



***Lyft General Support System Controlled Unclassified
Information (Lyft-GSS-CUI)***

Privacy Impact Assessment (PIA) - Guidance

[12/20/2023 - Date accepted by GSA for completeness]

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 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.

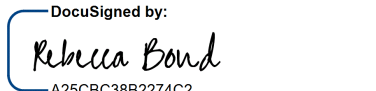
GSA Stakeholders

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

Name of GSA Information System Security Manager (ISSM): Arpan Patel

X 
8B059AABDAF1477...
GSA Information System Security Manager


Name of GSA Program Manager: Rebecca Bond

X 
A25C8C38B2274C2
GSA Program Manager

Name GSA Chief Privacy Officer (CPO): Richard Speidel

X 
171D541183F40A...
GSA Chief Privacy Officer

Name of GSA Contracting Officer Representative (COR): Lamarr Peppers

X 
71C99F9286CF415...
GSA Contracting Officer Representative

800-171 PIA 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
12/15/2023	Minor edits	1.5

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	4
SECTION 5.0 SECURITY	5
SECTION 6.0 INDIVIDUAL PARTICIPATION	6
SECTION 7.0 AWARENESS AND TRAINING	6
SECTION 8.0 ACCOUNTABILITY AND AUDITING	6

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:

Lyft Rideshare

B. GSA Client:

Federal Acquisition Services (Q) - Ride Sharing Program

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

Federal employees who are users of the Lyft platform.

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

- Biographic information (name, date of birth)
- Contact information (email address and phone number)
- Payment information
- Optional account information provided by the user (such as profile photo, saved addresses, address book contacts, preferred pronouns, and other app preferences)
- Ride ratings and feedback;
- Communications between riders and drivers, and between users and Lyft;

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."

- Location information
- Usage information (e.g. ride information like the date and time, route, etc.)
- Lyft app and website interactions;
- Device information;
- Cookies and analytics;
- Information about a user's participation in third party programs offered through Lyft;
- Information to operationalize loyalty and promotional programs;
- Enterprise programs and concierge service information;
- Lyft program referral information; and
- Other users and sources such as law enforcement, insurers, media, or pedestrians who may provide Lyft information about a user, for example as part of an investigation into an incident.

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

Lyft, Inc. partners with the General Services Administration (GSA) and federal agency customers to provide business transportation to federal employees. Lyft, Inc. [referred to throughout as "Lyft"] provides on-demand ridesharing and ride-hailing services by matching drivers and riders via a mobile application. Lyft has entered into a Blanket Purchase Agreement with GSA to allow federal agency customers [referred to throughout as "customer agencies"] to designated eligible employees [riders] to use Lyft for government travel. Including Lyft among the transportation options for government travel allows riders to benefit from the selection and convenience, availability, affordability, and trust and safety Lyft offers.

Lyft receives a secure transmission from each federal customer with the email addresses of employees in the customer agency's expense management system. The employee can then enter the business profile sign-up workflow and either (1) create a new business profile for an existing Lyft account, or (2) create a new Lyft account and a business profile. To start with Lyft, the user must first download the Lyft app and create an account by providing their name, phone number, email address, date of birth, and payment information. Once the account is created, the user can request a ride using the Lyft app.

Lyft provides customer agencies with transaction reports with ride details, fares and other charges for business profile rides linked to each government email address. Lyft also provides a report on charges made to government cards for rides taken on personal accounts; these reports do not include any personally identifiable information.

Lyft collects the following information from users when they create an account and

profile:

- Name
- Email address
- Phone number
- Date of birth
- Payment information (which may include a government payment card)

Users may opt to provide a profile photo, saved addresses, and other preferences such as preferred pronouns.

Lyft collects ride ratings and feedback from users about rides, as well as any information collected when the rider contacts Lyft or vice versa (e.g. content of messages).

Lyft collects the following information about a rider's use of the platform:

- Location information (device's precise location when the app is open and in use, including while the app is running in the background from the time the user requests a ride until it ends)
- Usage information (including ride information like the date, time, destination, distance, route, payment, and whether the rider used a promotional or referral code)
- Lyft app and website interactions (including pages and content viewed and the dates and times of use)
- Device information (including device model, IP address, type of browser, version of operating system, identity of carrier and manufacturer, radio type (such as 4G), preferences and settings (such as preferred language), application installations, device identifiers, advertising identifiers, and push notification tokens)
- Communication between riders and drivers (Lyft works with a third party to facilitate phone calls and text messages between riders and drivers without sharing either party's actual phone number with the other. Lyft collects information about these communications and Lyft Platform chat communications, including the participants' phone numbers, the date and time, and the contents of short messaging service (SMS) messages. For security purposes, Lyft may monitor or record the contents of phone calls made through the Lyft Platform, but always lets the user know before the call begins)
- Address Book Contacts (optional - riders may set device permissions to grant Lyft access to contact lists to help refer friends to Lyft. When the rider chooses this option, Lyft access and stores the names and contact information of the

- people in the address book)
- Cookies, Analytics, and Third Party Technologies: Lyft collects information through the use of “cookies”, tracking pixels, data analytics tools like Google Analytics, software development kits (SDKs), and other third party technologies. Lyft may use both session cookies and persistent cookies. Users may consult their web browser(s) to modify their cookie settings.

