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: 431
System Name: GSA Implementation of Genesys
CPO Approval Date: 9/25/2023
PIA Expiration Date: 9/24/2026

Information System Security Manager (ISSM) Approval

Ryan Palmer

System Owner/Program Manager Approval

Russell O'Neill

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

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

B: System, application, or project includes information about:
Business Information: For business information, quality assurance, contact workforce management information, and call recordings data are collected.

Device or Software-based device Information: For device or software-based device information, the system captures types of device and browser used.

C: For the categories listed above, how many records are there for each?
The GSA Implementation of Genesys captures/contains about 500,000 customer call records on annual basis; Less than 25,000 annually for Quality Assurance Information.

D: System, application, or project includes these data elements:
Phone numbers associated with each call recording is stored in GSA Implementation of Genesys.

Salesforce, which will be integrated with the GSA Implementation of Genesys has fields for a customer's first name, phone number, and email address. However, if a customer emails the contact center, a phone number is not requested or stored within the Salesforce. Likewise, if a customer chats or emails the contact center, only an email address and, if optionally provided, first name is stored.

Overview:

The Genesys application is a comprehensive and centralized omnichannel solution designed to facilitate all call center activities including, Telephony, Workforce Management and quality. This application is cloud hosted by Genesys which will utilize existing Tollfree phone numbers to be ported to the platform. The USAGov Contact Center answers questions from the public via phone, email, and chat. Salesforce is used by the contact center to provide case management , web chat, and knowledge base management functions.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
Pub. L. 107-347 § 204: The information collected is required to respond to customer enquiries. The information collected is not disseminated to the public.

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?
SORN: **GSA/OCSIT–1** (SYSTEM NAME: **USA.gov**)

https://www.federalregister.gov/documents/2016/07/18/2016-16868/privacy-act-of-1974-notice-of-an-updated-system-of-records

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.
The recordings are stored for a minimum of 90 days and the records are collected/stored for quality assurance purposes.

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.

This information is collected via Salesforce and Genesys when customers reach out to USAgov Contact Center. This information is needed when responding to the customer.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
The only listed/collected PII is the phone numbers of customers because this is associated with the customer call recordings.

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 GSA Implementation of Genesys has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ 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, Contingency Planning, security assessment and authorization, identification and authentication, system and services acquisition, system and communications protection.

3.4 Will the system monitor the public, GSA employees, or contractors?
Public

3.4 Explain: Please elaborate as needed.
Contractors receive call from the public that are monitored for quality assurance purposes.

3.5 What kinds of report(s) can be produced on individuals?
The system has capabilities to pull call reporting based on metrics

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?
Under most circumstances, no reports are generated with identifiable data. However, in certain cases it maybe required to report on how many times a particular caller, for example, calls the contact center to ensure calls are from legitimate customers.

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?
Federal Agencies

4.2How: If so, how will GSA share the information?
USAGov's customer agencies will have access to the call recordings in Genesys for internal quality assurance.

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?
Genesys will connect with Salesforce for purposes of creating cases in Salesforce for each received call.

This will be done automatically via APIs.

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

4.4NoAgreement: Why is there not a formal agreement in place?
Genesys will work within the Salesforce security boundary.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The information provided by the users is relied on for these purposes.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
The authorized GSA employees or Contractors

6.1b: What is the authorization process to gain access?
The authorization process follows GSA policy for granting access and every user is required to go through the formal access process and request from the program office to be granted access

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.
9/29/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The GSA Implementation of Genesys has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ 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, Contingency Planning, security assessment and authorization, identification and authentication, system and services acquisition, system, and communications protection.
GSA SecureAuth/SSO is leveraged for identification & authentication control; user accounts authorization procedure in place; telecommunications services provisioning; data in transit and at rest encryption capabilities for communications protection.

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?
The program office follows GSA IR policy.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
The entire program is opt-in

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?
The only information collected is information provided by the customer when contacting the contact center.

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.
GSA requires all personnel with access to data to go through annual privacy training through GSA Online University. This will be achieved by completing the annually assigned GSA “IT Security & Privacy Awareness Training” course.

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 system owner ensures the documented policies in the SSP are followed - Only authorized users are allowed access to the information. Additionally, only personnel that have completed the GSA IT Security & Privacy Awareness Training are considered authorized users.