GSA

Uber for Business (U4B): U4B Travel, Uber Health, & Uber Central

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):

DocuSigned by:

X *Arpan Patel*

—8B059AABDAF1477...

GSA Information System Security Manager

Rebecca Bond, GSA Program Manager:

DocuSigned by:

X *Rebecca Bond*

—A25CBC38B2274C2

GSA Program Manager

Richard Speidel, GSA Chief Privacy Officer (CPO):

DocuSigned by:

X *Richard Speidel*

—171D5411183F40A...

GSA Chief Privacy Officer

Lamarr Peppers, GSA Contracting Officer Representative (COR):

DocuSigned by:

X *Lamarr Peppers*

—71C93F9286CF415...

GSA Contracting Officer Representative

800-171 PIA Template Document Revision History

Date	Description	Version of Template
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
5/27/2022	Formatting and editing	1.4
5/31/2023	Vendor updated PIA to PIA Template Version 1.4	1.4
10/05/2023	Vendor updated the following sections of the PIA to include Uber Health specific verbiage: Section 1.1, Section 2.1, Section 3.3, and Section 6.1	1.4
12/15/2023	Vendor appended Document Revision History Table, defined acronyms and updated language for clarity	1.4
01/10/2024	GSA accepted Vendor revisions and approved PIA for 2023 Submission	1.4
05/20/2024	Vendor reviewed PIA and updated product names: Cover page, System Overview, and Section 5 for clarity and conciseness.	1.4
09/24/2024	Added note that GSA does not currently use the Uber Health dashboard to section E	1.5
4/17/2025	Formatting and editing	1.6

Table of Contents

          Version 1.6: 4-17-2025

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 Privacy Impact Assessment (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:

Uber for Business: U4B Travel, Uber Health, & Uber Central (U4B, UH, UC)

B. GSA Client:

Federal Acquisition Services (Q) - Ride Sharing Program

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

Individuals / federal employees who request or receive transportation through their enterprise profile on the Uber Application (Uber App), including those who receive transportation requested by a federal employee through Uber Central.

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

● Contact information: federal employee name, email address, phone number

● Agency information: agency name, agency ID (agency identification number)

● Payment method: exempli gratia (e.g.), Mastercard, Visa

---

[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."

- Trip Information: selected vehicle option, e.g., Uber X, Uber Black, transaction date, time, amount, type of fare, id est (i.e.), fare or tip, taxes, currency, fees, pick-up and drop-off address, city, distance, duration

- Other: date/time stamps of report, and optional categories including federal employee identification - (federal employee ID), expense code and memo

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

Uber for Business (U4B)[2] provides web-based solutions that leverage Uber's ride-hailing services on the Uber platform. Provisioned agency administrators can configure a solution from the U4B administrative dashboard (Dashboard) that meets the agency's needs by adding authorized federal employees, managing permissions, setting payment options, and spending limits.

For purposes of this PIA, U4B includes the following:

U4B Travel: the Uber for Business product that, in connection with Uber's technology systems, enables an agency's authorized federal employees to request on-demand ground transportation which an agency can manage through the Dashboard.

- For riders (federal employees): The U4B Travel product will surface as a billing option via an enterprise profile in the Uber rider app. This billing option enables federal employees to report expenses related to business trips to their employer automatically, for example by integrating with their employer's expense reporting system.

- For agency administrators: Within the Dashboard, federal employee administrators will have access to expense reporting related to business trips taken using the business profile in the Uber rider app for reporting, expensing, and controlling features. Below are data categories that are viewable in the U4B Dashboard. Note: The Dashboard does not surface trip data related to a federal employee's personal profile.

  - Contact information: federal employee name, agency email address
  - Agency information: agency name, agency ID

---

[2] Uber for Business is a platform for managing global rides. Drivers may choose to install and use video cameras, dash cams, or other recording devices to record rides or otherwise for the purpose of fulfilling transportation services. Local law or regulations may require individuals using recording equipment in vehicles to fully disclose to Riders that they are being recorded in or around a vehicle and obtain consent. See Uber's Community Guidelines for more information.
https://www.uber.com/legal/en/document/?name=general-community-guidelines&country=united-states&lang=en

Version 1.6: 4-17-2025

- Payment method: e.g., Mastercard, Visa
- Trip Information: selected vehicle option, e.g., Uber X, Uber Black, transaction date, time, amount, type of fare, i.e., fare or tip, taxes, currency, fees, pick-up and drop-off address, city, distance, duration
- Other: date/time stamps of report, and optional categories including federal employee ID, expense code and memo

An agency provides Uber the federal employee's first name, last name, and email address ("Linking Data"). These data elements are necessary for authentication and verification purposes to enable a federal employee to securely establish an enterprise profile within the Uber app. Federal employees consent to sharing trip information with the agency that provisioned the access any time they take trips using their enterprise profile. Rides taken on a federal employee's enterprise profile will be billed directly to the agency's enterprise account. Federal employees may toggle between using their enterprise profile and personal profile at any time. Agency administrators can view trips on the U4B dashboard and have visibility into trip information in one place, streamlining receipt and approval tracking.