Lyft may also collect the following information from other sources:

- Information about a user’s participation in third party programs offered through Lyft;
- Information to operationalize loyalty and promotional programs;
- Enterprise programs: for those who use Lyft through an employer, Lyft collects information about the user from those parties (including name and contact information).
- Concierge Service: If an organization has ordered a ride for a user using our Concierge service, they will provide us with the user’s contact information and the pickup and drop-off information.
- Lyft program referral information; and
- Other users and sources such as law enforcement, insurers, media, or pedestrians who may provide Lyft information about a user, for example as part of an investigation into an incident.

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.

Potential riders will receive an invitation to sign up for a business profile under their employer. Users are aware of Lyft's collection of their information when they submit their own information to create an account and to request rides. Lyft also provides detailed notice of the way it collects, uses, and maintains user information via its Privacy Policy, which is available both in the app and on the Lyft website. All users are provided with and must accept the Privacy Policy when they create a Lyft account (<https://www.lyft.com/privacy>).

SECTION 2.0 DATA MINIMIZATION

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

Lyft requires PII in order to deliver rideshare services. The following information collection is necessary:

- Basic user personal information including name, email address, phone number, and date of birth (to verify the user's identity)
- Payment information (to charge riders and pay drivers)
- Location information (to enable pickups and ride routes)

Users can modify or remove optional information like profile pictures and saved address shortcuts at any time, and can update and remove payment information. The rest of the personal information is necessary for the operation, safety, and security of the Lyft platform.

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

Lyft collects rider location information differently depending on the Lyft app settings and device permissions. For example, users can control Lyft's collection of background location information at any time by going into the Lyft app privacy settings. Detailed information about rider location is available on the Lyft website:

<https://help.lyft.com/hc/en-us/articles/360046897454-Rideshare-Passenger-Location>.

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

While Lyft does not create targeted “reports” on any specific individuals, various data sets containing personal information can be accessed by certain Lyft employees for specific business purposes (investigating an incident, providing customer support, etc.). This is restricted only to specific employees who have a business need through role based access controls. Lyft may also be obligated to share “reports” externally for regulatory compliance purposes; in such cases, the data is aggregated or de-identified. For example, Lyft may need to provide an airport authority with a regular cadence of reports regarding rides originating or ending at a given airport so per-ride airport authority fees can be assessed. Lyft provides further information on the types of personal information it collects and how it’s used and shared in the Lyft Privacy Policy.

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?

As mentioned above in 2.3., Lyft does not build “reports” on specific individuals. Access to granular personal data for specific business purposes (investigating an incident, providing customer support, etc.) at Lyft is controlled through role based access controls. For any reporting that is shared more broadly within the company such as for management reporting or financial reporting, the data set is typically aggregated and is handled in accordance with our internal policies for data classification. As mentioned above in 3.3, Lyft may also share reports externally for regulatory compliance purposes; in such cases, the data is aggregated or 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?

Lyft limits its use of rider information to the purposes described in the Privacy Policy:

- To provide the Lyft platform;
- To maintain the security and safety of the platform and its users;
- To build and maintain the Lyft community;
- To provide customer support;
- To improve the Lyft platform; and
- To respond to legal proceedings and obligations.

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?

Lyft will provide customer agencies with transaction reports with ride details (ride type, requested and actual pick-up and drop-off address, distance and duration), and fares and other charges linked to each government email address. Lyft will also provide a report on charges made to government cards for rides taken on personal accounts; these reports will not provide any personally identifiable information.

In general, Lyft shares personal information in the following circumstances, as detailed in the Privacy Policy:

- With other platform users (e.g. drivers) in order to ensure that the right person is getting into the right car;
- With third party service providers that support Lyft's businesses (e.g. by storing data, or providing telecom services to connect calls and texts between riders and drivers using masked numbers)
- With other third parties with the consent or at the direction of the user;
- When obligated, such as in response to valid law enforcement requests.

3.3 Is the information collected directly from the individual or is it taken from another source? If so, what are the other source(s)?

Lyft receives email addresses from the employer in order to send business profile invitations.

