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: 474
System Name: Touchpoints (TP)
CPO Approval Date: 9/6/2024
PIA Expiration Date: 9/6/2027

Information System Security Manager (ISSM) Approval

Sergio Mendoza-Jimenez

System Owner/Program Manager Approval

Ryan Wold

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Touchpoints (TP)

B: System, application, or project includes information about:

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

D: System, application, or project includes these data elements:

Overview:

Touchpoints (TP) is a web application designed and created to support Customer Experience (CX) initiatives across the federal government by streamlining the customer feedback and reporting process. TP is managed and operated by the GSA's Federal Acquisition Service (FAS) Technology Transformation Services (TTS) in the Data Portfolio's Feedback Analytics Program.
The Touchpoints web application is online at https://touchpoints.digital.gov.

Touchpoints Background

A "Touchpoint", as described in the vocabulary of service design, is an interaction point between a customer user and a service. The impetus for Touchpoints was a software prototype created in 2016 called "Recruiter." Recruiter was created to recruit participants for product research. It helped agile product teams schedule customer interviews by prompting users of a digital service with a web form to opt into further research opportunities.
Touchpoints is a natural extension of the Data Portfolio's charter; enhancing data governance and intelligence capabilities and leveraging data as a strategic asset. The initial business case in 2019 for Touchpoints included supporting more than 20 High Impact Service Providers (HISP) and providing the ability to accept and report on online feedback related to the Customer Experience (CX) Cross-Agency Priority (CAP) Goals.

Touchpoints Service Offerings

Touchpoints is designed to support the CX practice by allowing staff to manage web forms to solicit feedback after certain points of interaction between a customer and a federal agency. Touchpoints helps streamline the gathering and reporting of feedback data for the purposes of improving customer experience and public service delivery.
Staff users can create web-based feedback forms and receive submissions from internal and public users. A Touchpoint form is designed to be deployed in one of the following two ways: 1) as a stand-alone webpage via a URL on the Touchpoints website, and 2) as a javascript tag that renders a form on an agency's website.
The initial Touchpoint Form to be supported was the A-11 Customer Feedback form. Applicable laws and regulations are described in Section 11 of this document. Additional forms will be added in the future; with specific consideration to CX and the Paperwork Reduction Act (PRA).

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
GSA's work developing Touchpoints is done under the following authorities or Executive Orders:

- Executive Order 13571, Section 2B, which directs agencies to "establish mechanisms to solicit customer feedback on government services and use such feedback regularly to make service improvements"
- GSA's collection of contact information is authorized by the E -Government Act of 2002 (P.L. 107 -347, 44 USC § 3501).
- 2018 OMB Circular A -11, Section 280: compliance for High Impact Service Providers participating in Cross Agency Priority Goal 4: Customer Experience.
- 21st Century IDEA Act (2018) · Customer Experience CAP Goal, GPRA (2013 -2017, 2018 -2020)
- Policies for Federal Agency Public Websites & Digital Services (M -17 -06, 2016)
- M -23 -22 - Delivering a Digital -First Public Experience
- Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government

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?
SORN not required

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?

1.2b: Explain why a SORN is not required.
Touchpoints information is not searchable by a personal identifier. Each submitted form response is assigned a random numeric identifier in the system. Some forms may be designed with questions that ask for name and or/email. Given the information would be collected, it could be searched for, if somebody was to analyze the data. Touchpoints provides no features to search for or link personal information including identifiers.

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.
In consultation with GSA's Senior Records Officer, the following schedules provide retention periods for Touchpoints' data:

- 352.2/011 - Publicly-posted Information (DAA-0352- 2016-0001-0004) - 3 years
- 352.2/021 – Information Service Program Management Records (DAA0352-2016-0001-0005) - 3 years

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? No

2.1 Explain: If not, please explain.
All applicable survey instruments are required to have a valid OMB PRA Approval number, which requires notice of information collection be provided to the public in advance of the collection, and throughout the duration the instrument is accessible for response.

All agency customer users of Touchpoints' administrative interface are subject to its published Terms of Service.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
Administrative User (AU) information in Touchpoints administrative interface consists solely of email addresses provided via Login.gov authentication.

Survey response information may also be directly collected from individuals participating in surveys. Links to surveys can be published to both Agency Customer web properties, are accessible at https://touchpoints.digital.gov, and may also be distributed by email to survey respondents. Limited, voluntarily- supplied PII may be collected (such as a first name) as well as voluntary contact information (e.g., email address, telephone number) for the purpose of contacting the user to resolve customer service issues.

Additionally, users are warned not to submit sensitive personal information in- line on the survey interface itself.

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?

