ADTRAV - PIA

Privacy Impact Assessment (PIA) - Guidance

POINT of CONTACT

privacy.office@gsa.gov

Version 1.6: 4-17-2025

Instructions for GSA vendors:

This guidance is designed for nonfederal systems described in the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" and NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A supplement to NIST Special Publication 800-171". General Services Administration (GSA) requires vendors to conduct privacy impact assessments (PIAs) for electronic information systems and collections in accordance with GSA Order CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. PIAs offer an opportunity for vendors to highlight the data protection, privacy by design, data minimization and similar principles that their services may employ.

Vendors may use this or their own templates/forms to meet the requirement. If vendors use their own template, GSA requires that vendors order their sections/responses consistent with the below questions for the benefit of GSA's customer agencies and for simplicity during the review process. The vendor must demonstrate how it collects, stores, protects, shares, and manages personally identifiable information (PII). The purpose of a PIA is to demonstrate that nonfederal system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. GSA will publish the final product on its public website https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia. Please review all questions and the bracketed guidance, then develop your response.

GSA Stakeholders

The GSA representatives listed below have reviewed the information provided by the vendor for completeness.

Arpan Patel, GSA Information System Security Manager (ISSM):

X DocuSigned by: Arpan Patel 1/16/2026
8B059AABDAF1477...

GSA Information System Security Manager

Michael Salter, GSA Program Manager:

X DocuSigned by: Michael Salter 1/16/2026
ABA02A5B3FBB446...

GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X DocuSigned by: Richard Speidel 1/16/2026
171D5411183F40A...

GSA Chief Privacy Officer

Jason Cross, GSA Contracting Officer (CO):

X DocuSigned by: Jason Cross 1/20/2026
B793E8ECC5264E9...

GSA Contracting Officer Representative

800-171 PIA Template Document Revision History

Date	Description	Version of Template
	Initial Draft of Non-Federal System	
06/10/2020	Initial Draft of Non-Federal System PIA	1.0
08/05/2020	Version for rideshare vendors	1.1
10/20/2020	General updates for broader template usage	1.2
08/03/2021	Formatting and made 508 compliant	1.3
05/07/2022	Formatting and editing	1.4
01/14/2026	Privacy team review and updates requested	1.5
01/16/2026	Final revision	1.6

Table of Contents

Document purpose

This document contains guidance for vendors that maintain and operate nonfederal systems. To provide the requested service, the vendor collects, maintains and/or disseminates 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.

Vendors should use this PIA guidance to explain how and why they collect, maintain, disseminate, use, secure, and destroy information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals.

Overview

A. System, Application, or Project Name:

ADTRAV - RezDesk

B. GSA Client:

ADTRAV Travel Management - TMC Services

C. System, application, or project includes information about:

Federal Employees and their travel information.

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

- *Name*
- *Gender*
- *Birth Date*
- *Address*
- *Citizenship*

[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."

- *Email Address*
- *Cell Phone Number*
- *Drivers License Number*
- *Nationality*
- *Passport Information*
- *Employee Identification Number*
- *Loyalty Number*
- *Credit Card Number (PCI)*
  - *PAN*
  - *Expiration Date*
  - *CVV*
- *IP Address*
- *Browser Type*

E. The purpose of the system, application, or project is:

RezDesk, developed by ADTRAV, is designed to provide efficient and secure travel management services for government agencies, including the General Services Administration (GSA). By integrating advanced technology with high-quality customer service, RezDesk helps optimize travel processes and maximize return on investment (ROI) for its clients.

RezDesk collects Personally Identifiable Information (PII) from government employees to facilitate travel bookings and reservation management. This data is necessary to fulfill the Department's mission of providing employees with a streamlined and compliant method to book, modify, and manage travel reservations.