A federal employee's enterprise profile may be unlinked from his or her Uber account at any time by deleting the enterprise profile option from his or her Uber Rider account. In addition, an agency may, at any time, unlink a federal employee's Uber account from the enterprise account through the U4B Dashboard.

Uber Central: Enables agency administrators to arrange and pay for Uber rides on behalf of federal employees who don't need access to a smartphone or the Uber app.

- For riders (federal employees): Riders that don't require access to a smartphone or the Uber app will receive trip information, such as driver ETA (estimated time of arrival), via text message or automated call.

- For agency administrators: For agency administrators to arrange Uber rides on behalf of others, agency administrators must input the rider's name, phone number, and pickup and dropoff address in the Dashboard. The information viewable in the Dashboard include[3]:

---

[3] Driver information is also viewable on the Dashboard, which includes: driver real-time location, photo, first name, vehicle license plate number, and type of vehicle.

- ○ Contact information: rider name and phone number (provided by the agency administrator)
- ○ Post-Trip Information: selected vehicle option, e.g., Uber X, Uber Black, transaction date, time, amount, type of fare, i.e., fare or tip, taxes, currency, fees, pick-up and drop-off address, city, distance, duration
- ○ Other: date/time stamps of report, and optional categories including expense code and memo

Uber Health is a web-based portal (Uber Health Dashboard) that enables Healthcare organizations to seamlessly coordinate rides for those in need (i.e. patients, members and caregivers). The passenger is contacted by text or call with their trip details at the time the ride is booked and when a driver is on the way to pick up the passenger.

Uber Health offers a HIPAA-enabled environment that protects patients' information while coordinating rides. The Uber Health Dashboard was specifically designed to meet healthcare's Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards.

- ● For riders/patients: Riders/Patients that don't require access to a smartphone or the Uber app will receive trip information, such as driver ETA, via text message or automated call.

- ● For Uber Health administrators: For administrators to arrange Uber rides on behalf of others, administrators must input the rider/patient's name, phone number, and pickup and dropoff address in the Dashboard. The information viewable in the Dashboard include[3]:

    - ○ Contact information: rider/patient name and phone number (provided by the administrator)
    - ○ Post-Trip Information: selected vehicle option, e.g., Uber X, Uber Black, transaction date, time, amount, type of fare, i.e., fare or tip, taxes, currency, fees, pick-up and drop-off address, city, distance, duration
    - ○ Other: date/time stamps of report, and optional categories including expense code and memo

Note: GSA currently does not use the Uber Health Dashboard.

Version 1.6: 4-17-2025

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.

U4B Travel: Yes. An authorized federal employee will receive an email invitation that includes Uber's Terms and Privacy Notice https://privacy.uber.com/policy/. Accepting the invite will enable the federal employee to establish an enterprise profile linked to their Uber account. Federal employees consent to sharing trip information with the agency that provisioned the access any time they take trips using their enterprise profile. Federal employees may toggle between using their enterprise profile and personal profile at any time. Federal employees may unlink their enterprise profile from their personal Uber accounts at any time by deleting the enterprise profile option. Note: The Dashboard does not surface trip data related to a federal employee's personal profile.

Uber Central: Yes. Federal employees that don't require access to a smartphone or the Uber app will receive a text message that includes a link to Uber's Privacy Notice and the following message: {Agency} set up a ride with Uber for you. By taking this ride, you agree to Uber's terms which you can find with the privacy notice at uber.com/terms. {Agency} will be able to view the progress of your ride."

Uber Health: Yes. Riders/Patients that don't require access to a smartphone or the Uber app will receive a text message that includes a link to Uber's Privacy Notice and the following message: "{Agency} set up a ride with Uber for you. By taking this ride, you agree to Uber's terms which you can find with the privacy notice at uber.com/terms. {Agency} will be able to view the progress of your ride."

