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: 393
System Name: Real Estate Tax (RET)
CPO Approval Date: 10/7/2022
PIA Expiration Date: 10/6/2025

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chris McFerren

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Real Estate Tax (RET)

B: System, application, or project includes information about:
The application collects tax documentation and data from External GSA Lessors who hold a GSA lease where the agreement allows for Real Estate Tax Adjustments. These adjustments require submission of property tax bills and

proof of payment of property taxes for processing. This tax documentation is created by the associated taxing authority which sends it to the Lessor, who, as a registered RET Portal user, can search for their leases and upload the associated tax documentation.

C: For the categories listed above, how many records are there for each?
Information is captured for leases as required per the terms of the lease. Annual reporting requirement for those leases is currently less than 500 leases. The system has the ability to handle all government leases should the requirement be extended to additional leases, which could be up to +/- 8000 leases.

D: System, application, or project includes these data elements:
Privacy Risk: Information contained in submitted tax documents varies by municipality and by ownership entity; documents could contain Names, Addresses, Tax ID Numbers (which may be SSN for small business owners), Business or Home Addresses of Property Owners, Phone Numbers and other personally identifiable information.
Mitigation: Document submissions to RET Portal are only visible and accessible by the individual who has made the submission. No external entities are able to access information submitted by others. Documents are transmitted to G-REX via integration with Salesforce. GSA employees will access the documents through the electronic lease file in G-REX and process the escalation. Only GSA employees with the appropriate level of access to G-REX are able to view the submissions to the application.

Overview:

GSA Office of Leasing and PB-ITS maintains the RET portal to reduce inefficiencies by automating the intake and routing of documents from lessors, tracking processing of adjustment, reducing administrative burden associated with managing documentation and improving the accuracy of tax calculations and reimbursements to the Lessors.
GSA Office of Leasing has implemented a Real Estate Tax (RET) Portal on the Salesforce platform. This RET Portal allows for the electronic collection and efficient processing of Real Estate Tax adjustments for GSA Leased properties in accordance with GSA lease terms. GSA Leased building owners submit data and documentation relating to property taxes for buildings leased to GSA. Information contained in submitted tax documents varies by municipality and by ownership entity; documents could contain PII but are not required to. To use the portal, Lessors must register. Registered users have the ability to search for their leases and to upload the associated tax documentation. Registered users only have access to their lease information and to the documentation that they submit.
RET uses Salesforce two-factor authentication as a security measure. A visual flow will be initiated once the user logs in by providing a valid username and password. This flow generates a 5 digit random code and emails it to the user. The user is presented with a screen to enter this 5 digit code to successfully authenticate and once authenticated the user is allowed to login to the community.
Uploaded documentation is sent to GSA Real Estate Exchange (G-REX) via integration with the Salesforce application. When a user submits an RET case in Salesforce, a notification is sent from Salesforce to G-REX with information regarding the case and the documents that were submitted.
G-REX is the System of Record for Lease and Lease Project Documentation. GSA employees will access the documents through the electronic lease file in G-REX and process the escalation.
Information contained in submitted tax documents varies by municipality and by ownership entity; documents could contain Names, Addresses, Tax ID Numbers (which may be SSN for small business owners), Business or Home Addresses of Property Owners, Phone Numbers and other personally identifiable information. Submissions to RET Portal are only visible and accessible by the individual who has made the submission. No external entities are able to access information submitted by others. Documents are transmitted to G-REX via integration.
Only GSA employees with the appropriate level of access to G-REX are able to view the submissions to the application.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
Pursuant to 40 U.S.C. 585 the General Services Administration Administrator has the authority to enter into a lease agreement with a person, co-partnership, corporation, or other public or private entity for the accommodation of a federal agency in a building (or improvement) which is in existence or being erected by the lessor to accommodate the federal agency. More than half of GSA Lease Agreements allow for Real Estate Tax Adjustments. To make such adjustments, GSA requires submission of property tax bills and proof of payment of property taxes for processing. The application does not require PII specifically; however, GSA recognizes that there may be PII may be contained within the submitted property tax documentation generated by the taxing authority. The lease contract requires the lessor to provide these to GSA, at least annually.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?