Collection and Use of PII:

• Data Collection: Employee travel profiles, including name, contact information, and travel preferences, are received through ETSNext or entered directly by users. • Processing & Usage: This information is transmitted securely to external systems such as the Global

Distribution System (Sabre) to facilitate booking and itinerary management. • Data Protection: All sensitive information is encrypted in transit (TLS v1.2 or higher) and at rest (AES-256). Access is restricted through role-based access control (RBAC) and multi-factor authentication (MFA).

- *Data Retention & Disposal: PII is retained only as long as necessary to meet travel and compliance requirements. Once data is no longer needed, it is securely disposed of per federal data retention policies and the ADTRAV Media Sanitization Procedure. Data is considered as no longer needed based on the following criteria.*
    - *An account has left ADTRAV and is no longer active.*
    - *The information is no longer needed to process remaining travel requests.*
    - *The information meets thresholds defined in ADTRAV's Data Retention Policy.*

RezDesk ensures government employees have a reliable and secure platform for managing travel, reducing administrative burden while maintaining compliance, security, and efficiency.

SECTION 1.0 OPENNESS AND TRANSPARENCY

1.1 Are individuals given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

Yes, individuals are provided notice before the collection, maintenance, use, or dissemination of their personal information. This notice is presented through privacy policies, consent agreements, and system usage terms during the booking process. Users are informed about the purpose of data collection, how their information will be used, and the security measures in place to protect their data. https://www.adtrav.com/privacy-statement/

SECTION 2.0 DATA MINIMIZATION

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

The collection and use of Personally Identifiable Information (PII) are essential for facilitating travel arrangements and reservation management within RezDesk. PII elements such as name, date of birth, gender, email address, phone number, and passport details are required to ensure accurate booking, secure traveler identification, and compliance with travel regulations. This information enables seamless coordination with travel service providers, government agencies, and reservation systems, ensuring an efficient and secure travel experience for users.

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

No, RezDesk does not actively monitor or track the public, GSA employees, or contractors. The system is used solely for travel booking and reservation management and does not include any real-time tracking or monitoring of individuals. Any personal data collected is strictly for the purpose of facilitating travel arrangements and is handled in accordance with privacy and security best practices to minimize any impact on personal privacy.

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

RezDesk can generate reports related to individual travel arrangements and purchase history. These reports provide details such as itineraries, booking confirmations, travel expenses, and trip history to support travel management and compliance with government regulations.

RezDesk does not include any real-time tracking or cross-device monitoring capabilities. Access to reports is restricted based on role-based access controls (RBAC) to ensure that only authorized personnel can generate or view sensitive travel data. Audit logs track report access and generation to prevent misuse and ensure compliance with privacy and security policies.

2.4 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?

Reports generated within RezDesk are tailored based on client needs, requests, and contractual requirements. Depending on the use case, data within reports may be de-identified or aggregated to protect individual privacy.

- *De-Identification & Aggregation: When required, reports can be anonymized by removing personally identifiable information (PII) and aggregating data to prevent re-identification. This process may include replacing individual names with unique identifiers or summarizing travel trends at an organizational level.*
- *Access Controls: Only authorized personnel within ADTRAV and designated client representatives have access to these reports, as governed by role-based access control (RBAC) policies.*
- *Safeguards: Reports containing sensitive data follow encryption and secure transmission protocols to ensure protection. Additionally, audit logs track access and distribution to prevent unauthorized use.*

These measures ensure that reports provide valuable travel insights while maintaining data privacy and security.

SECTION 3.0 LIMITS ON USING AND SHARING INFORMATION

3.1 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?

RezDesk collects and retains only the minimum necessary information required to facilitate travel management and reservation processing. The data collected is limited to what is explicitly needed for booking, itinerary management, and compliance with travel regulations.

To ensure that PII is only used for its intended purpose:

- *RezDesk enforces strict access controls to prevent unauthorized use or disclosure.*

- *Data is not shared externally except with authorized travel service providers and government agencies required to coordinate and process travel arrangements.*
- *Regular security and privacy audits are conducted to verify compliance with data minimization and usage policies.*

These safeguards ensure that the collection and use of PII remain aligned with the purpose for which it was gathered, maintaining privacy and regulatory compliance.

