



Omega World Travel -PIA

Privacy Impact Assessment (PIA) - Guidance

POINT of CONTACT

privacy.office@gsa.gov

Instructions for GSA vendors:

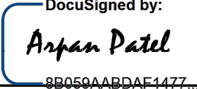
This guidance is designed for nonfederal systems described in the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-171, "[Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#)" and NIST SP 800-172, "[Enhanced Security Requirements 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

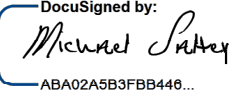
The GSA representatives listed below have reviewed the information provided by the vendor for completeness.

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

X  10/5/2026 | 22:38:11 BST
8B050AABDAF3477...

GSA Information System Security Manager

Michael Salter, GSA Program Manager:

X  10/13/2026 | 13:59:46 BST
ABA02A5B3FBB446...

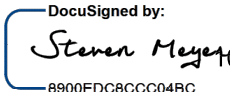
GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

X  10/6/2026 | 13:54:00 BST
171D5411183F40A...

GSA Chief Privacy Officer

Steven Meyer, GSA Contracting Officer Representative (COR):

X  10/6/2026 | 10:42:45 BST
8900EDC8CCC04BC...

GSA Contracting Officer Representative

800-171 PIA Template Document Revision History

Date	Description	Version of Template
5/27/2026	Initial Draft of Non-Federal System	1.6
4/14/2026	Review No Change	1.7
9/29/2026	Privacy Office revision approved	1.8

Table of Contents

Document purpose	1
Overview	1
SECTION 1.0 OPENNESS AND TRANSPARENCY	3
SECTION 2.0 DATA MINIMIZATION	3
SECTION 3.0 LIMITS ON USING AND SHARING INFORMATION	4
SECTION 4.0 DATA QUALITY AND INTEGRITY	5
SECTION 5.0 SECURITY	6
SECTION 6.0 INDIVIDUAL PARTICIPATION	11
SECTION 7.0 AWARENESS AND TRAINING	13
SECTION 8.0 ACCOUNTABILITY AND AUDITING	13

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 information¹ 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:

Omega World Travel

B. GSA Client:

Omega World Travel

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

Travelers requesting travel bookings

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

Address, Name, Date of Birth, Age, Gender, Address, Telephone Number, Email address, Passport Number or other government issued identifiers or images of documents, form of payment.

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."

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

The purpose is to provide travel for our clients. Our data regulations and storage are as such:

AWS Platform: As per IRS regulations, our data retention policy enforces a seven-year storage period for all data residing in our AWS infrastructure. Upon expiration of this retention period, data is securely disposed of leveraging native Amazon Web Services deletion functionalities. This includes the deletion of objects from S3 buckets and the execution of DELETE commands for records within our SQL database. We rely on the robust, inherent security mechanisms built into the AWS infrastructure to ensure the secure reclamation of storage space post-deletion.

On-Premises: Formal data disposal procedure is in place, managed by a certified third-party vendor. This vendor conducts annual on-site data disposal services strictly adhering to the guidelines outlined in NIST Special Publication 800-88 for media sanitization. Following their documented procedures, which ensure data is rendered unrecoverable, the vendor provides a certificate of destruction upon completion of the disposal process.

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.

2.5.5. Privacy and Personal Data Protection (as per Omega IT Security Policy v1.0)

Our commitment to safeguarding traveler privacy and personal data is paramount. We adhere to applicable data protection regulations and align our practices with established frameworks, including principles from the NIST Privacy Framework and relevant controls within NIST Special Publication 800-53. Comprehensive details regarding our data handling practices are readily available to travelers in our Privacy Policy, accessible on our website at <https://omegatravel.com/about-us-privacy-policy/>.

Informing Travelers and Obtaining Consent: Travelers are informed about our data handling practices through this readily accessible Privacy Policy and through clear consent agreements presented at key data collection points. These resources detail the types of personal data processed, the purposes of processing, data retention periods, potential data sharing, and the rights afforded to travelers

Storage of Traveler Acknowledgements: To maintain a verifiable record of compliance, Omega securely stores traveler acknowledgements of our privacy policies and consent agreements. These records, including the policy version and timestamp of acceptance, are associated with individual traveler profiles using unique identifiers within our database.

