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: 390
System Name: Enterprise Intelligent Document Processing (EIDP)
CPO Approval Date: 7/20/2022
PIA Expiration Date: 7/19/2025

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Laura Gerhardt

PIA Overview

A: System, Application, or Project Name:
Enterprise Intelligent Document Processing (EIDP)

B: System, application, or project includes information about:
The EIDP platform will be used to process documents such as acquisition contracts and commercial leases. For some acquisition contracts and real estate leases, such as those for small businesses, the small business owner may

not have an office and may use their home address and SSN as a way to uniquely identify the business. The acquisition contracts and real estate leases may include contact information and financial information, such as credit information and ACH for automated payment.

C: For the categories listed above, how many records are there for each?
The system process about 510,000 records.

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

- Name;
- Contact information (e.g., Address, Telephone Number, Email Address);
- Financial Information (Bank Routing, Bank Account #, and Tax Identification Number (TIN));
- Legal
- Procurement/Acquisition
- Proprietary Business Information

Overview:

Enterprise Intelligent Document Processing (EIDP) is an enterprise-scale intelligent data capture and extraction solution. It's a document capture platform and offers advanced recognition capabilities and NLP (Nature Language Process) to handle every type of document and every job size. The platform has a connector to allow RPA (Robotic Process Automation) integration. EIDP feeds content-driven business applications such as RPA and BPM, helping the organization focus on customer service, cost reduction, federal compliance, and competitive advantage.
EIDP uses the ABBYY FlexiCapture which is a highly scalable platform for intelligent data and document capture which can be successfully used to extract data from unstructured as well as structured paper documents, scans, e-mail messages, and other sources for subsequent use in document management systems. The four basic data extraction operations in ABBYY FlexiCapture include classification, optical recognition, verification, and export to ERP, ECM or BPM systems. ABBYY FlexiCapture is capable of handling the full range of data processing needs, from small-scale projects to distributed industrial capture of large volumes of data, providing high levels of security and reliability expected from enterprise-grade software solutions

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
Federal Property and Administrative Services Act, as amended (40 U.S.C. Sec. 585).

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?
GSA/PBS-5 (eLease)

https://www.federalregister.gov/documents/2008/04/25/E8-8934/privacy-act-of-1974-notice-of-updated-systems-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.
This follows the NARA record retention schedule.

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.
The system is process contracts that are entered into outside of the system.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
The EIDP processes the documents and extracts critical information including PII to analyze the payment schedule, forecasted revenue, and business risk to the agency. Given the volume and length of the documents, the EIDP is used to automate and substantially speed up the review of the portfolio of contracts.

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?
Role-based access control has been put in place.

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

3.4 Explain: Please elaborate as needed.
The system will not monitor the public, GSA employees or contractors.

3.5 What kinds of report(s) can be produced on individuals?
The EIDP platform could be used to produce reports about the business risk, payment status, expiration of the contracts. If the party to the contract uses his or her personal information, then that information may be displayed in the report to uniquely identify the contract.

3.6 Will the data included in any report(s) be de-identified?
Yes

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?
The ABBYY engine will extract the data from the PDF

3.6 Why Not: Why will the data not be de-identified?

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?
No information will be shared with

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?
ERPA

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

4.4NoAgreement: Why is there not a formal agreement in place?
The AO are the same for both systems. ISA is not required.

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 will be extracted from the PDFs and validated by the accountants.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
The administrators, Operations Manager, Processing Server, Monitoring Operator, and DBO

6.1b: What is the authorization process to gain access?
The EIDP platform will be authenticated using SecureAuth which requires Multi-Factor Authentication (MFA) through a PIV card and/or user id, password, and passcode. Additionally, the EIDP platform uses ACL to define roles and limit access to certain parts of the platform. Furthermore, data is encrypted at-rest and in-transit using FIPS 140-2 validated cryptographic modules.

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.
8/6/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
This system is housed in the on prem datacenter (RTP and STENNIS) and is segregated through firewalls and access is approved through the change control process.

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?
Audit logs for user activities have been configured

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
Opportunities exist for individuals to opt-out at the time of entering the agreement.

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 person can opt out during the contract formation which occurs outside of this system.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
They can send email to the program office to 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.
The persons entering the contract are provided with privacy rights through the contract formation process. Additionally, they often retain counsel to guide them through the process and negotiate the terms.

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 EIDP automation scripts are peer reviewed by many parties prior to being deployed to production to ensure that there is no unauthorized sharing of information. All parties who can access the data must sign an NDA, go through a background check, and be assigned a specific role.