3.2 Will the information be shared with other individuals, federal and/or state agencies, private-sector organizations, foreign governments and/ other entities (e.g. nonprofits, trade associations)? If so, how will the vendor share the information?

Information stored within RezDesk is shared only with service providers identified and authorized within this security package, or identified through ETSNext approved providers, to facilitate travel booking and management for government employees. These entities receive only the necessary data required to process travel arrangements in compliance with federal travel regulations. No information is shared with unauthorized individuals, private-sector organizations, foreign governments, or other external entities.

3.3 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 primarily obtained through automated data feeds from the client via secure methods such as API or SFTP. However, in certain cases, individuals may directly enter or update their own information within the RezDesk platform as needed to ensure accuracy and completeness of their travel records.

SECTION 4.0 DATA QUALITY AND INTEGRITY

4.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

RezDesk ensures the accuracy and completeness of collected information through a combination of technical validation, automated checks, and user verification processes.

- *Input Validation: Data entered directly into the platform undergoes basic input validation to minimize errors and ensure required fields are completed correctly.*

- *Automated Data Processing: Information received through automated methods (such as API or SFTP feeds from ETSNext providers) is validated upon import. Records with*

missing or incomplete traveler profile data are flagged for review or rejected to maintain data integrity.

- *User Verification: Travelers and authorized personnel have the ability to review and update their profiles, ensuring personal information remains current and accurate.*
- *Data Integrity Policies: Regular audits and reconciliation processes help maintain data accuracy and detect inconsistencies.*

These measures ensure that all traveler information remains reliable, complete, and up to date to support seamless travel management.

SECTION 5.0 SECURITY

5.1 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 data within the RezDesk system is strictly limited to authorized ADTRAV employees who have received prior approval. ADTRAV enforces access controls by defining user roles, group memberships, and specific access authorizations (i.e., privileges) based on job responsibilities. The system follows the principle of least privilege through Role-Based Access Control (RBAC), ensuring that users only have the minimum level of access necessary to perform their assigned tasks. Access requests undergo a formal approval process to maintain security and compliance with relevant policies and regulations.

5.2 Has a System Security and Privacy Plan (SSPP) been completed for the information system(s) or application?

The System Security Plan (SSP) for RezDesk was previously updated and approved in April 2024 for the Office of the Comptroller of Currency authorization. The SSPP was recently updated on January 14, 2026 to integrate additional controls required by the General Services Administration (GSA) to ensure continued compliance with evolving security and privacy requirements.

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

RezDesk is secured through a multi-layered approach that incorporates physical, technical, and managerial controls to protect data and ensure compliance with security best practices.

- *Physical Security: Access to ADTRAV's data center is restricted using multiple security zones, requiring electronic key cards for entry. Only authorized personnel, such as network administrators, security engineers, and executive leadership, can access critical infrastructure areas. Surveillance systems (CCTV) and alarm monitoring provide 24/7 oversight. The data center is supported by redundant power systems, including an N+1 uninterruptible power supply (UPS) and a natural gas-powered generator for continuity in case of power failure.*

- *Technical Security: RezDesk employs user identification and authentication controls, including role-based access control (RBAC) and multi-factor authentication (MFA) for privileged accounts. Sensitive data, including Personally Identifiable Information (PII) and Payment Card Industry (PCI) data, is encrypted in transit and at rest using industry standard encryption protocols. Network segmentation isolates sensitive systems to minimize risk, and firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint security tools help prevent unauthorized access.*

- *Managerial Security: ADTRAV enforces security policies through periodic security audits, continuous monitoring of user activity, and regular vulnerability assessments. Employees receive mandatory security awareness training upon hire and quarterly thereafter, including phishing simulations and updated threat awareness content. Data backups are conducted regularly using SAN snapshots, Veeam backups, and Zerto replication, ensuring disaster recovery and business continuity.*

These security measures align with federal and industry regulations, ensuring the confidentiality, integrity, and availability of RezDesk data.