SECTION 2.0 DATA MINIMIZATION

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

Travel Reservations cannot be made without the minimum PII information.

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

Location and monitoring are not performed on the traveler.

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

We do not track the location of travelers. We do have their itineraries but cannot tell if they actually boarded a flight or are staying at a particular location.

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?

We employ AWS volume-based encryption to protect data at rest on our storage volumes. This robust encryption utilizes the AES-256-XTS algorithm, a strong industry standard, to encrypt the underlying data.

Additionally, within the database tables containing PCI data, we implement credit card masking. This technique ensures that only the last four digits of a credit card number are visible, with the remainder of the number obscured. This serves as an additional layer of security for sensitive information when it is accessed or displayed, preventing full credit card numbers from being exposed.

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?

Only the minimum PII information needed to make a travel reservation is collected and it is not used for any other purposes like marketing or business development.

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 will be shared only upon request from GSA or the agency.

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)?

We prioritize the security of traveler information. All data is collected exclusively through our secure booking and reservation tool, which is accessed via a secure web interface.

Travelers are empowered to create their own profiles and directly input all personal and booking-related data. This ensures the accuracy and integrity of the information provided.

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

We use Cornerstone (Quality control and automation Platform) which plays a vital role in ensuring data accuracy and allows for necessary edits before a reservation is finalized, directly addressing the concern of travelers facing delays at check-in.

Cornerstone provides a centralized platform where traveler data, input during the booking process through our web interface, can be reviewed and managed. This enables several key steps to ensure accuracy:

- Pre-Confirmation Review: Before a reservation is confirmed, Cornerstone allows either the traveler or an authorized agent to review all the entered details, including names, dates of birth, passport information (if collected), and other critical data required for travel.*
- Data Validation within Cornerstone: Cornerstone is equipped with validation rules that can flag potential errors or inconsistencies in the entered data. For example, it can check for incorrect date formats, missing mandatory fields, or mismatches in name fields. These validations can prompt the user or agent to correct the information before the booking is finalized.*
- Editing Capabilities: Cornerstone provides the functionality to directly edit any incorrect or incomplete information identified during the review process. This ensures that the reservation details are accurate and match the traveler's official documents.*
- Integration with External Systems (Potential): Depending on how Cornerstone is integrated with airline or other travel provider systems, it may also facilitate a preliminary check against their requirements. This could help identify potential issues early on.*

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?

We have a well-defined authorization process to grant access to our systems, ensuring stringent security and compliance with relevant policies and regulations.

The process for gaining access involves a formal approval workflow:

1. Access Request: An individual requiring access initiates a request through our designated ticket system. This ensures a documented and auditable trail of all access requests. Additionally, an email process is in place: the request is sent to the supervisor for approval. Once approved, the IT department grants the necessary access to the requester.

2. Approval Routing: The access request is automatically routed to the concerned person for authorization. This is typically the individual's manager, the Chief Technology Officer (CTO), or the Operations Manager, depending on the system or data being requested and established roles and responsibilities.

3. Review and Approval: The designated approver reviews the access request, considering the requester's role, responsibilities, and the principle of "need to know." Approval is granted only if the access is deemed necessary for the individual to perform their job duties effectively and aligns with our security policies and regulatory requirements.

4. Access Provisioning: Upon receiving formal approval within the ticket system, our IT team proceeds to provision the necessary access. This is done according to the principle of least privilege, granting only the minimum level of access required to fulfill the user's responsibilities.

5. Access Monitoring and Review: Access privileges are periodically reviewed to ensure they remain appropriate and necessary. This helps maintain compliance and reduces the risk of unnecessary access over time.

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

Yes and updated last 09/21/2026 by the security and technology team in coordination with a 3PAO.

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

The data is in systems that are in Amazon Web Services (AWS), which has the “rules of least privilege” and passwords with multi-factor authentication, encryption at rest and in transit. The systems are subject to access controls, regular security audits and penetration tests, compliant with NIST-800-171 and NIST-800-53 guidelines. Data is backed up and subject to yearly Disaster Recovery drills.

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?

We Confirm SIEM tool in use, We currently utilize Wazuh as our primary Security Information and Event Management (SIEM) tool. Wazuh provides comprehensive capabilities for log data analysis, intrusion detection, vulnerability management, and continuous security monitoring across our infrastructure.