Touchpoints is scanned at regular interval for vulnerabilities in the information system and hosted applications, and when new vulnerabilities potentially affecting the system/applications are identified and reported, Feedback Analytics PMO staff analyzes vulnerability scan reports and results from security control assessments; remediates legitimate vulnerabilities within appropriate time periods relative to the severity of the finding.

CircleCI is a continuous integration tool used for running automated tests of the Touchpoints software. Snyk is a static code analysis tool used to scan Ruby and Javascript dependencies for vulnerabilities. Additionally, Touchpoints participates in GSA's Bug Bounty program.

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

3.4 Explain: Please elaborate as needed.
No. Touchpoints does not have the capability to locate or monitor individuals.

3.5 What kinds of report(s) can be produced on individuals?
While Touchpoints does collect IP addresses, the system does not enable, and makes no effort to, enable reporting on individuals.

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?
Touchpoints does not have the capability to report on individuals. Each agency can access only the comments submitted on its service/application. An agency may download all comments to .csv file, but there is no native reporting capability.
In practice, the data captured in Touchpoints is used by their respective agencies. And those respective agencies have their own data policies and practices.

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?
GSA does not access and will not share Touchpoints information with anyone other than the agency the user submitted it to.

In certain scenarios, GSA may access data with permission of an agency staff, in order to help troubleshoot an issue or generally provider customer support.

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?
Touchpoints is hosted on Cloud.gov and utilizes Login.gov for multi-factor authentication of customers to the Administrative Interface.

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

4.4NoAgreement: Why is there not a formal agreement in place?
Cloud.gov is a direct contract/MOU between Cloud and the Feedback Analytics Project Management Office (PMO); while the Login.gov implementation is a "subcontract," part of a larger acquisition by the Office of Solutions within the Technology Transformation Services.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
Since information submitted via Touchpoints is voluntary and subjective, information will not be verified for accuracy or completeness.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Feedback Analytics program staff and contractors have administrative access to Touchpoints data (e.g. access to repositories where the form templates are stored and may escalate agency customer privileges).

Agency staff users are granted access to the forms they create and forms shared by other Form Managers. Agency customers are responsible for determining which of their staff may access and download data through Touchpoints as Form Managers or Response Viewers.

6.1b: What is the authorization process to gain access?
Federal staff users can sign up for Touchpoints with a .gov or .mil email address. Thus, any manager manages their own's form's permissions.

For Touchpoints Administrative permissions: Requests are made in writing to feedback-analytics@gsa.gov, and the Touchpoints PMO may elevate a user's Touchpoints permissions.

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.
8/18/2019

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
Touchpoints enforces authorization via custom implemented roles and permissions. Access to resources is dependent upon a user’s role and permissions; e.g., Form Manager, or Response Viewer.
Touchpoints maintains an automated test suite that includes “feature tests” (also known as “specs”) that exercise the integrated application with a web browser, simulating a user’s experience. This is a first -pass check for exceptions and system integration issues.
On an annual basis, an OWASP ZAP scan is performed in coordination with GSA IT.
Touchpoints monitors and controls communications at the external boundary of the system and at key internal boundaries within the system, implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks, and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

From a managerial perspective, Touchpoints Product team operates on the principle of least privilege for users. And staff users are inactivated after 3 months of inactivity.

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?
Touchpoints is hosted by Cloud.gov, which monitors system activity and analytics and alerts application owners of any suspicious or anomalous traffic/patterns.
Touchpoints employs vulnerability scanning tools. Each code commit is scanned for vulnerabilities using Snyk, and GitHub (where source code is versioned) also sends alerts to staff based on known vulnerabilities. Monthly Invicti scans are performed on the system, coordinated by Touchpoints' ISSO, SecOps and GSA IT.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Participation in Touchpoints surveys is voluntary. A person's responses (or lack thereof) can in no way affect that person's eligibility for or access to any government benefit, service, or position. With the exception of contact information (name, work or personal email address and phone number) collected with the user's consent for the purpose of following up with a user about their feedback, response data is not associated with identifiable information about the respondent.

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?
Individuals can access and review their survey responses up until they "submit" the form. The system does not permit individuals to update or change previously- submitted survey responses.

Managers are responsible for determining access permissions for their Touchpoints forms.

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.
All Feedback Analytics Program staff with Administrator (full privilege) rights to access Touchpoints have undergone and are subject to GSA's annual Privacy and Security 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?
The Feedback Analytics program invalidates accounts that have not logged in in 3 months, and the program conducts biannual reviews of authorized Agency Customer accounts, requesting via email that each users confirms access to their surveys and survey responses in Touchpoints, and remove any out-of-date or otherwise invalid account access.