5.4 What mechanisms are in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

ADTRAV has a comprehensive Incident Response Plan (IRP) that outlines procedures for identifying, reporting, and mitigating security incidents, including breaches involving Personally Identifiable Information (PII).

- *Incident Detection & Reporting: Security monitoring tools continuously track system activity for anomalies. Employees are trained to recognize and report potential security incidents through established escalation procedures.*

- *Incident Response & Mitigation: A dedicated incident response team follows a structured process to assess, contain, and mitigate incidents. If a PII breach occurs, ADTRAV follows notification protocols in compliance with regulatory and contractual obligations.*
- *Forensic Investigation & Remediation: Third-party cybersecurity experts are available to assist with forensic investigations when necessary. Root cause analysis is conducted to implement corrective actions and prevent recurrence.*

  ADTRAV leverages WebCheckSecurity for virtual CISO services. This organization also has security experts that are available for forensic investigation if needed.

- *Training & Exercises: Regular incident response drills and tabletop exercises ensure personnel are prepared to handle security incidents effectively. Employees receive ongoing security awareness training to reinforce best practices for identifying and responding to threats.*

These mechanisms ensure a swift and effective response to security incidents, minimizing risks and protecting sensitive data.

ADTRAV follows notification protocols aligned with applicable federal laws, regulations, and agency contracts. In the event of a confirmed or suspected PII breach, designated authorities—including the affected agency—are notified in accordance with regulatory timelines, typically within 48 hours for confirmed incidents involving federal systems. Notifications include key details such as the nature of the breach, data affected, scope of impact, and actions taken for containment and remediation, following NIST and US-CERT guidelines.

SECTION 6.0 INDIVIDUAL PARTICIPATION

6.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

Basic traveler information is provided by the Federal Agency as part of the travel management process. Travelers cannot opt out of providing the minimum required information necessary for booking and managing travel arrangements (e.g., name, contact details, and travel credentials).

However, travelers have the option to opt-in or opt-out of providing any additional information beyond the required profile data. This may include preferences, frequent traveler numbers, or optional contact details to enhance their travel experience.

Consent for the collection and use of information is typically obtained during profile setup and system usage, with clear notifications about data usage and privacy protections.

6.2 What procedures allow individuals to access their information?

Procedures for accessing personal information depend on the ETSNext implementation and configuration. In most cases, individuals can access their travel profile through the ETSNext platform, where they can review and update their personal information as needed.

Additionally, some implementations may allow travelers to access and manage their profiles directly within the RezDesk platform. Access is controlled through secure authentication methods, ensuring only authorized users can view or modify their information.

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

The ability for individuals to amend their information depends on the ETSNext implementation and configuration. Typically, travelers can update their profiles through the ETSNext platform, where they can correct or modify personal details as needed.

In some cases, individuals may also have the ability to update their profiles directly within the RezDesk platform. Access to profile management is secured through authentication controls, and any critical changes may require verification or approval to maintain data integrity.

SECTION 7.0 AWARENESS AND TRAINING

7.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

All ADTRAV employees are required to complete privacy and security training to ensure proper handling of sensitive data, including Personally Identifiable Information (PII).

- *General Training: All staff undergo annual privacy and security awareness training, which covers data protection best practices, regulatory requirements, and incident reporting procedures.*

- *Role-Based Training: Employees with elevated access, such as developers and IT staff, receive additional training tailored to their roles, focusing on secure coding practices, data handling, and system security controls.*

- *Learning Management System (LMS): Training is managed and tracked through ADTRAV's InfoSec IQ LMS platform, ensuring completion is documented and compliance requirements are met.*

- *Ongoing Education: Quarterly updates, phishing simulations, and refresher courses help reinforce security awareness and keep employees informed of emerging threats.*

These training programs help ensure that all users of the system understand their responsibilities in protecting sensitive information and maintaining data privacy.