No

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
eLease SORN, GSA/PBS-5

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.
The information is not covered by the PRA.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Documents loaded into RET are considered "intermediary" to the ultimate location where these documents are stored; the leasing files themselves in GREX. To that end, RET will store the documents under DAA-GRS-2017-0003-0002 (GRS 5.2/020) - "Intermediary Records" with a retention period based on whether a lease is active or closed (aka terminated, expired). After a lease is closed, those documents stored in RET will be deleted 2 fiscal years following the lease close date. The official copy of those RET documents will be considered part of the Leasing File Records stored in GREX. (DAA-0121-2015-0001-0015 (121.3/031) - "Leasing File Records." Those Leasing File Records (with the RET-supplied documents) stored in GREX are retained for 12 fiscal years and destroyed unless there is a legal hold or business reason to hold up on that destruction.

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? Yes

2.1 Explain: If not, please explain.
The application contains the following Privacy Act Notice, developed in consultation with the GSA Privacy Office:
GSA collects and processes Real Estate Tax escalation documentation from individuals and businesses through this Real Estate Tax Portal (RET) pursuant to the terms of your GSA Lease Agreement and 40 U.S.C. Sec. 585.. GSA may use information you submit pursuant to its published Privacy Act system of records notice, GSA/PBS-5, eLease. Use of RET is intended to expedite the processing of your Real Estate Tax Escalation request. Your use of RET is voluntary; however, if you do not submit the requested information via this electronic portal, a delay in processing your Real Estate Tax Adjustment may occur. This is a gsa.gov website and is also subject to the GSA Privacy and Security Notice.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
The information collected in the RET Portal is used solely to process Real Estate Tax Adjustments pursuant to GSA Lease terms with External Lessors. This documentation is collected to ensure proper accurate and timely payment of property taxes. Data collected is related to the document uploads made each year for a lease for easy identification purposes in the G-REX Application. Submission dates, tax years and associated system data will be used to effectively manage the efficiency of the Lease Contract Administration program (analyze processing time, utilization).

In most cases PII is not collected and it is not required however, depending on the contractor entity, they may provide documents that contain a home address that is used for business purposes and or provide canceled checks as proof of payment of taxes. There is no standard format for these submissions since taxes are handled differently in each municipality where our leases are located. The PII is not necessary for the system but there is no guarantee that a lessor will not upload something that contains PII in response to contract Real Estate Tax requirements.

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?
No aggregate data is created or used by or within this application.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
Access to the Salesforce Real Estate Tax Application is managed by a similar ticketing process. Access requests are submitted through the ServiceNow request form where they are routed to the application owner for approval. Upon approval, the user and related access permissions are provisioned. In the event that a user leaves GSA, their account is automatically disabled via sync with Active Directory. Access is restricted to Lessors with the requirement to submit property tax docs to GSA. For RET there will be no internal users. External submissions by lessors will flow through RET to G-REX. GSA employees access to G-REX is governed by its own access policies. External individuals register for the RET application through a public facing web page. Upon registration, they do not have access to any system data and will only be able to access data and documents that they themselves create. The user access is denied only if the user is not registered in advance. However, an external contact logging on has access to only submissions made from that log on account. There is no requirement for, or approval process for external user registration. Anyone with a valid email address (needed for the 2-factor authentication) can register. There is no risk there as submission of tax documents does not guarantee approval. Review and approval is a separate process.

This control is implemented by the Salesforce Organization. Assigned authorizations for controlling access are enforced through Force.com Administration Setup Permission Sets & Public Groups.

1.) Practice least privilege permissions, where any user of the RET Salesforce app will have only the minimum privileges necessary to perform their particular job function.

2.) Assign a designated application owner. That application owner will receive auto-generated emails from the GSA Helpdesk (ServiceNow) to review and either approve/reject or ask for additional clarification for any pending tickets regarding system modifications (including adding users to access the application); attend Security de-briefs, to review and then digitally sign updated security packages as appropriate and outlined by their respective Security team; work with release managers to determine appropriate date/timing of deployment and any communication or training surrounding those changes.

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

3.4 Explain: Please elaborate as needed.
Audit trails are kept within the RET database for all inserts, updates, and deletions of data. This information can be queried by personnel with access to the audit logs to investigate or reconstruct potential issues related to the system. Role-based access is implemented in the system and each agency has a role assigned so that the users cannot see data which they do not have a business need to know. Accesses by the different individuals are audited at the platform level of the application and can be researched in the event of a security or privacy incident. The O & M team reviewed the logs and reported any anomalies to business owners and ISSO. ISSO also performs monthly log review.

3.5 What kinds of report(s) can be produced on individuals?
No information can be derived from any reports as there are no reports created from this system regarding any individual or PII. Access to the Salesforce platform ORG is monitored as required by GSA policy and requirements for auditing noted within the system SSP.

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?

Information is not included in any reports, so there is no process to de-identify any information.