What Incident Response Plan is in place?

Omega World Travel has a comprehensive Incident Response Plan (IRP) in place, detailed within its Incident Management Procedure (Section 1 of our policy Omega Procedures). The plan is designed to ensure the swift and effective handling of security and privacy incidents, aiming to minimize operational disruptions, protect sensitive data, and meet all legal and regulatory requirements.

The plan applies to all employees, contractors, systems, and data across the organization, encompassing cybersecurity breaches, privacy violations, data leaks, and other operational security incidents.

Key aspects of Omega's Incident Response Plan include:

- *Structured Phases: The plan follows a lifecycle approach, clearly outlining steps from incident detection to post-incident review and continuous improvement.*
- *Defined Roles and Responsibilities: A dedicated Incident Response Team (IRT) is established for coordination, management, investigation, containment, and recovery. The Information Security Manager oversees the process, while the Legal and Compliance Team ensures regulatory adherence and notification. HR and managers play roles in reporting and training.*
- *Comprehensive Detection Methods: Incidents are detected through a combination of automated security monitoring tools (such as SIEM systems like Wazuh, IDS/IPS, and network traffic analysis) and employee reporting via established channels. External notifications from third parties can also trigger a response.*
- *Immediate Reporting and Classification: There's a strict policy for immediate reporting of all suspected incidents. Incidents are then classified and prioritized into Critical, High, Medium, or Low categories based on factors like data exposure, operational disruption, and affected individuals, informing the urgency of the response.*
- **Clear Response Steps:**
 - *Containment: Focuses on immediate isolation of compromised systems and long-term measures like patching to prevent further harm.*
 - *Investigation: Involves thorough root cause analysis, forensic data collection from logs and systems, and interdepartmental collaboration.*
 - *Eradication and Recovery: Aims to eliminate threats (malware, vulnerabilities) and restore systems and services from backups after verification of cleanliness.*
- *Structured Communication and Notification: The plan dictates internal communication within the IRT and to senior management, as well as external notifications to data protection authorities and affected individuals when personal data breaches occur, adhering to legal mandates.*

- *Continuous Improvement: A crucial component involves post-incident reviews ("Lessons Learned Meetings") to identify process failures and areas for improvement. This leads to policy and process updates, regular training and awareness for employees, and annual incident drills to test organizational readiness.*
- *Record Keeping and Compliance: Detailed incident logs are maintained throughout the lifecycle for all incidents, ensuring secure storage and compliance with retention policies.*
- *Testing and Simulation: The plan emphasizes regular simulated incident response drills to proactively assess the organization's readiness and refine procedures based on review and analysis of test results.*

This structured approach ensures that Omega World Travel is prepared to respond effectively to a wide range of security and privacy incidents, mitigating impact and continuously strengthening its security posture.

What are your notification protocols, response timelines/thresholds?

Notification Protocols:

Our notification protocols are tiered based on the determined severity of the detected incident:

- *Internal Security Team: For all Wazuh-generated alerts and confirmed incidents, our primary security operations team is immediately notified via our internal alerting system and ticketing platform, Mojo Helpdesk.*
- *Management & Stakeholders: For Critical (Severity 1) or High (Severity 2) incidents, relevant management (including the Incident Response Team (IRT), Information Security Manager, and CTO) and business unit stakeholders are informed through secure communication channels (e.g., encrypted email, dedicated communication tools) within specific timeframes as outlined in our response timelines below.*
- *Legal & Compliance: In cases involving data breaches or regulatory implications, our legal and compliance teams are notified promptly to assess and ensure adherence to all reporting obligations.*

- *External Parties: If required by law or contract (e.g., confirmed customer data compromise), affected external parties will be notified in accordance with our legal and regulatory obligations and within mandated timeframes.*

Response Timelines and Thresholds:

Our response timelines and thresholds are directly defined by the incident's severity:

- *Critical (Severity 1): Incidents causing significant operational disruption or confirmed data breach.*
 - *Detection & Initial Triage: Within 15 minutes.*
 - *Containment: Within 1 hour.*
 - *Notification to Management: Within 30 minutes of confirmation.*
- *High (Severity 2): Incidents causing localized service degradation or potential data exposure.*
 - *Detection & Initial Triage: Within 30 minutes.*
 - *Containment: Within 2 hours.*
 - *Notification to Management: Within 1 hour of confirmation.*
- *Medium (Severity 3): Incidents with moderate impact, such as policy violations or successful but non-critical exploits.*
 - *Detection & Initial Triage: Within 1 hour.*
 - *Containment: Within 4 hours.*
 - *Notification to Management: Within 2 hours of confirmation (if relevant).*