SECTION 8.0 ACCOUNTABILITY AND AUDITING

8.1 How does the system owner ensure that the information is only being used according to the stated practices in this PIA?

ADTRAV ensures that information within RezDesk is used strictly in accordance with the stated practices in this Privacy Impact Assessment (PIA) through a combination of auditing measures, technical safeguards, and policy controls:

- *Access Reviews: ADTRAV conducts ongoing access reviews to ensure that only authorized personnel have the appropriate level of access to sensitive information.*
- *Data Loss Prevention (DLP): DLP systems monitor and prevent unauthorized transmission of sensitive data, ensuring compliance with security policies.*
- *Access Controls & Restrictions: Role-Based Access Control (RBAC) ensures that users only have the minimum necessary access to perform their duties. Read-only access is enforced where applicable to prevent unauthorized modifications.*
- *Auditing & Monitoring: System logs track user activities, access events, and data interactions, which are subject to regular audits by internal teams and third-party assessors when required.*
- *Information Sharing Protocols: Data sharing is restricted to authorized entities per contractual agreements and regulatory compliance requirements.*

These safeguards help maintain data integrity, security, and compliance, ensuring that RezDesk operates in alignment with its privacy and security commitments.

Certificate Of Completion

Envelope Id: DFF0E88D-C311-42C0-833D-D1BFD3223456
Subject: Complete with Docusign: ADTRAV - RezDesk PIA.pdf
Source Envelope:
Document Pages: 17
Certificate Pages: 2
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London

Signatures: 4
Initials: 0

Status: Completed

Envelope Originator:
Tiwalade Adebanjo
1800F F St NW
Washington DC, DC 20405
tiwalade.adebanjo@gsa.gov
IP Address: 136.226.20.187

Record Tracking

Status: Original
1/16/2026 5:31:54 PM
Security Appliance Status: Connected
Storage Appliance Status: Connected

Holder: Tiwalade Adebanjo
tiwalade.adebanjo@gsa.gov
Pool: FedRamp
Pool: US General Services Administration

Location: DocuSign

Location: Docusign

Signer Events	Signature	Timestamp
Arpan Patel arpan.patel@gsa.gov IT Specialist US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Arpan Patel 8B059AABDAF1477... Signature Adoption: Pre-selected Style Using IP Address: 136.226.18.192	Sent: 1/16/2026 6:03:10 PM Viewed: 1/16/2026 6:04:29 PM Signed: 1/16/2026 6:04:43 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Jason Cross jason.cross@gsa.gov CO US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Jason Cross B793E8ECC5264E9... Signature Adoption: Pre-selected Style Using IP Address: 136.226.18.203	Sent: 1/16/2026 6:03:11 PM Viewed: 1/20/2026 10:59:19 AM Signed: 1/20/2026 10:59:35 AM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Michael Salter michael.salter@gsa.gov Program Analyst US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Michael Salter ABA02A5B3FBB446... Signature Adoption: Pre-selected Style Using IP Address: 136.226.20.183	Sent: 1/16/2026 6:03:11 PM Viewed: 1/16/2026 6:24:33 PM Signed: 1/16/2026 6:24:39 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Richard Speidel richard.speidel@gsa.gov Chief Privacy Officer US General Services Administration Security Level: Email, Account Authentication (None)	DocuSigned by: Richard Speidel 171D5411183F40A... Signature Adoption: Pre-selected Style Using IP Address: 136.226.19.76	Sent: 1/16/2026 6:03:11 PM Viewed: 1/16/2026 6:10:17 PM Signed: 1/16/2026 6:10:22 PM
Electronic Record and Signature Disclosure: Not Offered via Docusign		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	1/16/2026 6:03:11 PM
Certified Delivered	Security Checked	1/16/2026 6:10:17 PM
Signing Complete	Security Checked	1/16/2026 6:10:22 PM
Completed	Security Checked	1/20/2026 10:59:35 AM

Payment Events	Status	Timestamps