SECTION 2.0 DATA MINIMIZATION

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

U4B Travel: The federal employee's first name, last name, and email address are necessary for authentication and verification purposes to enable a federal employee to securely establish an enterprise profile within the Uber app and to link the federal employee's rider account with his or her enterprise account so that the federal employee can bill rides directly to the agency.

Uber Central: For agency administrators to arrange Uber rides on behalf of federal employees, agency administrators must input the rider's name, phone number, and pickup and dropoff address in the U4B Dashboard.

Uber Health: For administrators to arrange Uber rides on behalf of riders/patients, administrators must input the rider/patient's name, phone number, and pickup and dropoff address in the U4B Dashboard.

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

A federal employee's trip information, such as pick up and drop off addresses, will be viewable within the U4B Dashboard for trips taken using their enterprise profile. In addition, agency administrators have the ability to set policies for usage on a managed agency business profile based on spending allowance, trip allowance, time of day/week, and vehicle type. Agency administrators may also set geofence restrictions to help ensure that subsidies are supporting the agency's trips for which they are intended. Once parameters are set, the trip cannot occur outside the parameters. Federal employees can toggle using their enterprise account and personal account any time. Note: The Dashboard does not surface trip data related to a federal employee's personal profile.

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

Agency administrators with appropriate permissions can access the U4B Dashboard and generate reports that help provide visibility into agency-sponsored trips. The information below is viewable by agency administrators on the U4B Dashboard.

- Contact information: Federal employee name, email address, phone number (Uber Central)
- Agency information: agency name, agency ID
- Payment method: e.g., Mastercard, Visa
- Trip Information: selected vehicle option, e.g., Uber X, Uber Black, transaction date, time, amount, type of fare, i.e., fare or tip, taxes, currency, fees, pick-up and drop-off address, city, distance, duration
- Other: date/time stamps of report, and optional categories including federal employee ID, expense code and memo

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?

Trip reports include: Trip ID, Transaction Timestamp, Request Date, Request Time, Request Date (Local), Request Time (Local), Drop-off Date, Drop-off Time, Drop-off Date (Local), Drop-off Time (Local), First Name, Last Name, Email, federal employee ID (if given by agency), Service City, Distance (mi), Duration (minutes), Pickup Address, Drop-off Address, Expense Code (if given by agency), Expense Memo (if given by agency), Invoices, Program Group (if given set agency), Payment Method, Transaction Type, Fare in Local Currency (excluding Taxes), Taxes in

Local Currency, Tip in Local Currency, Transaction Amount in Local Currency (including Taxes), Local Currency Code Fare in United States Dollar (USD) (excl. Taxes), Taxes in USD Tip in USD, Transaction Amount in USD (incl. Taxes), Estimated Service and Technology Fee (incl. Taxes, if any) in USD. This data will not be de-identified.

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?

Uber limits its use of rider information to the purposes described in Uber's Privacy Notice: https://privacy.uber.com/policy/. In addition, Uber contractually agrees that it may not sell or otherwise publicly disclose Linking Data (i.e., the approved list of federal employee names, and email addresses that will be allowed to use the agency's business profile) or use Linking Data for any purpose that is detrimental or harmful to the agency. Uber's purpose for processing Linking Data is to send a linking email, link the data to existing accounts, and enable account creation.

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?

An agency provides Uber the approved list of federal employee names and email addresses that will be allowed to bill trips to the agency's business profile, which Uber does not share with other third parties unless required by law and consistent with Uber's Privacy Notice. These data elements are necessary for authentication and verification purposes to enable a federal employee to securely establish an enterprise profile within the Uber app. Federal employees consent to sharing trip information with the agency that provisioned the access any time they take trips using their enterprise profile.

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)?

U4B Travel: Each agency will share "Linking Data" with Uber. Linking Data refers to the approved list of federal employee names and email addresses that is necessary for authentication and verification purposes to enable a federal employee to securely establish an enterprise profile within the Uber app so that the federal employee can bill rides directly to the agency.

Uber Central: For agency administrators to arrange Uber rides on behalf of federal employees, agency administrators must input the rider's name, phone number, and pickup and dropoff address in the Central Dashboard.

Version 1.6: 4-17-2025

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

Since a federal employee name, email, and phone number (for Uber Central/Health) is provided by the agency, the agency ensures that the information provided to Uber is accurate and complete. Federal employees can contact their agency regarding trips billed to the agency's enterprise profile. Federal employees can manage their personal account within the Uber App and may submit a privacy inquiry directly to Uber that will allow individual users to access their information. Uber maintains designated external feedback channels, for example, Help pages and call support, for individuals to voice privacy concerns. Uber's Privacy Team monitors these channels and has established processes to address and escalate this feedback, as appropriate.

