators and System Administrators.

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.

A privacy statement is presented to the user stating their information, if provided, will be shared with the appropriate agencies to assist in answering their questions. The privacy policy is located here: https://www.data.gov/privacy-policy.

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

The risks to public users are minimized because they are not required to provide either names or email addresses to ask questions or leave comments.

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?

Information included in the Data.gov system are from the users and general public who access the Data.gov site

3.2 What PII will the system, application or project include?

Data.gov collects names and email addresses of those users who choose to input that information. The input of names and email addresses from users is optional.

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

All users and the general public have the option to leave comments and ask questions regarding datasets within the application. If an individual is submitting a request, they have the ability to provide their name and email address if they would like to receive a response directly from Data.gov or the agency that provided the actual dataset.

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?

The application does not use technology to conduct electronic searches or queries within a database to discover predictive patterns or anomalies.

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

The only identifiable information collected by the general public is optional (First/Last Names and Email Addresses). If provided, this information is not displayed to the public and the system implements the least privilege principle and only allows Content Administrators and System Administrators to view the provided email addresses and names.

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

No

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

No reports are produced on individuals. Data.gov reports are designed to identify metrics about the datasets not the individuals who use them. For example, a data.gov report might indicate which dataset was the most popular over a given time period.

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?

N/A

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

N/A

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?

Yes - information collected (user names and email addresses - both of which are optional) is used to provide a response from Data.gov or the agency that supplied the actual dataset.

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?

Because Data.gov is a central catalog, users make comments and requests that need to be properly addressed by the agencies that own a particular dataset.

User are not required to provide names or email addresses in order to submit feedback. Data.gov forwards all comments/requests to the agency's open data lead for action. If the user provides a name and email address, Data.gov will share this information with the open data lead and at that point, the responsibility for responding to the user belongs to the agency that owns the relevant dataset. The Data.gov feedback system (Data.gov Help Desk) is designed to allow agency points of contact to access the feedback items for that agency only via OMB Max authentication.

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 collected directly from the user if the user chooses to release their name and email address.

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?

There are no information sharing agreements. The Open Data Policy directs agencies to comply with the policy requirements, which includes engaging with the public on dataset feedback in order to assist with the decision-making process to open additional federal datasets for public use.

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?

N/A

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?

Users of Data.gov are responsible for accurately submitting their information. There is no notice sent to the user concerning procedures for correcting their

personal identifiable information within the system. Any information inputted by the general public is accepted as is. Once submitted to the system, this information cannot be modified.

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?

The data collected by the system adheres to the Principle of Individual Participation because it is collected directly from the user. The information collected is optional and privacy risks are minimal. The systems itself captures email addresses and names, but this data can only be viewed by authorized Content Administrators and System Administrators.

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?

Access to the feedback items, a subset of which contains names and email addresses voluntarily provided by users, is limited to the Data.gov Program Management Office, which consists of three government FTEs. Technical support contractors who are cleared to work on GSA systems can access the system to address technical problems. For any agency point of contacts that sign up for access to feedback items for their agency only, access is granted via OMB MAX authentication and then assignment of access to agency feedback is granted by the Data.gov PMO. As of the date of this PIA, two (2) agency point of contacts have signed up for access. For both Data.gov PMO and agency point of contacts, there is no mechanism within the Data.gov website to disclose names and emails that are provided by users. In addition, Data.gov is working on a capability to anonymize or delete names and emails from feedback items after one year.

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

A 3 year ATO SSP has been completed for Data.gov. The system was granted its Authority to Operate (ATO) on March 30, 2018 as a Moderate system under the Federal Information Processing Standards Publication 199.

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

The security protections are discussed in detail in the Data.gov System Security Plan that supports the Data.gov 3-year Authority to Operate. The SSP discusses protections of any PII voluntarily submitted, such as names and emails of public users, such as data encryption, the limitation of access to such information to only the Data.gov PMO and its contractors, and the fact that any privileged use of Data.gov such as access to comments provided by the public is protected by authentication through OMB MAX with a PIV card or two-factor authentication.

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

Any security incidents regarding Data.gov data will be handled following the Data.gov Incident Response Plan as well as the GSA IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02.

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?

The data collected by the system adheres to the Principle of Individual Participation because it is collected directly from the user. The information collected is option and privacy risks are minimal. The system itself captures email addresses and names, but this data can only be viewed by authorized Content Administrators and System Administrators.

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.

The user can either provide their name or email address or not. The information is not required in order to provide feedback.

7.2 What procedures allow individuals to access their information?

Individuals are not required to provide any information to use Data.gov or to leave questions or comments. There is no process for allowing individual access to the information that is voluntarily provided.

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

Any information inputted by the general public is accepted as is. Once submitted to the system, this information cannot be modified.

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?

There is minimal privacy risk as there is no user account or information required to use Data.gov to access government data. Users are also not required to provide information to ask questions or provide comments, but may provide information if they wish and are seeking a specific response from Data.gov or an agency.

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.

GSA provides mandatory annual privacy and security training.

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?

Privacy risk is minimal as the only PII is name and email address voluntarily provided by certain users of Data.gov wishing to ask questions or leave comments. All Data.gov PMO and contractors with access to Data.gov are required to take the annual GSA mandatory privacy and security training.

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?

Access to the feedback items, a subset of which contains names and email addresses voluntarily provided by users, is limited to the Data.gov Program Management Office, which consists of three government FTEs. Technical support contractors who are cleared to work on GSA systems can access the system to address technical problems. For any agency point of contacts that sign up for access to feedback items for their agency only, access is granted via OMB MAX authentication and then assignment of access to agency feedback is granted by the Data.gov PMO. Thus far, two (2) agency point of contacts have signed up for access. For both Data.gov PMO and agency point of contacts, there is no mechanism within the Data.gov website to disclose names and emails that are provided by users. In addition, Data.gov is working on a capability to anonymize or delete names and emails from feedback items after one year.

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?

The data collected by the system adheres to the Principle of Individual Participation because it is collected directly from the user. The information collected is optional and privacy risks are minimal. The system itself captures

email addresses and names, but this data can only be viewed by authorized Content Administrators and System Administrators.

---

[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.