- *Low (Severity 4): Minor security events, informational alerts, or confirmed false positives.*
- *Detection & Initial Triage: Within 4 hours.*
- *Containment: Within 8 hours (if required).*
- *Notification to Management: Addressed in routine security reports.*

These established timelines are regularly reviewed and updated to reflect our evolving threat landscape, operational capabilities, and ensure continuous improvement of our incident response posture.

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.

We ensure transparency and provide opportunities for travelers to manage their data provision, primarily differentiating between information that is mandatory for service fulfillment and information that may be optional.

1. During Online Booking:

- *Explicit Consent for Essential Information: When a traveler initiates an online booking, they are presented with fields for essential information required to complete the travel reservation (e.g., name, contact details, payment information, passport details where applicable). Our booking flow is designed such that submission of this information and proceeding with the booking process implies consent for its collection and use solely for the purpose of making or facilitating the travel reservation.*
- *No Opt-Out for Essential Data: For these mandatory fields, there is no direct "decline" or "opt-out" mechanism if the traveler wishes to complete the reservation. If a traveler chooses not to provide this minimum required information, they will be unable to complete the booking, as this data is fundamental to securing their travel arrangements (e.g., a flight cannot be booked*

without a name). The system will prompt them for missing information before allowing them to proceed.

- *Privacy Policy & Terms of Service: Prior to finalizing any booking, travelers are required to acknowledge and often explicitly agree to our Privacy Policy and Terms of Service (via a checkbox or similar mechanism). These documents clearly outline how their data is collected, used, stored, and protected. This serves as a primary form of explicit consent for our overall data handling practices.*
- *Opt-In/Out for Non-Essential Data (e.g., Marketing): While not directly related to the booking itself, any opportunities for providing optional information (e.g., preferences for future marketing communications, newsletter subscriptions) would be presented with clear opt-in checkboxes. Travelers would have the explicit choice to consent or decline for these specific, non-essential uses. Currently, as stated, we do not use collected travel reservation information for marketing or business development purposes, meaning there's no "opt-in" for that specific use case for the data collected for the reservation.*

2. During Inbound Calls (Travel Reservation):

- *Verbal Consent & Purpose Explanation: When a traveler makes an inbound call to our reservation agents, the agent will clearly state the purpose of collecting necessary personal and payment information: to facilitate the requested travel reservation. By verbally providing the information, the traveler is implicitly consenting to its use for that specific purpose.*
- *Opportunity to Decline for Essential Data: Similar to online booking, if a traveler declines to provide essential information (e.g., full name, payment details, contact number), the agent will explain that the reservation cannot be completed without this data. The traveler has the choice to end the call or not provide the information, effectively declining the service.*
- *Data Minimization Confirmation: Agents are trained to only request the minimum information required for the specific reservation. If a traveler asks why certain information is needed, the agent will explain its necessity for the booking.*

6.2 What procedures allow individuals to access their information?

Individuals could request their itineraries via email, on the company's website, or by making calls to the call center or via the online booking tool.

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

The individuals can change the information about themselves in the travel profile maintained in the systems if they have access to it. If they do not have access the change can be made by calling the travel agent.

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.

Omega World Travel training is powered by Thinkzoom, with Business skills and Compliance training provided by HSI. Cybersecurity Training occurs annually every Fall. Mandatory HR training is conducted annually in the summer. New Hire Training programs include mandatory HR and Cyber Security training at the time of hire. Other training programs include industry and software-specific training applicable to the duties of the trainee.

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?

The systems are hosted in Amazon Web Services (AWS) and we have deployed 24x7x365 SIEM Monitoring, Digital Leak Protection (DLP), Multi-Factor authentication, upgrading to supported protocols, yearly penetration testing, weekly Application Security Vulnerability scans, regular review of access lists. Regular compliance checks to the NIST 800-0171, NIST 800-53, PCI-DSS, HIPAA standards are performed.