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?

Production Access - Role Access Permissions
Employee and contractor system access requirements are documented in the Human Resources Information System (HRIS) by the hiring manager prior to access being granted. Upon hire, employees are assigned a specific role based on location, employee type and job family, which then map to specific job profiles that grant employees and contractor baseline access permissions within their assigned role.

Customer Responsibility
The customer assigned as Account Administrator is responsible for establishing account access to the U4B products to only those individuals that require access. Customers are responsible for establishing their own separation of duties based upon their mission and Agency/Department policy. Customer application user accounts are created by the customer's designated account managers. This process is controlled by the customer's internal account management policies.

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

Yes - SSPP has been submitted.

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

The U4B products protect the confidentiality and integrity of transmitted information through the implementation of cryptographic mechanisms for data transmitted through the data and administrative sections of the environment. Secure Shell (SSH) is used to protect the confidentiality and integrity of all information transmitted for remote host access using bastion hosts. Uber leverages TLS (Transport Layer Security) 1.3 Hypertext Transfer Protocol Secure (HTTPS) with Federal Information Processing Standards (FIPS) compliant ciphers (i.e., AES-128, AES-256) for the transmission of data over the Internet.

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?

The Security Response and Investigations team is the principal responder for cybersecurity incidents and is involved throughout the entire incident response cycle. Alerts and escalated incidents are triggered in various ways and managed in Uber's incident management tracking tool. The Security Response and Investigations team provides 24/7 on-call coverage to investigate, research, validate findings and correlate the related audit logs/events to respond to any potential security incidents.

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.

U4B Travel: Federal employees may either accept or decline the invite sent from the agency administrator. If the federal employee declines the invite, an enterprise profile will not be established and no trip information will be shared with the agency. By accepting the invite, the federal employee can establish an enterprise profile within the Uber app. Federal employees consent to sharing trip information with the agency that provisioned the access any time they take trips using their enterprise profile. Federal employees may toggle between using their enterprise profile and personal profile at any time.

Uber Central: For agency administrators to arrange Uber rides on behalf of federal employees, agency administrators must input the rider's name, phone number, and pickup and dropoff address in the Central Dashboard.

Uber Health: For administrators to arrange Uber rides on behalf of riders/patients, administrators must input the rider/patient's name, phone number, and pickup and dropoff address in the Health Dashboard.

6.2 What procedures allow individuals to access their information?

Federal employees can contact their agency administrators regarding trips billed to the agency's enterprise profile. Federal employees can also manage their personal account within the Uber rider app or submit a privacy inquiry directly to Uber that will allow individual users to access their information (this service is available for riders without an Uber account, i.e., for Uber Central where an agency administrator arranges rides on behalf of federal employees). Uber maintains designated external feedback channels, for example, Help pages and call support, for individuals to voice privacy concerns. Uber's Privacy Team monitors these channels and has established processes to address and escalate this feedback, as appropriate.

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

Federal employees can contact their agency administrators regarding trips billed to the agency's enterprise profile. Federal employees can also manage their personal account within the Uber rider app or submit a privacy inquiry directly to Uber that will allow individual users to access their information (this service is available for riders without an Uber account, i.e., for Uber Central where an agency administrator arranges rides on behalf of others).

Uber facilitates transparency and choice by providing consumers with privacy settings and the right to access and correct personal information associated with their accounts. For example, Uber's data download service allows users to download mobile event data related to their Uber Rider trips. In addition, Uber has built several data minimization and management technical solutions, including a platform to manage account deletion requests, capabilities to support data deletion in big data systems, and other technical controls.

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.

Uber provides mandatory privacy and security foundational training to Uber personnel upon hire and annually thereafter. This training covers privacy and security practices and policies relating to physical and cyber security, data access, privacy by design, data minimization, retention and disposal, notice and transparency, consent, and data accuracy.

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?

Uber maintains a privacy program designed to meet requirements of the privacy and data protection laws in the jurisdictions in which Uber operates. The privacy program is overseen by Uber's Chief Privacy Officer. This privacy program includes efforts from Uber's privacy engineering and privacy legal teams, working to enforce privacy as a routine key consideration early in product and engineering life cycles and to advise other teams regarding privacy and data protection requirements.