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?
N/A

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
All information is provided by the designated lessee, who is responsible for submitting required documentation.

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?
Uploaded documentation is sent to GSA Real Estate Exchange (G-REX) via integration with the Salesforce application. The integration is a secure API connection using a system owner approved service account. As both systems belong to GSA PBS Office of Leasing there is no need for any MOU, agreement, etc.

GSA_ Real Estate Exchange (G-REX) is the system of record for all lease documentation, including Real Estate Tax documents. Documents are pushed to G-REX via an integration for storage. Data is emailed to lease contract administrators to notify them there is a Tax action to address.

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

4.4NoAgreement: Why is there not a formal agreement in place?
As both systems belong to GSA PBS Office of Leasing there is no need for any MOU, agreement, etc.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The application does not check the accuracy of the information provided. The review occurs manually via a document review in G-REX. The application is not intended to check the data. It is a communication conduit with the Government. The nature of tax documentation and data is such that manual review is required.
Documents and data are reviewed by the Lease Contract Administration teams in the regions.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Access to the Salesforce Real Estate Tax Application is managed by a similar ticketing process. Access requests are submitted through the ServiceNow request form where they are routed to the application owner for approval. Upon approval, the user and related access permissions are provisioned. In the event that a user leaves GSA, their account is automatically disabled via sync with Active Directory. Access is restricted to Lessors with the requirement to submit property tax docs to GSA. For RET there will be no internal users. External submissions by lessors will flow through RET to G-REX. GSA employees access to G-REX is governed by its own access policies.

6.1b: What is the authorization process to gain access?
External individuals register for the RET application through a public facing web page. Upon registration, they do not have access to any system data and will only be able to access data and documents that they themselves create. The user access is denied only if the user is not registered in advance. However, an external contact logging on has access to only submissions made from that log on account. There is no requirement for, or approval process for external user registration. Anyone with a valid email address (needed for the 2-factor authentication) can register. There is no risk there as submission of tax documents does not guarantee approval. Review and approval is a separate process. There is no restriction.

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.
8/14/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
As Salesforce is a cloud-based product, the minor application is protected by a multitiered security process. The cloud platform along with GSA implementation of security controls provides a robust security profile. The data is protected by multiple access controls to the data, including login controls, profiles within the application and permission sets in the program. Program management has authority to grant access to the application at all application levels. All higher level system support staff are granted access based upon need to know/requirement based needs.

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?
Intrusion systems at the agency level provide a layer of security monitoring. Access to the GSA WS ORG unit is reviewed on a weekly and monthly basis by the assigned security officer, application permission sets are annually reviewed by the application owner. Upon notification of a breach, GSA has a fully developed incident reporting plan in place to review and mitigate any incidents.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
See Privacy Act Notice within application. The notice explicitly states the intended purpose for the collection of this information and its use in processing Real Estate Tax Adjustments in accordance with the Lease Contract. The notice informs the user of the potential delay in processing for failing to submit documentation via this portal. Privacy notice is displayed at several places and across the community as a link in footer.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
The data requested is required to be submitted electronically to the RET. By signing the lease they are agreeing to share the required tax information.

7.2: What are the procedures that allow individuals to access their information?
Requests from individuals for access to their records may also be addressed to the G-REX Program Manager. GSA rules for individuals requesting access to their records are published in 41 CFR part 105-64.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?

Information regarding the contract/contractor are associated with the lease and can be changed using the System for Award Management.

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 Federal Government employees and contractors receive annual general security awareness and privacy training. This is relevant to how the application records are handled and users will understand the importance of protecting the records and documents stored in the system. None of the Salesforce applications encrypt documents and this would be a risk assumed by the Workspaces org or a larger SF entity, and not RET specifically. Federal employees and contractors acting on the government's behalf access the information collected in the RET Portal via internal application G-REX. Privacy and security training is required by all Federal Employees and contractors acting on their behalf and there is no specific security training in relation to G-REX. Since federal Employees do not use the Salesforce RET Portal directly the only applicable training would be for the recipient application G-REX. There is no required training for External users.

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?

Audit trails are kept within the RET database for all inserts, updates, and deletions of data. This information can be queried by personnel with access to the audit logs to investigate or reconstruct potential issues related to the system. Role-based access is implemented in the system and each agency has a role assigned so that the users cannot see data which they do not have a business need to know. Accesses by the different individuals are audited at the platform level of the application and can be researched in the event of a security or privacy incident. The O & M team reviewed the logs and reported any anomalies to business owners and ISSO. ISSO also performs monthly log review.