Lyft collects account information and platform use information (such as ride details) from the user and the user's device.

Lyft receives name and contact information from employers for users of enterprise programs.

Lyft collects some information from third party services:

- Related to participation in third party programs that provide things like insurance converge and financial instruments, such as insurance, payment, transaction, and fraud detection information;
- To operationalize loyalty or promotional programs,
- demographic and market segment information

Lyft may also receive information about users from the public or other third parties (such as law enforcement) as part of an investigation into an incident or to provide support.

SECTION 4.0 DATA QUALITY AND INTEGRITY

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

Government agencies provide Lyft with the email addresses of their employees. Lyft users provide their own data to Lyft during account creation. Users are able to correct and update their own information by logging into their account. They can change things like payment information, contact information, profile picture, preferred pronouns, and saved address shortcuts like home and work. Users may contact the Lyft Help Center for additional support.

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?

The Lyft-GSS-CUI environment is accessed by users (riders, individuals requesting vehicles on behalf of riders) through the front-end Lyft Application or Lyft Website and enter through Envoy Load Balancer. Connections are encrypted through a Hypertext Transfer Protocol Secure (HTTPS) connection (port 443). Lyft user roles (Lyft Admins, Engineering, Non-Engineering, Customer Support Partners) access the environment through a variety of means, depending on their job function. Access to the environment and the supporting third party services is secured with HTTPS, Remote Desktop Protocol (RDP), or Secure Shell or Secure Socket Shell (SSH) protocols. The supporting third party applications, including Amazon Web Services (AWS), authenticate using Duo single sign on with multi-factor authentication. Once the user has entered the environment, all connections between services are secured with HTTPS. All services and applications which store CUI data at-rest are securely encrypting the data storage with widely supported and recognized encryption ciphers and algorithms (i.e. AES [Advanced Encryption Standard]-256).

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

Yes, the SSPP has been submitted.

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

All relevant controls for physical, technical, and managerial perspectives are documented in the SSPP. These controls include security guards, ID badges, key cards, etc. for physical locations where applicable as well as a dependency on AWS for these same controls at data centers where Lyft data is processed/stored. In addition, technical protections for accessing information include unique user IDs, role-based access control, encryption at rest for databases and in-transit when outside of Lyft's service mesh. To ensure Lyft meets its customer contractual commitments as outlined in the SSP, Lyft conducts annual Service Organization Control (SOC) 2 Type II audits, NIST Cyber Security Framework (CSF) self and third party reviews, a continuous monitoring program, and NIST SP 800-171 assessments every three years (last assessment conducted 12/2020).

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?

Lyft maintains a dedicated Security Incident Response Team as well as a documented incident response plan that is reviewed and tested on an annual basis. Incidents are classified based on an internal risk assessment that includes the scope of a breach and the information that may be compromised as well as directions on notifying customers, authorities, etc. This incident response plan is reviewed as part of our annual SOC 2 Type II audit as to its design and operating effectiveness and is also evaluated as part of our NIST SP 800-171 assessment.

Lyft actively monitors security vulnerabilities, including through a Bug Bounty program, which allows researchers and members of the public to report suspected bugs and vulnerabilities. Lyft also maintains a robust vulnerability management program to track and address vulnerabilities.

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.

Government employees may not opt out of their employer's exchange of their email address with Lyft, but they may decline to set up an account with Lyft.

Some information, including name, contact information, and payment information, is required in order to use the Lyft platform. Users may choose to opt out of this collection only by declining to use the Lyft platform.

Some information (such as profile photo) is strictly optional for riders, and they may choose to opt out or delete the information at any time.

6.2 What procedures allow individuals to access their information?

Users can see information Lyft maintains by logging into their account and viewing their profile, settings, preferences, ride history, and payment information. Users may also request to download their data from Lyft via the privacy home page (<https://www.lyft.com/privacy/home>).

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

Users may correct and update their own account information (including payment and contact information and any optional information such as profile picture, preferred pronouns, and saved address shortcuts) by logging into their accounts.

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.

Lyft requires all employees to complete annual privacy training that explains how to protect user privacy and personal information.

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?

Lyft has the following protections in place to safeguard information:

1. Role-based access controls ensure access and usage of the data is limited to employees with a legitimate business purpose; access requires approval by role owners and regular recertification, as well as being subject to routine audits.

2. Dedicated Privacy and Security teams responsible for product and feature reviews that ensure PII and CUI is used only in accordance with Lyft's privacy policy.
3. Annual privacy and security training that reinforces the privacy and information security protocols employees are required to follow.

In addition, Lyft maintains multiple external compliance certifications/assessments focused on data security and security controls (such as Health Information Portability and Accountability Act [HIPAA] and SOC 2 Type II).